CENTRO DE EDUCAÇÃO SUPERIOR REINALDO RAMOS/CESREI

FACULDADE REINALDO RAMOS/FARR

CURSO DE BACHARELADO EM DIREITO

JOSÉ GABRIEL QUEIRÓS PINTO

DIREITO DIGITAL E ASPECTOS PENAIS DA LEI BRASILEIRA

CAMPINA GRANDE-PB

2016

JOSÉ GABRIEL QUEIRÓS PINTO

DIREITO DIGITAL E ASPECTOS PENAIS DA LEI BRASILEIRA

Trabalho Monográfico apresentado à Coordenação do Curso de Direito da Faculdade Reinaldo Ramos – FARR, como requisito parcial para a obtenção do grau de Bacharel em Direito pela referida Instituição.

Orientador (a): Prof. Ms.Rodrigo Reul

CAMPINA GRANDE-PB

2016

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DA CESREI

P Pinto, José Gabriel Queirós.

659l

Direito digital e aspectos penais da lei brasileira / José Gabriel Queirós Pinto. – Campina Grande, 2016.

42 f.

Monografia (Bacharelado em Direito) – Faculdade Reinaldo Ramos-FAAR, Centro de Educação Superior Reinaldo Ramos-CESREI, 2016.

"Orientação: Prof. Esp. Rodrigo Araújo Reúl".

1. Direito Digital – Brasil. 2. Internet – Crimes Digitais - Brasil. I. Reül, Rodrigo Araújo. II. Título.

CDU

34:004.738.5(81)(043)

JOSÉ GABRIEL QUEIROS PINTO

DIREITO DIGITAL E ASPECTOS PENAIS DA LEI BRASILEIRA

Aprovada em: 02 de Agosto de 2016.

BANCA EXAMINADORA

Prof. Ms. Rodrigo Araújo Reul
Faculdade Reinaldo Ramos – FARR
(Orientador)

Prof. Esp. Francisco Iasley Lopes de Almeida
Faculdade Reinaldo Ramos – FARR
(1º Examinador)

Prof. Ms. Vinicius Lucio de Andrade
Faculdade Reinaldo Ramos – FARR
(2º Examinador)

RESUMO

O presente trabalho objetivou averiguar a evolução da sociedade conjuntamente com o direito, onde ambos sofrem mutações a partir do desenvolvimento tecnológico e mais especificamente o crescimento da informatização em todos os processos sociais. Esses fenômenos atingem o direito gradativamente, gerando novas temáticas a serem abordadas, assim aconteceu com o Direito Digital, bem como modificando o Direito Penal, diante das invasões dos dispositivos informáticos foi preciso criar a Lei n. 12.737/2012 para que houvesse uma punição especifica para esse tipo de conduta que a cada dia virava rotina. Para tanto, foi utilizado como método na coleta de dados a pesquisa bibliográfica, através do estudo levantado no referencial teórico Direito Digital, artigos científicos, e projetos de lei que visam às modificações de legislação penal na seara digital. Apesar do avanço obtido nos últimos anos no que tange essa matéria, fica claro existem muitas lacunas a ser preenchida por leis que atendam de maneira satisfatória a junção do direito penal, com os avanços que acontecem no meio informático. Enfim, por meio de toda pesquisa realizada e das inovações que o legislativo conjuntamente com o judiciário vem fazendo, apesar de o legislativo caminhar em passos lentos, já se nota uma vertente disposta a trabalhar nessa área em virtude das grandes mudanças que ocorrem na mesma, fazendo com que se acompanhem de maneira satisfatória os novos fenômenos trazidos nessa nova seara do direito.

Palavras-chave: Direito Digital. Internet. Crimes Digitais. Direito Penal

SUMMARY

The present work aimed to ascertain the evolution of society together with law, where both are mutated from technological development and more specifically the growth of computerization in all social processes. These phenomena reach the law gradually, generating new topics to be addressed, as happened with the Digital Law, as well as modifying the Criminal Law, before the invasions of the computer devices was necessary to create Law n. 12.737 / 2012 so that there would be a specific punishment for this type of conduct that became routine every day. In order to do so, the bibliographical research was used as a method in the data collection, through the study raised in the theoretical reference Digital Law, scientific articles, and bills that aim at the modifications of criminal law in the digital field. Despite the progress made in recent years in this matter, it is clear that there are many gaps to be filled by laws that meet in a satisfactory way the joining of criminal law, with the advances that occur in the computer environment. Finally, through all the research carried out and the innovations that the legislature has been doing together with the judiciary, despite the fact that the legislature is moving slowly, there is already a tendency to work in this area due to the great changes taking place in it, So that the new phenomena brought into this new area of law are accompanied in a satisfactory way.

Keywords: Digital Law. Internet. Digital Crimes. Criminal Law

SUMÁRIO

INTRODUÇÃO

O direito é uma matéria que muda constantemente, sendo uma ciência social, a partir das mudanças presentes na sociedade o direito tem a obrigação de se adaptar para que atenda as demandas dos indivíduos, uma vez que elas modificam-se.

Esses fenômenos de mudanças veem acontecendo em virtude dos avanços tecnológicos e científicos do século XX, onde se iniciou o nascimento dos primeiros computadores e internet. Nesse contexto, à partir do fenômeno da globalização, houve uma integração das culturas diante do advento da internet causando uma série de avanços e modificações no seio da sociedade assim como também no direito, que fomentou uma nova matéria o Direito Digital ou Virtual.

De forma geral o Direito Digital surgiu como fenômeno da globalização, o crescimento tecnológico rápido foi o principal advento. Desta maneira o Direito Digital se inseriu em várias disciplinas do direito fazendo com que ambas passassem a andar lado a lado. E não podia ser diferente com Direito Penal, tendo em vista as modificações na prática de novos delitos na Era da Informação.

Diante do novo cenário mundial, em que existe uma integração muito grande dos indivíduos de toda a parte do globo terrestre graças ao poder da internet e suas ferramentas de comunicação, atualmente estimasse que mais de 2 bilhões de pessoas estejam conectados com a rede mundial de computadores. Logo notasse que as diversas interações produzidas gerem novas maneiras também de cometer atos ilícitos, nesse viés o Direito Digital e o Direito Penal tem sofrido modificações e buscado acompanhar para a prevenção e combate da criminalidade 2.0, conhecida por manter e praticar delitos na internet.

Nosso objetivo é acompanhar e debater sobre esse tipo recente de criminalidade que está em crescimento exponencial e necessita de uma maior atenção por parte dos nossos legisladores brasileiros, visando andar junto com a evolução da comunidade e atender os anseios.

Como se observa, para acompanhar os avanços da sociedade e suas interações, o direito precisa está em frequente modificação, nessa nova Era da Informática, com a facilidade e aumento das comunicações o surgimento de novas celeumas no meio social é frequente, seja por meio de uma discussão via rede social, ou até mesmo por fraudes causadas por vírus informático. Nesse intento a proposta cientifica é explanar as modificações da temática no âmbito brasileiro, como também atentar para a ocorrência de algumas atividades delituosas e como são tratadas perante nosso judiciário.

Para o desenvolvimento do presente trabalho foi utilizada a pesquisa bibliográfica, baseada em livros, artigos científicos, sítios eletrônicos, trabalho acadêmico. Como livro principal, trabalhamos com Direito Digital, Patrícia Peck Pinheiro, por ser um livro praticamente completo para a pesquisa na seara do Direito Digital.

O trabalho de conclusão de curso estrutura-se em três capítulos, onde no primeiro capitulo traz a evolução histórica do Direito Digital e suas mudanças com o decorrer do tempo e evolução tecnológica da sociedade, fazendo uma alusão ao Marco Civil da Internet no Brasil onde ocorreram algumas modificações na seara penal. No segundo capítulo falamos sobre os crimes cibernéticos de maneira geral e suas características, e uma pequena análise de alguns preceitos inseridos na matéria penal. O terceiro capítulo é responsável pela a maior parte do trabalho, sendo a análise das leis n. 12.735/2012 e a n. 12.737/2012 feita de maneira mais profunda, e alguns aspectos dos delitos mais comuns atualmente e como são tratados perante a jurisprudência brasileira.

1 HISTÓRICO DO DIREITO DIGITAL

Desde a revolução industrial que a sociedade vem em crescimento exponencial, tanto na criação de novas tecnologias, como no cenário atual, cada vez mais indivíduos adentram no espaço virtual. Essa era da informação tem sido importante na mudança em vários aspectos do dia a dia de uma grande parte da população mundial, tanto na parte das comunicações onde se aprimorou muito, nos dias atuais se conversa com uma pessoa do outro lado do hemisfério tranquilamente, seja por redes sociais, websites.

> A sociedade humana vive em constante mudança: mudamos da pedra talhada ao papel, da pena com tinta ao tipógrafo, do código Morse à localização por *Global Positioning System* (GPS), da carta ao *email*, do telegrama à videoconferência. Se a velocidade com que as informações circulam hoje cresce cada vez mais, a velocidade com que os meios pelos quais essa informação circula e evolui também é espantosa (PINHEIRO, 2013, p. 32)

Marcando o inicio dessa era de processamento de dados, temos a invenção da máquina ‘’computador’’, responsável por tratar automaticamente informações , processar e armazenar dados. Os primeiros computadores eletromecânicos remetem ao inicio do século 20, principalmente com as guerras sucessivas houve um crescimento na busca e aperfeiçoamento dessas máquinas, como exemplo temos o computador construído pela a marinha conjuntamente com a universidade de harvard chamado de harvard mark i.

> No ano de 1946, ocorreu uma revolução no mundo da computação com o lançamento do computador eniac (electrical numerical integrator and calculator), desenvolvido pelos cientistas norte-americanos john eckert e john mauchly. Esta máquina era em torno de mil vezes mais rápida que qualquer outra que existia na época. A principal inovação nesta máquina é a computação digital, muito superior aos projetos mecânicos-analógicos desenvolvido até então. Com o eniac, a maioria das operações era realizada sem a necessidade de movimentar peças de forma manual, mas sim pela entrada de dados no painel de controle. Cada operação podia ser acessada através de configurações-padrão de chaves e switches.(wikipédia).

.

A origem da internet remonta ao ápice da “guerra fria”, em meados dos anos 60, nos Estados Unidos, e foi pensada, originalmente, para fins militares. Basicamente, tratava-se de um sistema de interligação de redes dos computadores militares norte americano, de forma descentralizada. À época, denominava-se “Arpanet”. Esse método revolucionário permitiria que, em caso de ataque inimigo a alguma de suas bases militares, as informações lá existentes não se perderiam, uma vez que não existia uma central de informações propriamente dita.

Posteriormente, esse sistema passou a ser usado para fins civis, inicialmente em algumas universidades americanas, sendo utilizado pelos professores e alunos como um canal de divulgação, troca e propagação de conhecimento acadêmico-científico. Esse ambiente menos controlado possibilitou o desenvolvimento da internet nos moldes os quais a conhecemos atualmente.

Na década de 90, a Internet passou por um processo de expansão sem precedentes. Seu rápido crescimento deve-se a vários de seus recursos e facilidades de acesso e transmissão, que vão desde o correio eletrônico (*e-mail*) até o acesso a banco de dados e informações disponíveis na World Wide Web (WWW), seu espaço multimídia. Tecnicamente, a internet consiste na interligação de milhares de dispositivos do mundo inteiro, interconectados mediante protocolos (IP, abreviação de *Internet Protocol*). Ou seja, essa interligação é possível porque utiliza um mesmo padrão de transmissão de dados. A ligação é feita por meio de linhas telefônicas, fibra óptica, satélite, ondas de rádio ou infravermelho. A conexão do computador com a rede pode ser direta ou através de outro computador, conhecido como servidor.

Este servidor pode ser próprio ou, no caso dos provedores de acesso, de terceiros. O usuário navega na internet por meio de um *browser*, programa usado para visualizar páginas disponíveis na rede, que interpreta as informações do *website* indicado, exibindo na tela do usuário textos, sons e imagens. São *browsers* o MS Internet Explorer, da Microsoft, o Netscape Navigator, da Netscape, Mozilla, da The Mozilla Organization com cooperação da Netscape, entre outros.

A partir daí houve criação de computadores portáteis, a criação da internet e o ambiente virtual, assim as primeiras redes sócias na década de 90, até os tempos atuais onde temos smartphones que levamos para todos os cantos no bolso, onde o mesmo realiza tarefas de ligação telefônicas à tarefas de computadores propriamente ditos.

Nos dias atuais calcula-se mais de 2 bilhões de internautas no mundo, sendo assim, um terço da população interligada pela rede. Com os avanços na informática em conjunto aos de audiovisual e das telecomunicações, criou a possibilidade de novos serviços. Após o desenvolvimento de redes de banda larga com fio (adsl e fibra óptica) como também da comunicação sem fio (wifi, bluethooth e redes movéis 2g, 3g), e internet móvel (wap), ampliaram-se outras tecnologias e produtos da chama ‘’web 2.0’’, que seria nada mais que a segunda geração responsável pela massificação das comunicações interativas seja por via de blogs, sites de busca, redes sociais e de compartilhamento de fotos e vídeos. Assim transformando o modo de se comunicar e se expressar cada vez mais dos internautas, usando os vários serviços da internet, criando uma cultura de compartilhamento em rede.

Como destaca o site techtudo,

> A internet discada deu lugar à banda larga e até à conexão no seu próprio celular, com a rede 3g (e agora 4g). Ao invés de uma ferramenta de difícil acesso e ainda crescendo, a internet virou praticamente uma necessidade diária, seja no dia a dia das empresas ou na casa de um usuário que busca entretenimento ou faz pesquisas para o dever de casa. O compartilhamento de arquivos em sites p2p como o kazzaa surgiu para destacar uma faceta multimídia da internet. Veio a era das redes sociais, para reunir amigos e fazer os novos contatos, com orkut, myspace, twitter, facebook e etc. Os simples icq e msn deram lugar ao skype e ferramentas que permitem fazer até ligações para telefones comuns. Cresceu o número de provedores, o comércio online se estabeleceu, o mercado de jogos apostou no online e agradou, há centenas de redes de conteúdo multimídia usando tanto streaming como buffer para entreterem os internautas… hoje, a internet é um mundo de grandes possibilidades. E não há dúvida de que o futuro ainda reserva mais novidades. (BARROS, 2013).

1.1 PRIMEIROS ASPECTOS JURIDICOS DIGITAIS NO BRASIL

A sociedade vem em constante evolução com o passar dos anos, em muitos quesitos tais tecnológico, econômico e social. Com o nascimento da internet transformações vêm acontecendo, e em meio a essas transformações está o Direito Digital. Vale ressaltar que a internet não se trata de um simples meio de comunicação que se integra com uma gigante rede por todo o globo de computadores, assim como também milhões e por que não bilhões de indivíduos; empresas, instituições e empresas, acontecendo uma grande mudança na forma de ver e interpreta o Direito nesse contexto define Pinheiro,

> Pode-se dizer que existiram dois fatos históricos importantes para a abertura de muitas questões jurídicas que se apresentam na sociedade brasileira. Neste contexto, temos: em 1990, ano da criação do primeiro Código Brasileiro de Defesa do Consumidor e em 1995, quando ocorreu a publicação pelo o Ministério das Comunicações da Norma 004, regulando assim o uso de meios de rede pública de telecomunicações para o provimento e a utilização de serviços de conexão à Internet. Criando-se uma consciência do consumidor e a entrada da Internet nas residências, aos poucos se cria um raciocínio jurídico sustentável, observando os padrões de conduta no dia a dia de experiências de problemas práticos e de soluções (PINHEIRO, 2013, p. 30).

Como vemos, a evolução se deu de maneira tímida no Brasil, na década de 90, como citado, existe dois pontos onde nasce para o direito brasileiro a normatividade no âmbito digital com a regulamentação da rede pública de telecomunicações para o provimento e utilização da conexão da Internet.

1.2 DO MARCO CIVIL DA INTERNET E O DIREITO DIGITAL

Conhecido como Marco Civil da Internet, o Projeto de Lei 2.126/2011 constitui um regulamento civil do uso da Internet no Brasil. O inicio dos debates sobre a necessidade de um marco regulatório civil quanto à utilização da Internet foi iniciativa do Ministério da Justiça (MJ) e da Fundação Getúlio Vargas (FGV). O

professor Ronaldo Lemos, da FGV, publicou, em 22 de maio de 2007, um artigo defendendo a necessidade de criar regras para o uso da Internet.

O Marco Civil da Internet. Em vez de tratar da regulação da internet criminalmente, que seria o natural, seguido por diversos outros países, seria primeiro a construção dos direitos civis na internet. Em vez de repressão e punição, a criação de uma moldura de direitos e liberdades civis, que traduzisse os princípios da Constituição Federal para o território da internet.

A aprovação do Marco Civil da Internet veio para facilitar a resolução de crimes na internet, facilitando a investigação da autoria do fato pois os provedores são possibilitados de guardar logs que são dados responsáveis por pela a conexão do usuário, incluindo seu IP (endereço de identificação), a data e hora dos acessos. As empresas provedoras do serviço de conexão são as responsáveis por armazenagem de conversas, informações, sendo as mesmas capazes de identificação do usuário e podendo corroborar com o judiciário nesse sentido.

A privacidade é um dos fatores importantes do Marco, sendo em regra toda mensagem e comunicação sigilosa, salvo quando interesse da justiça na resolução de crimes. Como ressalta o delegado Carlos Miguel Sobral, chefe do Serviço de Repressão a Crimes Cibernéticos da Direção-Geral da Polícia Federal. ‘’As pessoas não devem ser obrigadas a se identificar. Sobral afirma que há instrumentos tecnológicos que o Estado pode utilizar como meios de investigação. ’’

Notamos certa apreensão das autoridades no quesito da punibilidade e extensão da pena, já que alguns crimes incorrem no Juizado Especial Criminal, sua pena não será superior a 2 anos, deixando assim um ar de impunidade para a sociedade e até mesmo para o aplicador da lei que fica de mãos atadas.

2 CRIMES CIBERNÉTICOS

Em virtude de toda evolução e dinamismo social, cultural, tecnológico, no contexto atual da Internet e da era informacional, existe certa dificuldade em legislar sobre crimes na era Digital. Tendo em vista as ''máquinas'' onde se praticam os delitos, consequentemente geram também as provas são incapazes de diferenciar a culpa do dolo e vice e versa. Dentro de toda essa atmosfera, temos novas condutas, assim como condutas antigas passíveis de novas punições, fazendo-se necessária uma atualização na legislação penal e processual penal pátria.

No dizer de Pinheiro (2013) Não se modificam o conceito de questões em relação ao crime, delito, ato e efeito, permanecem as mesmas seja aplicadas para o Direito Penal ou para o Direito Penal Digital. Neste contexto, fica claro que surgem novas condutas jurídicas no seio Digital no que se refere à territorialidade e à investigação probatória, assim como uma busca pela a tipificação penal de diversas modalidades que, diante da sua particularidade se ensejam a um tipo penal próprio.

É interessante, aliás, observar a crescente escalada que se deu o direito nas últimas décadas, tendo em vista a nova era informacional onde se agrupam milhões, bilhões de indivíduos, empresas e repartições governamentais, gerando assim uma grande gama de novas condutas dentro do espaço virtual. Na busca pela a tipificação dessas condutas está o Direito Penal, porém, sabemos que o direito deveria evoluir conjuntamente com a sociedade, mas não o faz assim de maneira fácil e ágil, oque gera uma serie de condutas não qualificadas dentro do Direito Penal, como assevera Filho:

> Não se deve deixar de lado a ideia de informatização dos meios eletrônicos, seria um retrocesso, vislumbrando uma aplicação do Direito Digital e processual, adotando-se na esfera penal no que se refere aos meios probatórios. Excetuando-se o interrogatório e a citação, todo o resto do processo tem uma grande possibilidade de tornasse totalmente eletrônico, sendo armazenado em sistema computacional seguro nos termos da norma ABNT nº 27.001/2006, que versa sobre a segurança em termos de tecnologia de informação. De acordo ainda com a Lei 9.296/1996 no que tange a provas, onde se tem direito material, tipificando o crime de interceptação de dados telefônicos com matéria de direito processual no que se refere à prova obtida por interceptação telefônica ou telemática. (FILHO, 2012, p. 52).

Pode se dizer neste contexto que a congruência das normas penais, processuais penais não andam lado a lado com Direito Digital, sendo evidenciada a evolução desse direito, é necessária sua aplicabilidade adequada dentro da seara criminal. Fatores como a territorialidade e identidade digital ou prova de autoria dificultam esse trabalho, assim como os legisladores também sofrem para criação e adequação de tipos penais devidamente qualificados.

Assim como a criminalidade clássica, a cibercriminalidade se mostra em diversas condutas, podendo ocorrer em qualquer lugar e horário. Os criminosos cibernéticos usam métodos diferentes segundo suas habilidades e seus objetivos. Esse fato não deveria ser surpreendente, afinal, o crime cibernético é nada mais que um "crime" com um ingrediente "informático" ou "cibernético".

De acordo com Krone, O Tratado do Conselho Europeu sobre Crime Cibernético decidiu usar a terminologia ‘’cibercrime’’, para classificar delitos que vão desde atividades criminosas contra dados até infrações de conteúdo e de coryright. Porém, buscando uma análise mais extensa, Zeviar-Geese sugerem que dentro desse rol, seja incluso atividades como fraude, acesso não autorizado, pornografia infantil e, assédio virtual. Já o Manual da ONU de Prevenção e Controle de Crimes Informáticos compreende os delitos de fraude, falsificação e acesso não autorizado, na sua acepção de cibercrime.

Com base nessas divergentes definições, o cibercrime passa a ser entendido como qualquer delito em que o núcleo objetivo tenha como objeto um computador, uma rede ou um dispositivo de hardware. Devemos atentar para que o computador ou dispositivo possa ser tanto o agente, quanto o facilitador ou mesmo a vítima do delito. O crime poderá acontecer apenas no computador, assim como em outras localidades. Para uma melhor compreensão é necessária a divisão da diversa gama de crimes virtuais, sendo divididos em:

> Os crimes cibernéticos do tipo I apresentam as seguintes características:
>
> Do ponto de vista da vítima, trata-se de um evento que acontece geralmente apenas uma vez. Por exemplo, a vítima baixa sem saber um Cavalo de Tróia que instala um programa de registro de digitação no computador. Também é possível que a vítima receba um e-mail contendo o que parece

> ser um link para uma entidade conhecida, mas que na realidade é um link para um site malicioso. Isso é frequentemente facilitado por software de atividades ilegais, tais como programas de registro de digitação, vírus, rootkits ou Cavalos de Tróia. *Em muitos casos, falhas ou vulnerabilidades no software fornecem um ponto de apoio para o criminoso. Por exemplo, criminosos que controlam um site podem aproveitar a vulnerabilidade de um navegador da Web para introduzir um Cavalo de Tróia no computador da vítima. (Symantec).*

Dentro desse rol de crimes, temos o *phishing*, que seria um roubo ou manipulação de dados ou serviços através de pirataria ou vírus, visando roubo de identidade, fraudes no setor bancário e no comércio virtual. A palavra phishing deriva da língua inglesa, mais especificamente da palavra *fishing,* ou seja, pescar. O termo faz referência aos internautas que mordem a ‘’isca’’. Desta maneira vejamos o conceito técnico:

> *Phishing* é uma forma de fraude em que o atacante tenta extrair informações como credenciais de *login* ou informações financeiras, se passando por uma entidade respeitável ou por uma pessoa, seja via e-mail, mensagens instantâneas ou websites. Normalmente, neste tipo de fraude, a vítima recebe uma mensagem, aparentemente enviada por um contato ou organização conhecida, por exemplo, uma instituição financeira. Um arquivo anexado ou links na mensagem podem instalar *malware* no dispositivo do usuário ou direcioná-lo para um site malicioso criado para induzi-lo a fornecer informações pessoais e financeiras, tais como senhas, identificações de contas (agência, conta-corrente, por exemplo) ou cartão de crédito. Phishing é um método muito popular entre os cibercriminosos. É muito mais fácil induzir alguém a clicar em um link malicioso de um e-mail aparentemente legítimo do que tentar romper as defesas de um computador.*(BATISTA,2016)*

Já nos delitos no ambiente virtual de tipo II, englobam uma série de crimes, como espionagem, assédio, violência, atividade terroristas, extorsão, dentre outros, vejamos suas características:

> As características do crime cibernético do tipo II são: Trata-se geralmente de uma série contínua de eventos envolvendo interações repetidas com a vítima. Por exemplo, o criminoso entra em contato com a vítima em uma sala de bate-papo para estabelecer uma relação ao longo do tempo. Com o tempo, o criminoso aproveita a relação para cometer um crime. Outro exemplo: membros de uma célula terrorista ou organização criminosa usam mensagens ocultas para se comunicarem em um fórum público para planejarem atividades ou discutirem sobre localizações para lavagem de dinheiro. Geralmente, eles usam programas que não estão incluídos na classificação de atividades ilegais. Por exemplo, as conversas podem

> acontecer usando clientes de IM (mensagens instantâneas) ou arquivos podem ser transferidos usando FTP. (Symantec)

São vários tipos de infrações cometidas pela internet, entre elas estão: falsificação de dados, estelionatos eletrônicos, pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito), racismo e xenofobia (difusão de imagens, idéias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica, injúria e ameaças qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade).

No próximo capitulo iremos dar alguns exemplos de crimes virtuais, dentre eles um que recentemente alterou nossa legislação com a aprovação da Lei n. 12.737, de 30 de novembro de 2012, apelidada de Lei Carolina Dieckmann, modifica no velho Código Penal e tipifica uma série de condutas no ambiente digital, principalmente em relação à invasão de computadores, além de estabelecer punições específicas.

2.1 TERRITORIALIDADE

O princípio da territorialidade está interligado com a aplicação da lei penal em face do território criador da norma, não tendo prejuízo os tratados e acordos internacionais, não sendo levada em consideração a nacionalidade do sujeito passivo ou ativo.

Então vejamos oque está expresso na nossa Constituição Federal de 1988:

> Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
>
> § 1º - Para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar.
>
> § 2º - É também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em voo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil.

Alguns outros princípios do Direito devem ser repensados dentro do escopo do Direito Digital, como o princípio da territorialidade. Onde fica a porta? Até onde um ordenamento jurídico tem alcance? O problema não está apenas no âmbito da Internet, mas em toda sociedade globalizada e convergente, na qual muitas vezes não é possível determinar qual o território em que aconteceram as relações jurídicas os fatos e seus efeitos, sendo difícil determinar que norma aplicar utilizando os parâmetros tradicionais.

No dizer de Pinheiro (2013), No mundo tradicional, a questão da demarcação do território sempre foi definida por dois aspectos: os recursos físicos que esse território contém e o raio de abrangência de determinada cultura. A sociedade digital rompe essas duas barreiras: o mundo virtual constrói um novo território, dificilmente demarcável, no qual a própria riqueza assume um caráter diferente, baseada na informação, que, como vimos, é inesgotável e pode ser duplicada infinitamente. A questão se complica se lembrarmos que, com a Internet, as diferentes culturas se comunicam o tempo todo. Não precisamos ir à Turquia para nos relacionarmos com alguém que vive no território geográfico da Turquia. Também, se pretendemos relacionar-nos culturalmente, por via do mundo virtual, com alguém desse território (aqui entendemos cultura no seu modo mais amplo, que inclui, por exemplo, a maneira como os Indivíduos encaram transações comerciais ou questões jurídicas), talvez seja preciso entendermos sua cultura de uma maneira mais profunda do que

se nos deslocássemos fisicamente até lá. Em suma, no Direito Digital, temos de ter uma existência e um entendimento global.

2.2 IDENTIDADE DIGITAL

Uma das questões desafiadoras no que tange ao Direito Digital é a prova de autoria, como se identificaria quem estaria fazendo o uso da máquina. Com o passar dos anos, avanços foram feitos para colaborar no reconhecimento de quem está do outro lado do disposto informático, porém o espaço virtual com toda sua dinâmica e mobilidade induz com que apenas uma identificação biométrica seria capaz de autenticar de maneira segura e válida quem faz uso da internet.

Dessa forma, a dificuldade estaria em operacionalizar o acesso à Internet, salientando-se o crescimento das redes Wi-Fi (internet sem fio), tendo em vista que a difusão das conexões só aumenta por todo o globo terrestre, e que cada vez mais indivíduos vivem no mundo virtual. Nesse conglomerado internacional não possuímos fronteiras de fiscalização, ou seja, não se sabe quem está passando por aquela divisa para a prática de delitos.

O avanço no âmbito brasileiro nos últimos anos para padronização dessa identidade digital, a fim de se tenha com mais solidez uma prova de autoria contundente, vejamos o nosso panorama e os avanços ainda a serem buscados. No dizer de Pinheiro,

> *Esta discussão atinge desde a forma como o Brasil melhorou o padrão do documento de passaporte, o uso de coleta de digitais pela Polícia Federal, inclusive na imigração em diversos países, bem como a entrada em vigor do RIC — Registro Único de Identidade Civil, trazido pela Lei n. 12.058, anunciado pelo Governo Federal, para unificar os documentos de identidade. O documento seria similar a um cartão de crédito com chip, que reúne dados da cédula de identidade atual, CPF e título de eleitor, podendo até ter informações de tipo sanguíneo e se a pessoa é doadora de órgãos. O mesmo será integrado ainda com sistema informatizado de identificação de*

> *impressões digitais, o AFIS. O RIC foi concebido com objetivo de integrar todos os bancos de dados de identificação do Brasil, inclusive podendo receber uma camada de biometria, além de um certificado digital.(PINHEIRO,2013, p. 57)*

Vemos uma preocupação e com razão na que tange a capacidade de identificação do cibercriminoso, pois sem a capacidade da realização da prova de autoria fica difícil caracterizar o crime já que não possui sequer um suposto autor do fato. Um documento de identificação biométrica seria o para formação de um banco de dados com as informações dos usuários da web.

2.3 PRINCÍPIO DA LEGALIDADE

Dentre os vários princípios que norteiam o Código Penal, existe o Principio da Legalidade, que define a não existência de crime sem que haja lei anterior que o defina. Estando estritamente ligado ao art. 5° da Constituição federal em seu inciso II “ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei”. Dessa maneira, ainda dentro da Constituição, temos, em uma acepção jurídico-penal a consagração dos direitos e garantias fundamentais em seu artigo 5°, XXXX, “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”. Como assevera Assis Toledo:

> O princípio da legalidade, segundo o qual nenhum fato pode ser considerado crime e nenhuma pena criminal pode ser aplicada, sem que antes desse mesmo fato tenham sido instituídos por *lei* o tipo delitivo e a pena respectiva, constitui uma real limitação ao poder estatal de interferir na esfera das liberdades individuais.

Dessa forma, a partir do momento em que se exige lei penal anterior, para criminalização de uma conduta, existe uma proteção por trás visando a não violação das liberdades individuais das pessoas, sobretudo considerando que normas que tipificam delitos e criam penas não possuam caráter intimidativo próprio da lei penal.

Portanto ocorreria em injustiça uma lei que regulasse fato anterior à sua vigência, sendo admitida nos casos em que trouxesse benefícios ao réu ou condenado.

Após tal explanação é deveras importantes alguns elementos para constituição do fato criminoso, o fato deve ser típico, contendo o verbo do crime, antijurídico, atingindo de alguma forma a lei vigente e culpável, gerando dolo ou culpa na conduta do agente. Não sendo possível o uso da analogia tendo em vista que o ordenamento jurídico brasileiro não permite para prejudicar o réu.

Diante de o fato acontecer no ambiente digital a situação poderá ocorrer de duas formas diferentes. Quando ocorre do crime ser tipificado pelo ordenamento jurídico, será mudado apenas o ‘’modus operandi’’ na prática do delito. Quando se utiliza de dispositivo eletrônico, seja ele computador, celular, será necessária a inovação de novo tipo penal para a tipificação de tal conduta.

Desta maneira, cabe fazer menção a importante decisão do Ministro do Supremo Tribunal Federal, Sepúlveda Pertence, no julgamento do Habeas Corpus 76689/PB:

> "Crime de Computador": publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte. 1. O tipo cogitado - na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" - ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial. (STF - HC: 76689 PB, Relator: SEPÚLVEDA PERTENCE, Data de Julgamento: 21/09/1998, Primeira Turma, Data de Publicação: DJ 06-11-1998 PP-00003 EMENTA VOL-01930-01PP-00070). BRASIL. Supremo Tribunal Federal. **Habeas Corpus** nº. 76689. Relator: Sepúlveda Pertence, julgada em 21/09/1998, Primeira Turma, Data de Publicação: DJ 06-11-1998 PP-00003 EMENT VOL-01930-01 PP-00070.

Imperioso aqui destacar tal decisão tendo em vista a falta de legislação vigente a tal época, que de maneira exemplar, caracterizou o crime mesmo sendo efetuado por meio diferente, não mudando o núcleo penal da lei, sendo aplicada a pena mesmo sem previsão de lei especificando tal conduta, cabe ressaltar que nem todo delito na seara digital poderá ser analisado dessa maneira.

3 ASPECTOS DAS LEIS QUE TRATAM CYBERCRIME NO BRASIL

Diante do cenário atual, os legisladores brasileiros tiveram que avançar e buscar a produção de leis que protegessem nossos direitos no ambiente digital, dando uma maior segurança jurídica para aplicadores do direito e para a população de maneira geral, já que estaria coibindo práticas delituosas.

Nesse aspecto foram criadas leis que inibissem e ajudassem no combate a propagação desse tipo de delito, de início temos a criação da Lei n.12.735, também conhecida como Lei Azeredo, nome de seu relator deputado Eduardo Azeredo (PSDB-MG). Em conjunto, nessa corrente digital, temos a criação da Lei n. 12.737, mais conhecida como Lei Carolina Dieckmann, atribuição de nome a atriz que sofreu invasão do dispositivo telefônico e teve fotos vasadas na internet.

3.1 LEI AZEREDO

A Lei n.12.375, chamada dessa maneira por que seu idealizador foi o Deputado Eduardo Azeredo, em seu projeto inicial continha pontos polêmicos,como por exemplo, salvar logs de acesso de usuários pelos os provedores, alguns artigos vetados demonstram o quanto foi difícil a aprovação, e o quanto é difícil legislar nessa matéria do direito. Abordando ainda o texto polêmico o Art. 2° buscava equiparar o cartão de crédito a documento particular, sofrendo veto, em seguida tem-se o Art. 3° vetado, em que buscava a tipificação de traição e favorecimento ao inimigo, porém sem a delimitação de dado eletrônico a sua interpretação ficaria prejudicada.

Diante de tantos vetos, ocorram duas aprovações importantes, o artigo 4° que trata da implementação de órgãos investigativos especializados, vejamos:

> *Art. 4° - Os órgãos da policia judiciaria estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.*

Apesar de ser uma medida de grande validade, essa norma é programática, ou seja, depende do Poder Público para sua concretização, investindo em treinamentos e especialização da Polícia nesse sentido e para o combate efetivo dos crimes virtuais.

Do mesmo modo, a lei nº 12.735 no art. 5º, determinou que a lei nº 7.716 adicionasse o inciso II no § 3º do art. 20 obrigando que a prática, a indução ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, praticados por intermédio dos meios de comunicação social ou publicação de qualquer natureza, tenham a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio.

Assim, tínhamos um complemento à lei que veem a tipificar os crimes de descriminação, trazendo um rol de meios em que se poderia fazer a remoção dos conteúdos que infringissem a lei.

Não podemos dizer que foi um total sucesso, após anos de tramitação o projeto n. 84/99 teria sido finalizado em apenas duas normas. Porém, foram bem recepcionadas, mas na prática não alterava muita coisa pois o magistrado com seu poder geral de cautela, por si só determinava a remoção de conteúdos indesejados ou ofensivos que viessem a ser lesivos.

3.2 LEI CAROLINA DIECKMANN

Após a Lei Azeredo, que buscou a tipificação de alguns crimes no ambiente virtual, e que não teve tanto sucesso, veio à criação da Lei n. 12.737, mais conhecida também como Lei Carolina Dieckmann logo após a atriz sofrer violação do seu dispositivo informático, a época não existia norma que previsse tal conduta.

Sendo assim a lei ficou encarregada de tipificar o crime de invasão de computador alheio.

A situação vivida em Maio de 2012 por Carolina Dieckmann demonstrou a fragilidade do código penal na hora de punir o invasor de dispositivo informático, quando teve seu e-mail invadido e Crackers vazaram 36 fotos intimas sem a prévia autorização, sendo um total de 60 arquivos roubados da sua máquina.

A lei promoveu algumas alterações no Código Penal, inserindo os artigos 154-A e 154-B, dando um novo significado ao tipo penal denominado ‘’Invasão de dispositivo informático’’. Ainda no código penal inseriu o § 1o ao art. 266 caracterizando como crime a conduta de interromper “serviço telemático ou de informação de utilidade pública”. Não conseguida antes pela lei 12.735 (Lei Azeredo), implementou o parágrafo único ao art. 298 estabelecendo que configura também o crime de falsidade de documento particular (art. 298) a conduta de falsificar ou alterar cartão de crédito ou de débito.

3.2.1 Algumas alterações promovidas pela Lei n. 12.737 – Lei Carolina Dieckmann

Explanaremos mudanças importantes que a Lei n. 12.737 trouxe para nosso ordenamento jurídico, trazendo assim uma maior segurança à aplicação do judiciário, assim como também uma proteção ao jurisdicionado. Vejamos a lei na integra:

> **“Invasão de dispositivo informático**
>
> 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.

§ 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**.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

"IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

"Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."

Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266. .....

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ "2o Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (NR)

> **“Falsificação de documento particular**
>
> Art. 298 **Falsificação de cartão**
>
> Parágrafo único. ”Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)

Como notasse, a lei aprovada inova quando coloca no rol de crimes a invasão de dispositivo informático alheio, mediante a quebra de segurança do aparelho, sendo agravante ainda a realização de tal fato para obtenção de vantagem para si próprio. Por mais, tipifica o agente que interrompe o serviço telemático ou de informação ao público, e mais importante ainda categoriza no seu art. 298 a falsificação de cartão de crédito, equiparando-o a documento particular.

3.3 INVASÃO DE DISPOSITIVO INFORMÁTICO

O Art. 154-A onde está descrita e caracterizada a invasão de dispositivo, incluindo computadores, celulares, tablets, para resumir, qualquer aparelho que possua conexão de dados ou não, que armazene dados ou informações sem a prévia autorização do seu possuidor. Diante deste cenário cabe ressaltar que aqui o bem protegido é a privacidade, assim como buscasse a proteção da intimidade e vida privada, preceitos esses garantidos pela nossa constituição. Como assevera Pimenta:

> *O direito a privacidade está ligado ao conceito de privado e particular, significando a proteção constitucional à vida privada e aos valores íntimos da pessoa, dentro de sua individualidade. A constituição brasileira em seu art. 5°, inciso X, estabelece que ‘’ são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito de indenização pelo o dano material ou moral decorrente de sua violação’’. A partir desse dispositivo, é de se observar que o direito à privacidade, na Constituição brasileira, deve ser entendido como uma denominação genérica , a qual compreende, de forma específica, a tutela da intimidade, da vida privada, da honra e da imagem das pessoas*.(PIMENTA, 2007, p. 180).

Assim, notamos a importância do Art. 154-A, no que tange a assegurar a privacidade, vida privada, intimidade do jurisdicionado, de maneira que se tem uma maior segurança jurídica. Uma conquista importante com a aprovação desse ponto na lei.

Na classificação dos sujeitos o ativo obviamente pode ser qualquer pessoa que tente violar o dispositivo sem autorização, no polo passivo fica o titular do dispositivo seja ele pessoa física ou jurídica. Ainda sim é possível que o sujeito ativo não seja o dono efetivo do dispositivo invadido, é o caso de computador utilizado por várias pessoas da mesma família, como também a possibilidade da que mantém uma conta de armazenagem de dados em nuvem, por meio de acesso a internet.

Uma grande abertura na lei permite o uso indevido do dispositivo sem anuência prévia, como por exemplo, não configura invasão de o dispositivo for desprotegido por senha ou mecanismo de segurança, como exemplo temos o crime se o indivíduo, na hora do almoço, aproveita para acessar o computador do colega de trabalho, que não é protegido por senha ou qualquer outro mecanismo de segurança não configurara infração penal. O mesmo vale para pen drives desprotegidos, caso alguém pegue e vá vasculhar, não possuindo senha, não configura invasão, como exemplos de mecanismos de seguranças temos senhas, firewall, antivírus, anti-malweres, spywares, entre outros.

Como elemento subjetivo temos o dolo, sendo acrescentado o fim especial de agir, esse dolo especifico pode ocorrer de duas maneiras, para obter, adulterar ou destruir dados e informações do titular do dispositivo; ou a instalação de aberturas que possibilitem uma vantagem ilícita. Para exemplos tomamos o conceito de Spyware a seguir:

> *Spywares são programas espiões, isto é, sua função é coletar informações sobre uma ou mais atividades realizadas em um computador. Todavia, isto não significa que eles sejam em sua totalidade programas maus. Existem sim, muitos spywares de má índole, criados para coletar informações pessoais e, com elas, praticar atividades ilegais. Entretanto, nem todos são assim. Por exemplo: existem empresas de anúncio que se utilizam de spywares para, de forma legal, coletar informações de seus assinantes, com*

> *vistas a selecionar o tipo de anúncio que irão lhes apresentar. (XAVIER, 2008).*

A partir do momento que se tem um spyware em sua máquina, ela se torna insegura sendo vulnerável a invasões e possibilitando assim o roubo de dados.

Entendesse que a consumação seja crime formal, sendo consumada com a simples invasão, dispensando o resultado naturalístico. Sendo assim, não precisa ocorrer obtenção, adulteração ou destruição de dados para que o crime ocorra de fato, via de regre a pericia quem determina a invasão, no entanto é possível a comprovação mediante prova testemunhal.

Nos casos em que houver obtenção de vantagem, caso ocorra prejuízo econômico por parte da vitima incidira aumento de pena previsto no § 2o do art. 154-A, aumentando-se a pena de um sexto e um terço, caso resulte de prejuízo econômico. Vale salientar que não haverá crime de invasão com a causa de aumento de pena do § 2o caso o prejuízo econômico tenha sido pela invasão e subtração de valores, e sim de delito de furto qualificado, pois o furto é mais especifico que o delito de invasão.

No paragrafo terceiro, temos a qualificadora no caso em que a invasão resultar na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, produzindo um pena de 6 meses e multa, caso a conduta não produza crime mais gravoso. Assim caso o agente obtenha conteúdo como e-mails, SMS, diálogos em redes sociais, segredos comerciais ou industriais ou informações sigilosas definidas em lei, incidira a qualificadora.

A tentativa é completamente possível, pois ocorre que o invasor tenta burlar a segurança do dispositivo, mas não consegue a violação do mesmo. Outro ponto de destaque é a pena irrisória, que não protege o bem jurídico de maneira adequada, sendo muito frequente a ocorrência de prescrição retroativa pela pena concretamente aplicada.

O art. 154-A se enquadra em crime de menor potencial ofensivo, sendo sujeito a o Juizado Especial Criminal (art. 61 da Lei n. 9.099/95), como podemos ver:

> **Art. 61.** Consideram-se infrações penais de menor potencial ofensivo, para os efeitos desta Lei, as contravenções penais e os crimes a que a lei comine pena máxima não superior a 2 (dois) anos, cumulada ou não com multa. (Redação dada pela Lei nº 11.313, de 2006)

De maneira geral nos delitos de menor potencial ofensivo a apuração é feita à partir do termo circunstanciado pela a autoridade policial, no entanto, para apuração de autoria e materialidade no caso do art. 154-A não será suficiente o TCO, sendo necessária a instauração de inquérito policial, se considerarmos que na grande maioria dos casos será necessário a realização de busca e apreensão, pericia e oitiva de testemunhas.

Será configurado aumento de pena de um a dois terços caso ocorra divulgação, comercialização ou transmissão a terceiro, a qualquer titulo, dos dados ou informações obtidos, essas são hipóteses § 4o e do § 3º, do artigo 154-A da lei 12.737. Sendo concretizada tal pratica o delito deixa de ser de competência do Juizado Especial Criminal, considerando que, aplicada a causa de aumento sobre a reprimenda prevista no § 3o o crime terá pena máxima superior a 2 anos. No quinto paragrafo temos o aumento de pena caso o delito ocorra contra autoridades eis o rol pertinente:

> § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal

Mediante tal rol, a caracterização de aumento de pena quando o delito envolve agentes políticos, ou da administração direita ou indireta federal, estadual, municipal ou do Distrito Federal, no caso de dirigente, visando a proteção das autoridades.

3.4 AÇÃO PENAL

O artigo 154-B define como será o procedimento de ação penal no caso dos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime for cometido contra administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Em regra no art.154-A é ação penal pública condicionada à representação. Vejamos um conceito breve:

> *No caso da ação penal pública condicionada, o ofendido autoriza o Estado a promover processualmente a apuração infracionária. A esta autorização dá-se o nome de representação, com a qual o órgão competente, ou seja, o* parquet*, assume o* dominus litis*, sendo irrelevante, a partir daí, que venha o ofendido a mudar de idéia.* (CARLOS, 2016).

A justificativa para tal condição se dar em razão da privacidade, vida privada e intimidade serem bens disponíveis, como também dar oportunidade a vitima, que tem o direito de avaliar se deseja seguir ou evitar o processo judicial, tendo em vista a proteção da mesma em virtude de possíveis efeitos negativos com a divulgação das circunstâncias de fato, já que outras pessoas terão acesso ao conteúdo como investigadores, delegados, servidores, promotores e juízes.

3.4.1 Inserção do § 1º ao art. 266 do código penal

A modificação proveniente da Lei n. 12.737/2012 inserindo a § 1o ao art. 266 do Código Penal, no caso alterando a numeração do antigo parágrafo único, passando a ser o § 2º, sem que houvesse modificação no caput. Passando a punir quem interromper serviço telemático ou de informação de utilidade pública, ou impedir ou dificultar o restabelecimento de serviço telegráfico, radiotelegráfico ou telefônico.

Uma das maneiras modernas desse tipo de interrupção é o ataque DoS, notasse que o artigo 266 está com uma defasagem, e muitos desses serviços citados já estão em desuso, porém os ataques DoS são comumente utilizados na rede de internet hoje em dia para derrubar sites, ou qualquer serviço que esteja ligado a rede, bloqueando assim seus serviços, neste sentido vemos o conceito desses ataques:

> Os ataques DoS (sigla para **Denial of Service**), que podem ser interpretados como "Ataques de Negação de Serviços", consistem em tentativas de fazer com que computadores - servidores Web, por exemplo - tenham dificuldade ou mesmo sejam impedidos de executar suas tarefas. Para isso, em vez de "invadir" o computador ou mesmo infectá-lo com malwares, o autor do ataque faz com que a máquina receba tantas requisições que esta chega ao ponto de não conseguir dar conta delas. Em outras palavras, o computador fica tão sobrecarregado que *nega serviço*. (ALECRIM, 2012)

Esse tipo de ataque incorre em quedas de redes e sistemas informacionais, muitas vezes motivados por grupo específicos fazendo protestos contra determinada empresa, buscando prejudicar a prestação de seu serviço, e consequentemente prejudicando quem depende do serviço daquela empresa.

3.4.2 Inserção do parágrafo único ao ar. 298 do código penal

A lei n. 12.737 ainda inseriu no art. 298 do CP o parágrafo único, equiparando a documento particular o cartão de crédito ou débito. Como se trata de falsificação, vejamos oque o STJ entende sobre a clonagem de cartões o qual a subtração ocorre e logo após realizada o saque na conta bancária do titular:

A jurisprudência do STJ entendia tratar-se de furto mediante fraude (art. 155, § 4o, II). Confira:

> "(...) Esta Corte firmou compreensão segundo a qual a competência para o processo e julgamento do crime defurto mediante fraude, consistente na subtração de valores de conta bancária por meio de cartão magnético supostamente clonado, se determina pelo local em que o correntista detém a conta fraudada. (...)"(AgRg no CC 110.855/DF, Rel. Ministro Og Fernandes, Terceira Seção, julgado em 13/06/2012, DJe 22/06/2012).

Após a análise da Lei n. 12.737/2012, a seguir buscaremos discorrer com brevidade sobre alguns delitos praticados no âmbito virtual, e o atual entendimento dos tribunais, como estão sendo trabalhados e julgados, mesmo sem ter uma lei penal especifica para alguns tipos criminais.

3.5 ALGUNS DOS PRINCIPAIS CRIMES PRÁTICADOS NO AMBIENTE VIRTUAL

Mediante a edição das leis vista anteriormente, observamos um pequeno avanço na seara criminal no que tange a tipificação de alguns crimes digitais. Essa tipificação levou uma segurança jurídica maior, à partir desse avanço, o legislativo não deve ficar inerte e produzir cada vez mais leis que contemplem essa temática tão pertinente no nosso dia a dia atual.

3.5.1 Delitos contra a honra na internet

Diante dos avanços da comunidade mundial de internet, a cada dia temos mais facilidade de comunicação e interação com todo o mundo, noticias chegam mais rápido, conferências virtuais são feitas com facilidade de qualquer parte do mundo. Em meio a isso temos as redes sociais, são sites capazes de gerar uma interação enorme entre seus usuários, como Facebook, Whatsapp, LinkediN.

Como leciona PINHEIRO,

> Em razão da falsa aparência de anonimato e de ser a Internet uma ‘’terra sem lei’’, as ofensas propagadas por meios eletrônicos tornaram-se muito comuns no dia a dia. Lembramos que a Constituição Federal garante a liberdade de expressão, mas proíbe o anonimato, oque legitima a identificação do agente para posterior responsabilização.
>
> Aos meios eletrônicos se aplicam as mesmas regras já aplicáveis aos delitos cometidos por outros meios, como, por exemplo, nos crimes contra a honra. Por isso, cresce a responsabilidade de quem publica manifestações de pensamento na Internet e também daqueles que viabilizam os meios para tanto. (PINHEIRO, 2013, p. 369)

Os crimes contra a honra são previsto nos artigos 138, 139 e 140 do código penal, se dividem entre Calúnia, Difamação e Injúria. Vejamos os dispositivos:

> ***Calúnia***
>
> *Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime.*
>
> *(...)*
>
> ***Difamação***
>
> *Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação.*
>
> *(...)*
>
> ***Injúria***
>
> *Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro.*
>
> *(...)*

Dessa forma se observa comumente no dia a dia virtual, vários internautas cometendo tais delitos, seja por inocência, explosão do momento, seja pela a sensação de impunidade, por se esconder atrás de um máquina o individuo acha que tem o direito de falar oque quer sobre outras pessoas. Vejamos alguns julgados e jurisprudência sobre casos:

> *"Constitucional. Dano moral. Art. 5º, V e X, da CF/88. Veiculação maliciosa de notícia em jornal e página da Internet. CRTR — 4ª Região. Sentença confirmada.* I — Evidente a ofensa à honra e à imagem, merece a correta reprimenda judicial, através da fixação do dano moral e da retirada da informação da página mantida pelo Conselho-Réu na Internet, devendo a indenização por dano moral ser fixada em patamares razoáveis, de modo a aquilatar a ofensa efetivamente realizada, não podendo ser estabelecida em valor tão elevado que importe em enriquecimento sem causa, nem tão baixo que o ofensor esteja incentivado a reincidir em sua conduta. II — Reza o art. 5º, V, da *Lex Magna* que 'é assegurado o direito de resposta, proporcional do agravo, além de indenização por dano material, moral ou à imagem', dispondo, igualmente, seu inciso X, que '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'. III — Não se verificando qualquer ilegalidade e não havendo provas que ratifiquem as matérias lançadas no jornal, irretocável a r. sentença ora atacada. IV — O direito à indenização surge quando a publicação transborda do simples objetivo de informação, atingindo a honra e a imagem dos indivíduos. V — Sentença mantida. VI — Remessa necessária e apelação a que se nega provimento" (TRF, 2ª Região, Apelação Cível 1999.51.01.000353-2, rel. Fernando Marques, publ. 28-10-2008).

Notamos aqui a ofensa à honra em página hospedada na internet, e a sentença em corolário com os princípios jurídicos, apesar de que nada data, não havia previsão legal, assim os tribunais já vinham se adaptando aos novos aspectos adquiridos com o advento da informatização.

Podemos observar na próxima jurisprudência, a incisão de uma rede social, site de relacionamento, e a responsabilização objetiva do servidor responsável por armazenar a informação:

> "*Ação de indenização. Dano moral. Orkut. Rede social. Sítio de relacionamento. Internet. Provedor de serviços de informações. Responsabilidade por fato do serviço. Direito do consumidor. Responsabilidade objetiva. Usuário vítima do evento. Ofensas de cunho moral. Expressão 'fazendo a fila andar'. Quantum.* Os provedores de acesso são aqueles que possibilitam ao usuário o acesso à Internet e a

> armazenagem de conteúdo e aplicações que dão vida ao meio virtual. Os provedores de serviços ou informações alimentam a rede com dados (conteúdo e aplicações que tornam a própria Internet útil e interessante) que podem ser armazenados em provedores de acesso. A relação entre os provedores e usuários da Internet é regida pelas normas do Código de Defesa do Consumidor. Por consumidor conceitua-se 'toda pessoa física ou jurídica que adquire ou utiliza produtos ou serviços como destinatário final', abrangendo os usuários da Internet que se utilizam das redes sociais. Os provedores se enquadram como fornecedores de serviços descritos no art. 3º do CDC, visto que são pessoas jurídicas que desenvolvem as atividades de criação, transformação, distribuição e comercialização de serviços de informação telemática a ser utilizada no meio virtual. A teor do art. 17 do CDC, quanto à responsabilidade por fato do serviço, equiparam-se aos consumidores todas as vítimas do evento, qual seja, a ofensa realizada por meio da rede social *Orkut*, não sendo sequer imprescindível que o ofendido seja usuário dos serviços do provedor de informações. A expressão 'fazendo a fila andar', aposta por usuário inidôneo na denominação do perfil pessoal da usuária, atinge a sua honra subjetiva. A expressão 'fazer a fila andar', no jargão popular, significa sucessão de parceiros amorosos, denotando promiscuidade por meio de relacionamento sexual não monogâmico, ou seja, com muitos parceiros diferentes. Fica ao arbítrio do magistrado a fixação do *pretium doloris*, devendo, contudo, ser observados parâmetros razoáveis para que seja atendido tanto o caráter punitivo da parte que deu causa, bem como o sofrimento psíquico e moral suportado pela vítima. Apelo parcialmente provido. V.V." (TJMG, Recurso 1.0145.08.471404-0/001(1), rel. Cabral da Silva, j. 3-8-2010).

Diante das ofensas de cunho moral, atingindo a honra subjetiva da vitima, se estabeleceu um vinculo com o provedor responsável pelo armazenamento do conteúdo, sendo o mesmo responsabilizado a fazer a retirada do conteúdo ofensivo.

3.5.2 Cyberbullying

As redes sociais são meros provedores de conteúdo, contudo seria errado afirmamos que não exista responsabilidades e deveres no ambiente das redes sociais. Diante de tal problemática é essencial aos provedores a identificação de indivíduos que praticam atos ilícitos dentro do seu sistema, afastando a responsabilização de terceiros, dessa forma Pinheiro nos ensina que:

> De fato, a única forma de se manter isento nessa relação é por meio da guarda dos registros de acesso do usuário de seus serviços. Isso, em regra, tem isentado os provedores de conteúdo da responsabilidade por ato ilícito. No tocante aos incidentes de *cyberbullying*, por envolver em sua maioria menores de idade, é fundamental agir rápido para retirada do

> conteúdo ofensivo e vexatório do ar. E os responsáveis legais respondem pela má conduta, pela indenização da vítima.(PINHEIRO,2013, p. 421)

Já temos algumas decisões de tribunais caracterizando o Cyberbullying, uma intimidação no ambiente virtual que pode gerar sérios danos a vitima, que geralmente é bombardeada pelo o individuo atrás do seu dispositivo informático, seja através de uma rede social, site especifico. Podendo agir em grupo ou individualmente.

Vejamos oque disciplina a jurisprudência acerca do tema:

> APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS. A INTERPOSIÇÃO DE RECURSO SEM PREPARO NÃO IMPORTA EM DESERÇÃO QUANDO O PLEITO DE CONCESSÃO DO BENEFÍCIO DA AJG FORMULADO NA RESPOSTA NÃO FOI APRECIADO PELO JUÍZO SINGULAR.
>
> A falta de recolhimento do preparo não autoriza o decreto de deserção do apelo, sem que antes o Tribunal aprecie o requerimento de concessão da gratuidade judiciária, sobretudo quando a questão é suscitada no próprio apelo, como no caso. Aplicação da regra inscrita no § 1º do artigo 515 do CPC. BENEFÍCIO DA ASSISTÊNCIA JUDICIÁRIA GRATUITA. LEI Nº. 1.060/50. PRESUNÇÃO DE NECESSIDADE. Legítimo a parte requerer o benefício da gratuidade na contestação, com esteio no art. 4º da Lei nº. 1.060/50, que se harmoniza com o art. 5º, inciso LXXIV, da Constituição Federal. Condição social e financeira dos réus, ora apelantes, compatível com o benefício da AJG. RESPONSABILIDADE OBJETIVA DOS PAIS PELOS DANOS CAUSADOS PELOS FILHOS MENORES. ART. 932, INC. I, C/C 933, AMBOS DO CÓDIGO CIVIL. CYBERBULLYING. CRIAÇÃO DE COMUNIDADE NO "ORKUT". CONTEÚDO OFENSIVO À HONRA E À IMAGEM DA AUTORA. VIOLAÇÃO A DIREITOS DA PERSONALIDADE. ILÍCITO CONFIGURADO. DEVER DE INDENIZAR CARACTERIZADO. DANOS MORAIS IN RE IPSA. Criação de comunidade no "Orkut" pela ré, menor impúbere, na qual passou a veicular comentários depreciativos e ofensivos a colega de turma de colégio. Conteúdo ofensivo à honra e imagem da autora. Situação... concreta em que verificados o ato ilícito praticado pela menor corré (divulgação de conteúdo ofensivo à imagem-atributo da autora na internet), o dano (violação a direitos da personalidade) e o nexo causal entre a conduta e o dano (pois admitida pela ré a confecção e propagação na internet do material depreciativo), presentes estão os elementos que tornam certo o dever de indenizar (art. 927, CC). Os genitores respondem de forma objetiva, na seara cível, pelos atos ilícitos praticados pelos filhos menores. Responsabilidade que deriva da conjugação da menoridade do filho e da circunstância fática desse se achar sob o pátrio poder dos pais, a quem incumbe zelar pela boa educação da prole. Dano "in re ipsa", dispensando a prova do efetivo prejuízo. ARBITRAMENTO DO "QUANTUM" INDENIZATÓRIO. VALOR REDUZIDO. Montante da indenização pelo dano moral reduzido em atenção aos critérios de proporcionalidade e razoabilidade, bem assim às

> peculiaridades do caso concreto e parâmetro adotado por Órgãos Fracionários deste Tribunal em situações similares. APELO PROVIDO EM PARTE. (Apelação Cível Nº 70042636613, Nona Câmara Cível, Tribunal de Justiça do RS, Relator: Miguel Ângelo da Silva, Julgado em 27/05/2015).

No relato exposto a produção de uma comunidade em rede social ou de relacionamento com o objetivo de denegrir a imagem e a honra da ofendida. Nota-se a responsabilização dos genitores pela ação da prole que não possui maioridade.

3.5.3 Pedofilia

Após o advento da Lei n. 11.829/2008 que alterou a redação do Estatuto da Criança e do Adolescente, passando a criminalizar o armazenamento de conteúdo envolvendo menores, senda a sua pena estipulada de três a seis anos de reclusão e multa. Assim sendo, o individuo que armazena ou produz cenas de sexo explicito ou pornográficos envolvendo crianças está incorrendo no crime de pedofilia, assim sujeitando-se a pena do mesmo.

No que se refere aos crimes relacionados à pedofilia, “a internet, e seu uso como mídia de massa, transformou o mercado da pornografia infantil, aumentando seu público e, consequentemente, transformando também o seu significado.” (LANDINI, 2007, p. 171-172). Os mecanismos gerados pela informática são amplamente utilizados para difundir registros que contenham cenas de sexo explícito ou pornográficas envolvendo crianças e adolescentes, favorecendo a prática de crimes dessa natureza.

Conforme preceitua Kalb, “Alguns dos motivos para que o abuso sexual e a publicação de fotos e vídeos pornográficos aumentasse significativamente foram a “confidencialidade de usuários de salas de bate-papo; hospedagem de *sites* nos mais variados países, dificultando a identificação e a prisão dos responsáveis; pouca legislação específica para crimes de informática, etc. [...].” (2008, p. 121)

Vejamos jurisprudência acerca do tema explanado:

> “Penal. Publicação de fotografias, contendo cenas de sexo explícito e pornográficas, envolvendo crianças e adolescentes. Art. 241 da Lei n. 8.069/90 (Estatuto da Criança e do Adolescente — ECA), em sua redação original, c/c art. 71 do Código Penal. Tipicidade da conduta, espelhada em duas práticas distintas, descritas na denúncia, a despeito da alteração introduzida, posteriormente, pela Lei n. 10.764/2003. Precedentes. Autoria e materialidade comprovadas. Dosimetria atenta ao disposto no art. 59 do Código Penal. Continuidade delitiva caracterizada. Sentença mantida. I — Réu denunciado, como incurso na pena do art. 241 da Lei n. 8.069/90 (Estatuto da Criança e do Adolescente — ECA) — em sua redação original — c/c art. 71 do Código Penal, por ter (1) publicado fotos de pornografia infantil em ‘grupo de discussão’ do ‘Messenger Groups’, denominado ‘Thamansplace’, e (2) enviado um ‘e-mail’ para outra pessoa, contendo ‘links’ de acesso à pornografia infantil. II — A conduta imputada ao acusado, caracterizada por publicidade via Internet, espelhada nas duas práticas descritas na denúncia, é típica, diante da original redação do art. 241 da Lei n. 8.069/90, a despeito da alteração introduzida, posteriormente, pela Lei n. 10.764/2003, podendo ser autor do aludido crime qualquer pessoa, e não somente o proprietário de ‘site’ ou o provedor (Precedentes do STJ e do TRF/1ª Região: HC 2003.01.00.029307-6/MT, rel. Des. Federal Olindo Menezes, 3ª Turma do TRF/1ª Região, unânime, j. 21-10-2003, DJU de 31-10-2003, p. 36; HC 76.689/PB, rel. Min. Sepúlveda Pertence, 1ª Turma do STF, unânime, DJU 6-11-1998, p. 3; HC 84.561/PR, rel. Min. Joaquim Barbosa, 2ª Turma do STF, unânime, DJU 26-11-2004, p. 31). III — Autoria e materialidade delitivas comprovadas, à saciedade, tornando inafastável a condenação imposta, pela prática de atos de verdadeira bestialidade humana, como se depreende das chocantes imagens constantes das fotografias colacionadas aos autos. IV — Dosimetria da pena que atende, criteriosamente, as circunstâncias judiciais do art. 59 do Código Penal, fazendo com que a pena-base fosse fixada em quantidade necessária e suficiente para a reprovação e prevenção do crime. V — Continuidade delitiva caracterizada pela prática de duas condutas absolutamente distintas, de forma continuada e materialmente comprovada, a ensejar o aumento da pena base, pela aplicação da fração mínima (um sexto), prevista no art. 71 do Código Penal. VI — Apelação improvida” (TRF01, ACR 2003.36.00.014182-3/MT, rel. Assusete Magalhaes, publ. 4-12-2009).

Desse modo, verificamos como atuam esses indivíduos que utilizam de salas de bate-papo, redes sociais, no caso em tela o e-mail utilizado para o compartilhamento de links referentes a pornografia infantil, tendo sua materialidade comprovada para a aplicação da pena cabível por tal ato nefasto.

3.5.2 Pornô de Vingança (*Revenge porn*)

Aumentando cada vez mais a sua ocorrência, o Pornô de Vingança é uma nova modalidade de intimidação com a divulgação ou compartilhamento de fotos, vídeos íntimos na rede mundial de internet, com o objetivo de causar danos a vitima, causados pela a exposição, que em sua maioria das vezes é do sexo feminino.

Com o objetivo de solucionar a problemática cada vez mais crescente, eis que surge o projeto de Lei n. 5.555/2013, com o intuito de inserir na Lei Maria da Penha (Lei 11.340/2006) normas que tipifiquem a pornografia da vingança como crime. Bastante óbvio, pois a violência psíquica sofrida é gigantesca, com um dano gerado sem precedentes, já que, uma vez na internet, não se tem mais o controle, ficando a vitima sujeita a julgamento de toda a sociedade, acarretando em vários problemas.

As modificações acontecem nos artigos 3°, 7° e 22, da Lei Maria da Penha, alterando o artigo terceiro sendo incluso no rol de direitos assistidos às mulheres, o direito a comunicação. No artigo 7° a modificação prevista cria o inciso VI, onde se faz referência à violação da intimidade da mulher nos meios de disseminação de informação, sem a sua anuência, vejamos a redação do artigo sétimo:

> *Art. 7º,VI* – violação da sua intimidade, entendida como a divulgação por meio da internet, ou em qualquer outro meio de propagação da informação, sem o seu expresso consentimento, de imagens, informações, dados pessoais, vídeos, áudios, montagens ou fotocomposições da mulher, obtidos no âmbito de relações domésticas, de coabitação ou de hospitalidade.

No artigo 22, §5º encontramos as ações que podem ser tomadas pelo o magistrado quando configurada a vingança pornô, destarte leciona de tal maneira:

> *§5º Na hipótese de aplicação do inciso VI do artigo 7º desta Lei, o juiz ordenará ao provedor de serviço de e-mail, perfil de rede social, de hospedagem de site, de hospedagem de blog, de telefonia móvel ou qualquer outro prestador do serviço de propagação de informação, que remova, no prazo de 24 (vinte e quatro) horas, o conteúdo que viola a intimidade da mulher.*

Diante dessa análise, pode notar que o referido projeto de lei, se assim concretizado em norma efetiva dar o devido poder ao magistrado para que aja com urgência na retirada do conteúdo lesivo da internet, no intuito de evitar a propagação do ato nocivo.

CONSIDERAÇÕES FINAIS

O desenvolvimento do presente trabalho possibilitou uma análise da nova sistemática penal e como o Direito Digital e suas possibilidades modificam essa matéria. Com a evolução em constância da sociedade nosso legislativo tem que ficar cada vez mais atento para a elaboração e aprovação de novos projetos de leis com a temática digital, já que a mesma está presente no nosso dia a dia cada vez mais.

De maneira geral nota-se a dificuldade do legislativo brasileiro na aprovação de novas leis que ensejem no tratamento do direito digital, apesar da aprovação das leis n. 12.735/2012 e a n. 12737/2012 criminalizarem algumas condutas que antes estavam com lacunas, ainda a um caminho a percorrer. A punição de invasão a dispositivos eletrônicos, a criação de delegacias específicas para a investigação de crimes cibernéticos por mais que esteja a cargo da administração pública, foram grandes inovações no cenário brasileiro.

Existem várias condutas criminosas que os indivíduos praticam por estarem atrás de um dispositivo informático se sentem no direito de pratica-las livremente, por exemplo, temos o Pornô de Vingança, sem legislação própria que acaba denegrindo a imagem das pessoas perante a sociedade praticamente de maneira irreversível.

Dada à importância do tema, ficou claro com a pesquisa que a incisão de alguns crimes como de menor potencial ofensivo na lei n. 12.737, sendo tratado pelo o Juizado Especial Criminal, gera um sentimento de mínima punibilidade. Diante o exposto o trabalho, vemos com clareza a naturalidade com que esses delitos acontecem na internet, e consequentemente como preveni-los de algumas maneiras e no caso de efetivação como deve ser levado o delito ao judiciário para responsabilização do individuo.

Nesse sentido, chegamos a conclusão de que diante das novações cotidianas abordadas pelo o Direito Digital e consequentemente o Penal, o legislativo deve melhorar sua atuação na aprovação de leis combatentes das diversas praticas

delituosas, assim como o judiciário deve manter-se constantemente atualizado para que dê sua contribuição a sociedade nos casos que não existem previsão legal.

5. REFERÊNCIAS

BARROS, Thiago. **INTERNET COMPLETA 44 ANOS**: RELEMBRE A HISTÓRIA DA WEB. Disponível em:http://www.techtudo.com.br/artigos/noticia/2013/04/internet-completa-44-anos-relembre-historia-da-web.html. Acesso em: 16 nov. 2016.

BATISTA, Ricardo Córdoba. **O QUE É PHISHING**? Disponível em: http://www.mycybersecurity.com.br/o-que-e-phishing? . Acesso em: 01 nov. 2016.

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 07 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União. Seção 1. 03/12/12. p.1. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm >. Acesso em 15 de outubro de 2016

BRASIL. Supremo Tribunal Federal. Habeas Corpus nº. 76689. Relator: **Sepúlveda Pertence**, julgada em 21/09/1998, Primeira Turma, Data de Publicação: DJ 06-11-1998 PP-00003 EMENT VOL-01930-01 PP-00070. Disponível em: < http:// stf.jusbrasil.com.br/jurisprudencia/740355/habeas-corpus-hc-76689-pb>. Acesso em 15 de outubro de 2016.

CAVALCANTE, Karla Karênina Andrade Carlos . **Ação penal pública condicionada e incondicionada**. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=4739>. Acesso em: 11 nov. 2016.

CAVALCANTE, Marcio André Lopes. **Primeiros comentários à Lei n.° 12.737/2012, que tipifica a invasão de dispositivo informático**. Disponível em: <http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html>. Acesso em: 18 nov. 2016.

COM INFORMAÇÕES DO FANTÁSTICO, Do G1. **Suspeitos do roubo das fotos de Carolina Dieckmann são descobertos**. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html>. Acesso em: 23 nov. 2016.

DUMAS, Véronique. **A origem da internet**: A história da rede de computadores criada na Guerra Fria que deu início à Terceira Revolução Industrial. Disponívelem:<http://www2.uol.com.br/historiaviva/reportagens/o_nascimento_da_internet.html>. Acesso em: 01 nov. 2016.

FILHO, José Carlos de Araújo Almeida. **Processo eletrônico e teoria geral do processo eletrônico; a informatização judicial no Brasil**. 4◦ edição. Rio de janeiro: editora Forense, 2012

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social.** 6◦ edição. São Paulo: Editora Atlas, 2008.

Krone, T., 2005. **High Tech Crime Brief**. Australian Institute of Criminology. Canberra, Australia. ISSN 1832-3413. 2005.

LANDINI, Tatiana Savoia. **A pornografia infantil na internet: uma perspectiva sociológica**. In: LIBÓRIO, Renata Maria Coimbra; SOUSA, Sônia M. Gomes de

(Org.). **A exploração sexual de crianças e adolescentes no Brasil: reflexões teóricas, relatos de pesquisas e intervenções psicossociais.** 2ª. ed. São Paulo: Caso do Psicólogo Livraria e Editora Ltda., 2007, Parte. I, p. 165-182.

SYMANTEC, Norton. **O que é crime cibernético?** . Disponível em: <https://br.norton.com/cybercrime-definition>. Acesso em: 01 nov. 2016.

PINHEIRO, Patrícia Peck. **Direito digital.** 5° edição. São Paulo: Editora Saraiva 2013.

PIMENTA, Marcelo Vicente de Alkmin. **Direito Constitucional em perguntas e respostas**. Edição única. Belo Horizonte: Editora Del Rei, 2007

TOLEDO, Francisco de Assis. **PRINCIPIOS BÁSICOS DO DIREITO PENAL**. 5. ed. São Paulo: Saraiva, 1994. p. 21.

XAVIER, Andressa. **O que é Spyware**. São Paulo. TecMundo**.** [2008]. Disponível em: <http://www.tecmundo.com.br/spyware/29-o-que-e-spyware-.htm>; Acesso em: 13 de outubro de 2016 .

HTTPS://PT.WIKIPEDIA.ORG/WIKI/COMPUTADOR