UNIFACIG - CENTRO UNIVERSITÁRIO

A RESPOSTA ESTATAL QUANTO AOS CRIMES CIBERNÉTICOS: UMA ANÁLISE DIRECIONADA ÀS LEIS Nº 12.735/2012 E 12.737/2012

Natália Alves Dornelas

MANHUAÇU / MG
2019

NATÁLIA ALVES DORNELAS

A RESPOSTA ESTATAL QUANTO AOS CRIMES CIBERNÉTICOS: UMA ANÁLISE DIRECIONADA ÀS LEIS 12.735/2012 E 12.737/2012

Projeto de Pesquisa apresentado no Curso de Superior de Direito da UniFacig - Centro Universitário, como requisito parcial à aprovação na disciplina de Projeto de Pesquisa em Direito.

Área de concentração: Direito Penal

Orientador: Patrick Leonardo Carvalho dos Santos

NATÁLIA ALVES DORNELAS

A RESPOSTA ESTATAL QUANTO AOS CRIMES CIBERNÉTICOS: UMA ANÁLISE DIRECIONADA ÀS LEIS Nº 12.735/2012 E 12.737/2012

Trabalho de Conclusão de Curso apresentado no Curso Superior de Direito do Centro Universitário UNIFACIG, como requisito parcial à obtenção do título de Bacharel em Direito.

Área de Concentração: Direito Penal
Orientador: Patrick Leonardo Carvalho dos Santos

Banca Examinadora

Data de Aprovação: ____/____/_____

_____
Prof.

_____

Prof.

_____

Prof.

Manhuaçu

2019

RESUMO

O presente trabalho tem como objetivo examinar o histórico dos cibercrimes e seu surgimento e da criação de leis que se propõem a criminalizar delitos informáticos. E também demonstrar que o Poder Legislativo é tardio quanto à evolução dos cibercrimes e sua tipificação, exemplificando alguns crimes cibernéticos, relatando situações tipificadas e ainda não abrangidas pelo Código Penal.

Diante das questões atuais, onde milhões de pessoas possuem acesso à internet no Brasil, muitos indivíduos são vítimas de crimes cibernéticos, o presente trabalho visa estudar esses crimes e a atuação do Poder Legislativo quanto à criação de leis que acompanhem o progresso da sociedade, e consequentemente, a evolução dos crimes. O estudo se voltará principalmente as legislações mais recentes sobre o tema, a Lei nº 12.735/2012 e a Lei nº 12.737/2012 que tratam principalmente da invasão de dispositivos e da exposição de fotos e vídeos íntimos, crimes recorrentes no atual contexto da internet. Nesse contexto, a questão problema que orienta a pesquisa é analisar a necessidade ou não de leis específicas para os crimes virtuais. Assim, considerando o avanço tecnológico da sociedade, o surgimento e popularização da internet, seria possível o Estado controlar a criminalidade nos ambientes virtuais. No tocante ao procedimento metodológico, utilizou-se pesquisa bibliográfica com a finalidade de proporcionar melhores e mais precisas informações sobre o tema. E ainda analisará qual o grau de dano à vítima até que as providências estatais sejam tomadas. Serão traçadas o conceito básico de crime cibernético, as situações em que tal delito pode ser praticado no contexto das Leis nº 12.735/2012 e 12.737/2012 e propostas legislativas para tipificação desses crimes.

Palavras-chave: Crimes cibernéticos; Internet; Crimes digitais; Legislação; Criminosos.

ABSTRACT

This paper aims to examine the history of cybercrime and its emergence and the creation of laws that aim to criminalize computer crimes. And also demonstrate that the Legislative Power is late in the evolution of cybercrime and its typification, exemplifying some cyber crimes, reporting situations typified and not yet covered by the Penal Code.

Given the current issues, where millions of people have access to the Internet in Brazil, many individuals are victims of cyber crimes, the present work aims to study these crimes and the Legislative Power regarding the creation of laws that accompany the progress of society, and consequently, the evolution of the crimes. The study will focus mainly on the most recent legislation on the subject, Law No. 12.737 / 2012 and Law No. 13.718 / 2018 that deal mainly with the invasion of devices and the exposure of intimate photos and videos, recurring crimes in the current context of the Internet. In this context, the problem that guides the research is to analyze the need or not of specific laws for cybercrime.

Thus, considering the technological advancement of society, the emergence and popularization of the Internet, it would be possible for the state to control crime in virtual environments. Regarding the methodological procedure, a bibliographic research was used in order to provide better and more accurate information on the subject. It will also analyze the degree of damage to the victim until state action is taken. The basic concept of cyber crime will be traced, the situations in which such crime can be committed in the context of Laws 12.737 / 2012 and 13.718 / 2018 and legislative proposals to typify these crimes.

KEYWORDS: Cybercrime; Internet; Digital crimes; Legislation; Criminals.

UNIFACIG
CENTRO UNIVERSITÁRIO

SUMÁRIO

1 INTRODUÇÃO

Com a pós-modernidade surgiram vários riscos, sendo que a internet é um deles. Apesar da sua facilidade como meio de informação e manter a sociedade informada de tudo que acontece no cotidiano, contudo trouxe vários desafios a sociedade que necessita de os operadores do direito encarar.

Mas é evidente com a introdução da internet proporcionou vantagens imensuráveis para as pessoas, facilitou em vários quesitos, como forma de meio de comunicação, de realização de compras virtuais, acesso a contas bancárias, para estudos acadêmicos, acesso a redes sociais de relacionamentos como ponto de encontros e também empresas que utilizam esse meio como um caminho para melhorar seus lucros e vendas e dentre outras várias formas de uso da internet.

Entretanto, com todas as vantagens que o uso da internet proporcionou as pessoas, trouxeram também várias desvantagens em que a facilidade de acesso ao sistema de informação fez com que surgisse os crimes cibernéticos, em que são aqueles crimes contra o sistema virtual que vem crescendo bastante com o passar do tempo e com o crescimento do conhecimento da sociedade com o mundo virtual.

Atualmente, é inimaginável um mundo sem a internet, a conexão constante com o resto do mundo globalizado faz parte do cotidiano da sociedade, o *e-commerce* – comércio totalmente via internet – torna-se cada vez mais comum, transformando as relações jurídicas e assim, modificando a forma em que a própria lei rege e tipifica esses atos.

Porém, com o passar dos anos, a internet tornou-se “terra de ninguém”, como é o dito popular, os crimes *on-line* são cada vez mais comuns e os usuários estão expostos a diversos tipos de ameaças, sejam eles vírus, ou até mesmo a conduta inadequada de outros usuários. Além disso, os crimes cibernéticos se subdividem entre crimes cibernéticos abertos e crimes exclusivamente cibernéticos. A questão é que diversas vezes alguém se vê prejudicado, sendo vítima de um suposto “crime” que não está tipificado no Código Penal.

Assim, com o presente trabalho será estudado o conceito de crimes cibernéticos com o fim de entender como funciona na prática os delitos praticados em face do sistema

de informação e consequentemente a classificação desses crimes conforme base doutrinária.

Ainda não existe uma real definição para tais crimes, porém é para ser considerado crime cibernético,deve ter sido praticado contra sistemas de informática e comunicação ou com o auxílio do mesmo. Ou seja, são os crimes praticados contra o sistema de informação e seus acessórios ou sendo o computador o meio para a prática de outro delito. Sendo o computator o meio de acessar a rede de internet.

Dada a inexistência de uma norma penal capaz de tipificar essas condutas, os criminosos só recebem sanções cíveis e não recebem qualquer repressão na esfera criminal, trazendo o sentimento de impunidade na sociedade. Esses comportamentos recebem diversos nomes, sendo todos sinônimos referentes a condutas ilegais – ou que deveriam ser ilegais – cometidas na internet: Crimes Cibernéticos, Crimes Digitais, Crimes informáticos e Cibercrimes. Surge um ambiente com plenas condições de cometimento de crimes sem qualquer tipo de punição:

Deve-se ressaltar que a criatividade do ser humano voltada para a práticas de atos prejudiciais é extensa, principalmente mesmo pela internet, local em que se tem o benefício do anonimato. Alguns exemplos de delitos praticados por meio eletrônico são: acesso não autorizado, ameaças, discriminação racial, social ou de gênero, modificação de dados, *bullying*, terrorismo e até mesmo crimes sexuais.

Os casos de exposição de imagens íntimas – seja de uma figura pública ou uma pessoa comum – tornaram-se comuns e até mesmo conveniente para certos indivíduos, que fazem uso dessas fotos ou vídeos para ameaçar a vítima. Essa problemática foi tema de debates jurídicos por muito tempo na década passada, entretanto, somente com o caso de Carolina Dieckmann, vítima de *hackers* que quebraram o sistema de proteção de seu computador, obtendo acesso ao e-mail da atriz e expondo diversas fotografias íntimas. Essas fotografias foram lamentavelmente compartilhadas em massa, circulando desde as redes sociais *facebook* e *twitter* até sites de pornografia.

Esse infeliz episódio deu origem a Lei Carolina Dieckmann, haja vista que os criminosos foram localizados pela Polícia Federal, presos com os instrumentos do crime – nesse caso, computadores e celulares – e curiosamente foram indiciados pelos crimes de furto extorsão qualificada e difamação não havendo tipo penal para o crime efetivamente cometido, o debate acerca dos crimes cibernéticos se levantou.

Na tentativa de tipificar tal conduta, o Poder Legislativo, através da Lei nº 12.737/12 – também chamada de Lei Carolina Dieckmann – tornou crime a invasão de dispositivo informático, acrescentando o artigo 154-A no Código Penal.

Apesar de criar um tipo penal inexistente, somente em 2018, com a Lei nº 13.718, sobreveio a modificação do Código Penal que tratasse diretamente dos crimes sexuais relacionados à internet e a exposição de imagens ou vídeos íntimos, propriamente ditos, adicionando o artigo 218-C Lei Penal.

Sendo assim, atualmente tornou-se crime o compartilhamento, de fotografia, vídeo ou outro registro que contenha cena de sexo, ou da intimidade da vítima, sem a autorização desta. Esse fato típico abrange também a divulgação de cenas de estupro e pornografia infantil, haja vista que a relação com menor de 14 anos, independente do consentimento, sendo tipificado como estupro de vulnerável.

E ainda, a monografia se dividirá em três capítulos, sendo que o primeiro ‘‘Dos Crimes Cibernéticos’’, irá tratar acerca do conceito de crime e de crimes cibernéticos, apresentando seus aspectos gerais e tipos de classificações doutrinárias.

O segundo capítulo ‘‘Princípios Norteadores’’, tem como objetivo esclarecer os princípios basilares no que se refere a aplicação do caso concreto nos delitos contra o sistema de informação.

E por fim, o terceiro capítulo ´‘Análise da Legislação Brasileira sobre os Crimes Cibernéticos’’ abordará sobre as leis específicas existentes no ordenamento jurídico brasileiro em relação a proteção contra os crimes cibernéticos e ainda o posicionamento jurisprudencial e doutrinário sobre a necessidade ou não da existentes de leis específicas sobre o tema frente ao Código Penal.

Enfim, a pesquisa buscará a análise dos crimes cibernéticos em geral, a história por trás da criação de leis que tipificam essas condutas, quais condutas são tipificados como cibercrimes e a competência para julgamento e processamento desses crimes.

2 DOS CRIMES CIBERNETICOS

2.1 OS CRIMES

Primeiramente é importante fazer uma abordagem jurídica dos crimes em geral, para depois abordar os crimes cibernéticos; e um conceito que é senso comum quando se trata de crimes é de que é um ato ou ação típica, antijurídica e culpável, que a sociedade julga indesejáveis em âmbito coletivo.

Greco (2014) define como tipicidade a conduta física que tem características específicas de um modelo abstrato de tipo penal já definido em lei. Se tratando de ilicitude, ele caracteriza pela proibição de uma determinada ação, sem que haja exceção normativa. Já a culpabilidade, tem relação ao *animus* do agente na conduta seja ativa ou omissiva, ou seja, a vontade de tal ato.

O artigo 163 do Código Penal é totalmente aplicável ao dano informático, e Flávio Augusto Maretti Sgrilli Siqueira e o doutrinado Tulio Vianna, entendem:

> O crime de dano previsto no art.163 do Código Penal Brasileiro é perfeitamente aplicável à tutela dos dados informáticos, sendo completamente prescindível a criação e um novo tipo penal para tal fim. Trata-se de interpretação extensiva da palavra “coisa”, elemento objetivo do tipo penal.

Definido o crime *lato sensu* passa-se à abordagem aos crimes cibernéticos. Machado (2013) explica que somente a utilização do agente em computadores para executar um delito, por si só, não configuraria um crime informático, caso o direito afetado não seja informação automatizada. No entanto, muitos autores acabaram denominando como crimes cibernéticos infrações penais em que o computador serviu apenas como instrumento utilizado na prática do delito; por mais que essa denominação seja imprópria, ela se tornou bastante popular e não tem mais como ignorá-la. Então, criou-se uma classificação dos crimes cibernéticos em impróprios, próprios, mistos e mediatos ou indiretos.

Aquelas condutas, que atingem um bem jurídico comum, e utilizam dos sistemas informáticos para a realização do crime, mas que foi apenas um instrumento, não sendo ferida a inviolabilidade dos dados, se classificam como crimes cibernéticos impróprios. Crimes cibernéticos impróprios praticados contra o patrimônio não mais difíceis de reconhecer, por reconhecer na informação um bem imaterial, insuscetível

de apreensão como objeto. Já as condutas que se verifica a violação das informações, classifica-se como próprios. Os crimes mistos, são aqueles mais complexos, que se verifica mais de um tipo penal, que além da proteção aos dados, a norma visa ainda a tutela de bem jurídico diverso ao informacional. Por fim, temos os crimes mediatos, que são aquelas que são cometidos como meio para outro principal; um ótimo exemplo é a invasão de um site de banco para o cometimento do crime patrimonial.

O surgimento de crimes virtuais vem desde a década de 1960, onde foram denunciados em jornais os primeiros casos da prática delituosa por meio do uso de computadores e sistemas, sendo somente na década seguinte que começou a estudar sistematicamente essa matéria. (FURLANETO, NETO, 2013).

Segundo Augusto Rossini:

> [...] o conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade. (ROSSINI, 2004, p. 56).

Segundo Mário Furlaneto Neto e José Augusto Chaves Guimarães:

> [...] observa-se que, como fator criminógeno, cabe reconhecer que a informática permite não só o cometimento de novos delitos, como potencializa outros tradicionais (estelionato, por exemplo). Há, assim, crimes cometidos com o computador (The computer as tool of a crime) e os cometidos contra o computador, isto é, contra as informações e programas nele contidos (The computer as the object of a crime). (FURLANETO, NETO, 2013, p. 146).

Ivette Senise Ferreira "define crime de informática como sendo toda ação típica, antijurídica e culpável, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão".

Várias condutas praticadas pela internet tipificam crimes que já são previstos pela legislação, e a principal delas é a pornografia infanto-juvenil, que está previsto no Estatuto da criança e do adolescente, em seu artigo 241. E de acordo com Alexandre Daoun ele é suficiente e já estabelece uma sanção bastante dura.

2.2 ASPECTOS GERAIS DOS CRIMES CIBERNETICOS

Inicialmente, pretende-se entender o contexto de surgimento dos crimes virtuais, para tanto, Barreto Júnior (2007) esclarecem que, com o advento da internet, da sociedade da informação, uma nova modalidade de crimes do espaço virtual vem ganhando espaço, esses crimes são cometidos através e-mails, web sites e até mesmo em chats de relacionamentos.

Com a entrada da internet no mundo a tecnologia sofreu um enorme avanço significativo. Hoje em dia a internet é o maior meio de comunicação entre as pessoas, em que conversar, realizar comprar e até mesmo namoros vem acontecendo pela internet.

Contudo, com toda essa facilidade de comunicação via virtual os crimes nessa face estão crescendo a cada dia mais e repletos de armadilhas. Desta forma, surge os crimes chamados de crimes digitais ou crimes virtuais.

A conceituação de crimes cibernéticos é algo um pouco dificultoso, tendo em vista várias formas de tecnologias crescendo a cada dia.

Dessa forma, Carneiro dispõe sobre o conceito de Crimes Cibernéticos:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. (CARNEIRO, 2012, p. 156).

No mesmo sentido estabelece Cassanti:

> Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital. (CASSANTI, 2014, p. 3).

Salienta-se que apesar de vários conceitos de crimes cibernéticos existentes, é importante destacar que para que seja considerado crime cibernético a conduta realizada deve ser feita contra ou por meio de um computador, e na maioria das vezes a conduta é praticada por meio do uso de internet.

Percebe-se que os crimes cibernéticos são diferentes dos crimes tradicionais, pois os crimes virtuais são praticados contra os sistemas de informação ou utilizando o próprio sistema.

Uma definição um pouco mais complexa sobre crimes cibernéticos expõe Maia:

> Uma definição bem completa para o crime de informática é a que o caracteriza como uma conduta atentatória ao estado natural dos dados e recursos oferecido pelos sistemas de processamento de dados, e pela compilação, armazenamento, e transmissão dos dados. O crime de informática, portanto, é aquele procedimento que ataca os dados armazenados, compilados, transmissíveis, ou em transmissão. (MAIA, 2017, p. 31 MONGR).

Assim para que o crime virtual seja praticado necessita do uso do software e do hardware, assim, sendo a conduta antijurídica, tipifica nas normas jurídicas e culpável aplicada ou utilizada por meio de processamento eletrônico ou transmissão de dados já é suficiente para que seja considerado crime.

Conforme dito acima, são vários os conceitos estabelecidos pelos doutrinadores a respeito dos crimes cibernéticos, um pouco diferente dos autores acima estabelece Velloso sendo: todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou 26 fraudar (VELLOSO, 2015, P.43).

Percebe-se que neste caso, o dano seria contra a máquina virtual, ou seja, contra os dados contidos dentro do computador, como exemplos de danos quando o agente furta informações ou até mesmo apaga dados causando danos irreversíveis ao computador.

2.2.1CLASSIFICAÇÃO DE CRIMES CIBERNÉTICOS

Esgotando o estudo do conceito de crimes cibernéticos, cabe agora detalhar a classificação dos tipos de crimes informáticos existentes.

Uma das classificações se subdividem-se da seguinte forma: crimes caracterizados pela agressão ao meio informático, e pelo conteúdo da mensagem disponível em rede. Em todas essas modalidades, o bem ou meio informático deve aparecer como elemento típico ou determinante (ASCENSAO, 2002, p.256).

Essa classificação tem por finalidade de entender o agente da conduta criminosa, ou seja, a real intenção do agente na prática do delito. Com a classificação pode-se compreender se o agente que praticou o ato deseja atingir diretamente um determinado sistema de informação, ou se a invasão no sistema era somente um meio para prática de outro delito.

Em relação a essa classificação minucia Pinheiro:

> a) quando o computador é o alvo – p. Ex.: crime de invasão, contaminação por vírus, sabotagem do sistema, destruição ou modificação de conteúdo do banco de dados, furto de informação, furto de propriedade intelectual, vandalismo cibernético, acesso abusivo por funcionário, acesso abusivo por terceirizados, acesso abusivo por fora da empresa; b) quando computador é o instrumento para o crime – ex.: crime de fraude em conta corrente e/ou cartões de crédito, transferência de valores ou alterações de saldos e fraude de telecomunicações, divulgação ou exploração de pornografia; c) quando o computador é incidental para outro crime – ex.: crimes contra honra, jogo ilegal, lavagem de dinheiro, fraudes contábeis, registro de atividades do crime organizado; d) quando o crime está associado com computador – p. Ex.: pirataria de software, falsificações de programas, divulgação, utilização ou reprodução ilícita de dados e programas de comércio ilegal de equipamentos e programas. (PINHEIRO, 2013, P. 75).

No primeiro caso, pode-se perceber que o crime está mirado no computador, sendo este o alvo, o agente pratica o ato com o intuito de atacar os sistemas de informação. No segundo verifica-se o computador serve somente como ferramenta para prática de outro delito, neste caso abre a possibilidade da prática dos crimes tradicionais, por exemplos dos crimes definidos no Código Penal. No terceiro caso o crime virtual é incidental em relação a outro crime.

Outra classificação definida pela doutrina brasileira é em relação dos crimes cibernéticos serem próprios ou impróprios.

É fato que o crime virtual pode se apresentar de várias maneiras, assim como o crime tradicional, pode acontecer em qualquer lugar e a qualquer tempo, e ele se caracteriza com a conduta sendo informática, ou virtual. Dessa forma, o cibercrime se caracteriza de duas maneiras, a comum, que consiste no uso da informática apenas como um instrumento pelo qual o crime é praticado, sendo que este já está tipificado em lei; e a mista, que são aqueles em que a internet é de fundamental importância para que a condutada criminosa seja realizada (VIANNA; MACHADO, 2013).

Além disso, há o crime cibernético próprio, o qual se configura como aquele cuja conduta ilícita tem por objetivo prejudicar o sistema informático e corromper os dados da vítima, conduta esta que é praticada por hackers; e os crimes impróprios, onde a característica é atingir o patrimônio ou bem jurídico, e que usa a informática como ferramenta para executar o feito (VIANNA; MACHADO, 2013). Para essa complexa conceituação, serão utilizadas as concepções de Rossini:

> [...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança Informática, que tem por elementos a integridade, disponibilidade a confidencialidade. (ROSSINI, 2004, p. 110.)

Quanto ao conceito de crime próprio estabelece Viana:

> Nessa classificação os crimes próprios são aqueles que em que o sistema informático do sujeito passivo é o objeto e o meio do crime. “São aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados) (VIANA, 2003, p. 13).

Nota-se que nos crimes próprios o ato ilícito é praticamente com a finalidade de atingir o hardware ou software e só podem ser executados pelo computador e os seus periféricos, ou seja sem a informática o crime não acontecerá.

Em relação aos crimes impróprios Adeneele Garcia Carneiro classifica-os da seguinte forma:

> Afirma-se que os crimes digitais impróprios são aqueles realizados com o auxílio do computador, ou seja, este é meio/ instrumento para a concretização do crime, crime este cujo bem jurídico já é tutelado, ressaltando que o computador ou internet não seria o único meio em que pode ser realizado tal crime. (CARNEIRO, 2013, p. 5).

Neste tipo de classificação, o crime pode ser praticado de várias formas, em que pode ser realizado por meio da informática ou não, ou seja, a internet é utilizada como uma ferramenta para a pratica de outro ato ilícito.

Outra classificação dos crimes cibernéticos que a doutrina desenvolveu é a divisão em crimes puros, mistos e comuns.

No que tange aos crimes puros Marcos Aurélio Rodrigues Costa dispõe:

> Crimes cibernéticos puros podem ser definidos como "toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas (COSTA, 1997, p.6)

Nos crimes puros o agente criminoso tem a intenção de atingir diretamente o sistema de informação ou os dados de informação inseridas dentro do computador. Um exemplo dessa classificação são os hackers que tenham a finalidade de invadir os sistemas de informação na colheita de dados ou na finalidade de causas danos ao sistema virtual.

Outra classificação é no caso dos crimes mistos, além de se proteger a inviolabilidade de dados, a legislação também procura proteger bem jurídico de natureza diversa a exemplo do crime eleitoral da Lei nº 9504/1997, do artigo 72. (VIANA, 2013, p. 15).

Nos crimes mistos, percebe-se que mesmo concretizando o crime virtual a internet é somente um meio para efetivar outro tipo penal tipificado no Código Penal. E por último tem os crimes cibernéticos comuns que o acesso a internet é um instrumento para prática de outro delito.

O delito informático se funda em uma conduta considerada ilícita e típica, é irrelevante o modo com que é praticada, seja dolosamente ou com culpa, além disso, o crime pode ser cometido tanto por pessoas físicas quanto por pessoas jurídicas. O jurista ressalta que é não é necessária que a prática do delito seja fruto do uso da internet, basta que o dispositivo acesse o ciberespaço, ou os dispositivos alheios.

Seguindo na conceituação de cibercrime, Rosa (2005) determina que o crime virtual é uma conduta que desvirtua os dados que um certo sistema que processa os armazena ou dados. Esse delito tem como objetivo modificar, alterar ou até mesmo excluir os dados, prejudicando assim, as informações.

As compras e as vendas que exigem a identificação dos números de segurança dos cartões de crédito, dados referentes as contas bancárias, e até mesmo senhas de alguns mecanismos de segurança, propiciam o surgimento de novas modalidades dos crimes virtuais, atualmente, as compras *on-line* somam o montante de R$ 166,2 bi no Brasil (FORBES, 2018), é inegável que existem *hackers* preparados para invadir os dados dos compradores.

Ultrapassadas as conceituações, trataremos da exemplificação dos crimes virtuais, desde os crimes contra o patrimônio até os delitos que atingem a própria dignidade da vítima, como, por exemplo, os crimes sexuais e contra a honra.

Um popular exemplo de crime cibernético, é a criação e instalação de programas maliciosos no ciberespaço, estes *softwares* possuem a mesma

característica de um vírus biológico, multiplicando-se e se propagando entre os dispositivos. Esses vírus têm como propósito se instalar em computadores para danificar o desenvolvimento da máquina, ou seja, aquele computador infectado se torna vulnerável para que os criminosos por trás desse ataque furtem roubem dados, sejam senhas, informações bancárias e de cartões de crédito, até mesmo documentos e imagens íntimas.

Um exemplo de vírus é o Cavalo de Tróia, recebido como um presente, em forma de um álbum de fotos, jogos, protetor de tela ou documento, além de executar as tarefas nas quais ele foi programado, também projeta funções diversas que são prejudiciais para o servidor, e claro, sem o conhecimento do usuário. Outro tipo bastante popular, é o Spam, que consiste em uma mensagem não solicitada, geralmente enviada em grande escala, libera vírus e golpes que podem afetar a segurança do usuário e da internet. Com as novas tecnologias e o despreparo dos usuários, esse tipo de vírus têm se distribuído com muita eficácia e vem se tornado um dos principais problemas da comunicação.

É importante ressaltar que não são apenas os computadores que estão vulneráveis a esses tipos de ataques, mas celulares e tablets que possuem sistema operacional também podem ser atacados por esses programas nocivos.

Além desse tipo de ataque no meio eletrônico, em que a intenção é roubar dados e infectar a máquina, existem diversas outras modalidades de ataques, demonstrando mais uma vez a criatividade do ser humano para obter vantagem indevida ou prejudicar o seu igual:

> Crime contra a segurança nacional, preconceito, discriminação de raça-cor e etnias, pedofilia, crime contra a propriedade industrial, interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software, calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação de direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, incitação ao crime, apologia ao crime ou criminoso, falsa identidade, inserção de dados em sistema de informações, falso testemunho, exercício arbitrário das próprias razões e jogo de azar (COLARES, 2002, p. 02)

Importante reforçar que tais crimes são abarcados tanto se praticados na internet, quanto em sistemas informáticos; conforme Felizardo (2010), os delitos cometidos no meio virtual, dispõem uma extensa lista, que com a globalização da

internet, aumentou consideravelmente a sua prática. Demonstrar-se-á alguns deles na prática e os casos de grande comoção que levaram essas condutas a serem tipificadas pelo Código Penal brasileiro.

A partir do caso da atriz Carolina Dieckmann, que teve suas fotos íntimas expostas a nível nacional por meio de redes sociais e sites de cunho pornográfico, abriu-se o debate sobre o "vazamento" de vídeos e imagens particulares – geralmente de cunho sexual – não ser tipificado em lei. Com isso, no ano do ocorrido, foi criado um tipo penal contido na Lei nº 12.737/2012 que trata da invasão de dispositivos informáticos. Entretanto, o bem jurídico tutelado pela lei não é o mesmo atingido diretamente pelo crime:

> O bem jurídico penalmente tutelado é a inviolabilidade dos dados informáticos, corolário do direito a privacidade e intimidade presentes na Constituição da República, em seu art. 5º, X. A inviolabilidade compreende não só o direito à privacidade e ao sigilo dos dados, como também à integridade destes e sua proteção contra qualquer destruição ou mesmo alteração. (VIANNA; MACHADO, 2013, p. 94)

De fato, essa lei não comportou as condutas mais gravosas que são o compartilhamento de mídias íntimas sem autorização da vítima, atentado direto à dignidade sexual da vítima e, em segundo plano, à privacidade, à intimidade e inviolabilidade de dados. Resta a crítica à deficiência da lei no tocante aos crimes sexuais cometidos virtualmente especificamente ditos, em que a vítima é completamente exposta.

Quanto a esses crimes, a Comissão Parlamentar de Inquérito (CPI) de Crimes Cibernéticos, demonstrou em seu relatório a necessidade urgente de investimentos na ótica forense, para perícia de cibercrimes e apresentou diversos projetos de lei visando a tipificação de algumas condutas (CÂMARA DOS DEPUTADOS, 2016).

Devemos abrir o debate nesse estudo sobre a pornografia infanto-juvenil disseminada na internet, apesar de ser um campo de estudo um pouco obscuro, estudos demonstram que esse crime aumentou drasticamente com a popularização da internet, Pinheiro (2009) aponta como um dos ilícitos mais cometidos em 2009. O problema se complica pela falta de recursos e preparação dos responsáveis pela investigação desses crimes, haja vista que com a internet esses criminosos tornaram-se cada vez mais ardilosos em seus métodos:

> Finalmente, é importante que os governos, as universidades e as indústrias entendam as mudanças no modus operandi dessas atividades criminais, trabalhando continuamente em conjunto para desenvolver novas tecnologias e soluções de investigação, que melhorarão a performance da tecnologia disponível para encontrar material de pornografia infantojuvenil de uma maneira forense e com um correto estabelecimento da cadeia de custódia. Somente assim poderemos vislumbrar um futuro mais seguro para as crianças, em que todas as ocorrências de abuso sexual e seus danos resultantes. (CAIADO; CAIADO, 2018, p. 22).

Uma pequena vitória na tipificação dos crimes virtuais que atingem diretamente a dignidade sexual da vítima, é a Lei nº 3.718, de 24 de setembro de 2018, norma que alterou o Código Penal para tornar crime a divulgação sem autorização de fotos, vídeos e demais imagens íntimas, além de tipificar a divulgação de pornografia infantil (CAIADO; CAIADO, 2018). Com o uso dos aplicativos de conversa, como *WhatsApp* e *Messenger*, as redes sociais e inúmeros sites de pornografia, tornou-se comum a cultura dos conteúdos “vazados”, ou seja, cenas que se encontram na internet sem autorização daquele – geralmente uma mulher – que a protagoniza.

É muito comum que essas imagens sejam expostas pelos próprios ex companheiros das vítimas que não se conformam com o fim do relacionamento, o chamado *revenge porn*, na tradução livre, pornografia de vingança (LELIS; CAVALCANTE, 2016). O conteúdo de modo geral, é inicialmente produzido com o consentimento da vítima, havendo uma relação de confiança, a protagonista da foto ou vídeo não autoriza a divulgação, resultando num crime de extorsão ou até mesmo, na exposição do conteúdo na internet, configurando o crime tipificado pelo artigo 218-C do Código Penal (CAIADO; CAIADO, 2018). É comum encontrar esse tipo de vídeo em sites pornográficos, basta uma rápida pesquisa, além disso, é rapidamente difundido em grupos de WhatsApp e nas redes sociais, trazendo um prejuízo imensurável para a vítima.

Resta-nos refletir sobre a capacidade de destruição da internet no que tange aos crimes cometidos em ambiente virtual, é interessante e infeliz ao mesmo tempo, que uma vez publicado o conteúdo, ele se perfaz pelo tempo e jamais expira. Por conta disso, os cibercrimes merecem atenção especial por parte do legislador e dos juristas, haja vista que a abrangência do dano sofrido pela vítima é quase imensurável (WENDT; JORGE, 2013. CAIADO; CAIADO, 2018).

Percebendo os crimes virtuais como tão importantes quanto os delitos ocorridos na realidade, a necessidade de melhor tipificação e o desdobramento para a investigação em um ambiente tão desconhecido, teremos a concepção de que se necessita de uma vigilância e controle mais rígido do Estado no aspecto de cibercrimes.

2.2.2 SUJEITO ATIVOS E MÉTODOS PARA COMETIMENTO DO CRIME VIRTUAL

Sujeito ativo do crime digital pode ser qualquer pessoa, uma vez que o tipo não determina nenhuma característica especial para tal cometimento.

De acordo com Tulio Vianna, aqueles que cometem o crime virtual não são obrigatoriamente os “gênios” da informática como a maior parte das pessoas imaginam, na maioria dos casos, o agente delituoso utiliza de técnicas bastante simples. Ele não se apresenta pessoalmente, podendo agir que qualquer lugar do mundo.

Tais agente são reconhecidos por algumas nomenclaturas, sendo uma delas o *Cracker*, que é aquele que tem o pleno conhecimento em informática e o utiliza para burlar sistemas de segurança ilegalmente; o *Preaker*, aquele que burla meios de comunicação telefônica para uso próprio; o *Lammer*, aquele agente que detêm certos conhecimentos e pretende se tornar um *hacker*, onde fica invadindo sites, sendo basicamente um iniciante, tendo o diferencial que utiliza esses maios para prejudicar terceiros; o *Hacker*, aquele que tem um amplo conhecimento em sistemas operacionais, e se utiliza disso para invadir sistemas apenas para mostrar para si mesmo o quanto é capaz, se causar danos a outras pessoas; e por fim o *Guru*, o qual tem domínios sobre os mais diferenciados tipos de sistema, e é considerado o mestre dos *hackers*.

Para o cometimento desses crimes virtuais, são utilizados alguns métodos, sendo eles: o Cavalo de Tróia, que é instalado no computador se tornando uma fonte de subtração de informações, dentre elas, senhas e arquivos; os vírus que podem destruir dados informatizados; *spayware* que serve de uma programação espiã, onde monitora os hábitos do computador e da vítima; *sniffers* que serve para interceptar informações que circulam nesse meio.

3 PRINCÍPIOS NORTEADORES

3.1 PRINCÍPIO DA LEGALIDADE

Este princípio não tem incidência somente no direito material, mas também a todo ato processual que estabelece uma limitação de um direito fundamental, como é o caso do direito de locomoção.

O princípio da legalidade tem por finalidade proibir a existência de medidas coercitivas desprovidas de lei. Pois a aplicação da prisão provisória fica restrita aos casos estabelecidos em lei.

Nesses termos, estabelece o inciso LXI do artigo 5º da Constituição Federal de 1988:

> Art. 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
> (...)
> LXI - ninguém será preso senão em flagrante delito ou por ordem escrita e fundamentada de autoridade judiciária competente, salvo nos casos de transgressão militar ou crime propriamente militar, definidos em lei. (BRASIL, 2019).

Estabelece também Aquino e Nalini (2005, p. 97) sobre o princípio da legalidade:

> Também denominado princípio da obrigatoriedade. É a exteriorização do princípio da oficialidade, segundo a qual, tanto a polícia judicial como o Ministério Público titularizam o dever de exercer a ação penal pública de acordo com a lei. Não podem inspirar-se em critérios políticos de conveniência, oportunidade ou utilidade social.[...] com a edição da Lei 9.099/95, teve seu campo de atuação reduzido vez que [sic] agora o Ministério Público pode suspender consensualmente o processo nas ações penais públicas cuja pena for igual ou inferior a um ano.

Assim, pode observar que é do princípio da legalidade que proíbe qualquer medida coercitiva que não esteja estabelecida em lei.

3.2 PRINCÍPIO DA INTERVENÇÃO MÍNIMA

O princípio da intervenção mínima não está previsto expressamente no ordenamento jurídico, nem no texto constitucional nem nas normas penais**.** Este

princípio tem por finalidade que só será aplicado nos casos de extrema necessidade, pois o direito penal é a intervenção mais severa que o Estado possui, devendo ser aplicada somente em último caso.

O postulado da intervenção mínima diferencia um bem jurídico penal do bem jurídico em sentido geral que Artur de Brito Gueiros Souza comenta:

> Nesse sentido, o princípio da intervenção mínima diferencia um bem jurídico penal do bem jurídico em sentido geral. O bem jurídico lato sensu é todo e qualquer valor importante para a sociedade, cuja proteção venha a ser determinada por força de lei, ou por força de ato administrativo. Já os bens jurídicos penais são os valores essenciais, que devem constituir o núcleo central do estado democrático de direito. Desse rol, por exemplo, fazem parte a vida, o patrimônio, a identidade corporal e a liberdade psíquica ou individual (SOUZA, 2018, p.121).

Assim sendo, o direito penal não protege qualquer bem jurídico, mas somente aqueles bens que tem valores caros para a sociedade, e só deve ser utilizado quando os outros ramos do direito se demonstrem insuficiente para proteger o direito da vítima

A respeito do princípio da intervenção mínima estabelece Capez:

> a subsidiariedade como característica do princípio da intervenção mínima, norteia a intervenção em abstrato do Direito Penal. Para intervir, o Direito Penal deve aguardar a "ineficácia" dos demais ramos do direito, isto é, quando os demais ramos mostrarem-se incapazes de aplicar uma sanção à determinada conduta reprovável. É a sua atuação ultima ratio. (CAPEZ, 2012, p.615).

Nesse mesmo sentido estabelece Cezar Roberto Bitencourt:

> O princípio da intervenção mínima, também conhecido como ultima ratio, orienta e limita o poder incriminador do Estado, preconizando que a criminalização de uma conduta só se legitima se constituir meio necessário para a prevenção de ataques contra bens jurídicos importantes. Ademais, se outras formas de sanção ou outros meios de controle social revelarem-se suficientes para a tutela desse bem, a sua criminalização é inadequada e não recomendável. Assim, se para o reestabelecimento da ordem jurídica violada forem suficientes medidas civis ou administrativas, são estas as que devem ser empregadas, e não as penais. Por isso, o Direito Penal deve ser a ultima ratio do sistema normativo, isto é, deve atuar somente quando os demais ramos do Direito revelarem-se incapazes de dar a tutela devida a bens relevantes na vida do indivíduo e da própria sociedade. (BITENCOURT, 2013, p.54).

Portanto, para resolver os conflitos na sociedade, deve-se primeiramente esgotar todos os outros ramos de direito além do direito penal para depois em último caso ser aplicado a esfera penal na proteção d bens jurídicos.

3.3 PRINCÍPIO DA LESIVIDADE

O princípio da lesividade também conhecido como da ofensividade traz a ideia que uma conduta somente poderá ser protegida pela esfera do direito penal se a conduta praticada pelo agente criminoso seja apta a causa dano ou risco a bem jurídico relevante.

Nessa linha leciona Souza sobre o princípio da lesividade:

> Uma norma penal, portanto, deve necessariamente proteger um interesse jurídico fundamental contra lesões ou risco de lesões. Dessa maneira, veda-se o estabelecimento de delitos que sejam meras infrações de obrigações ou de deveres, o que significaria uma excessiva intervenção estatal, que não pode ser aceita (SOUZA, 2018, p. 119).

Portanto, um cidadão somente pode ser punido quando seu comportamento afeta bens ou direito de um terceiro, assim o direito penal não pode intervir e punir a intimidade das pessoas.

3.4 PRINCÍPIO DO ESTADO DE INOCÊNCIA

Este princípio está relacionado à tutela jurisdicional, em que transmite a ideia de que ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória.

Assim para que alguém seja condenado deve ser realizado todo procedimento legal que garante o direito ao contraditório e ampla defesa.

No que tange ao princípio da presunção de inocência estabelece Reis:

> Assim, nada mais natural que a inversão do ônus da prova, ou seja, a inocência é presumida, cabendo ao MP ou à parte acusadora (na hipótese de ação penal privada) provar a culpa. Caso não o faça, a ação penal deverá ser julgada improcedente.(REIS,2017, p. 1728)

E o ordenamento jurídico brasileiro prevê a possibilidade de aplicação de prisão provisória quando ainda não há sentença penal condenatória transitada de julgado. Em que estabelece o encarceramento mesmo não declarado culpado.

Observa-se a existência de um conflito entre os princípios da presunção de inocência e da liberdade pessoal. Pois a medida de prisão antes da sentença penal afronta o princípio da presunção da inocência, pois, caso futuramente seja o indivíduo absorvido, comprove que não é autor do crime que foi acusado, terá comprido pena injustamente.

Deixa claro, por ser um princípio que está expresso na Constituição Federal como um direito fundamental deve ser respeitado. Em que garante ao acusado.

3.5 PRINCÍPIO DA LIBERDADE DE EXPRESSÃO

O princípio da liberdade de expressão é uma norma constitucional, previsto na Constituição em seu artigo 5º, no inciso IX em que estabelece que é livre a expressão da atividade intelectual, artística, científica e de comunicação. E além dessa norma está inserido no artigo 220, §1º do mesmo diploma normativo em que dispõe que é vedada toda e qualquer censura de natureza política, ideológica e artística.

O princípio da liberdade de expressão é basilar para a concretização das liberdades fundamentais e de outros direitos humanos, por esse motivo, a liberdade de expressão é elemento essencial para uma sociedade democrática, é a livre circulação de informação que proporciona o acesso ao conhecimento e à cultura, sendo, portanto, fundamental. (ARTIGO 19, 2013, p. 4).

Percebe-se a importância desse princípio, pois traz a ideia a liberdade de expressão de todas as pessoas que procuram, e ainda estabelece o direito a informação que tem a capacidade de gerar outros direitos fundamentais.

O direito à informação pode ser subdividido, sendo analisado por perspectivas diferentes, quais sejam: a) o direito de prestar informações; b) o direito de busca e acesso à informação; e c) o direito de ser informado (BOFF, 2012, p. 333).

Percebe-se, portanto, que a informação é um elemento primordial na vida das pessoas, tem a finalidade de transmitir o direito de ser informado e de cada indivíduo poder acessar as informações necessárias.

4 ANÁLISE DA LEGISLAÇÃO BRASILEIRA

No ordenamento jurídico existe uma sucessão de leis que procuram tratar de crimes cibernéticos, mas ainda não existe um código específico nem ao menos com uma conceituação jurídica adequada, e isso se torna bastante preocupante, levando em consideração o crescente número de usuários da informática, e consequentemente as vítimas nesse ambiente, necessitando assim de uma urgente revisão das normas jurídicas. E nada mais é como adota Pinheiro:

> "Portanto, as condutas chamadas de crimes virtuais (embora inexista legislação específica) encontra-se tipificada em textos legislativos existentes (Código Penal e legislação esparsa) e, ao contrário do que alguns autores afirmam, a aplicação da lei já existente a essas condutas não é caso de analogia, pois não são crimes novos, não são novos bens jurídicos necessitando de tutela penal, a novidade fica por conta do modus operandi, de como o criminoso tem feito uso das novas tecnologias, com foco na Internet, fazendo com que os estudiosos e os aplicadores do Direito tenham que renovar o seu pensamento". (Pinheiro, 2013, p. 28).

Junto aos cybercrimes vêm dois intérpretes, o hacker que é um programador com um amplo conhecimento acerca de sistema, que não tem o objetivo de causar danos; e o cracker, que pratica a quebra de sistemas de segurança, senhas e códigos de segurança, de maneira ilegal, onde alguns visam o lucro e outros visam apenas a notabilidade.

A maior parte dos magistrados e consultores jurídicos, declara que cerca de 95% das infrações cometidas no meio eletrônico já estão tipificadas no Código Penal, por configurar delitos comuns praticados no meio da internet. Os outros 5% abrangem delitos que só existem no meio virtual, como a propagação de vírus, cavalos-de-troia.

A Lei 7. 232/84 foi uma das primeiras a ser criada exclusivamente para o meio informático, onde estabeleceu as diretrizes sobre a Política Nacional de Informática por meio do Conselho Nacional de Informática, e a partir disso começaram a surgir algumas das legislações com o intuito de proteger o bem jurídico informático. Essa lei foi revogada por meio da Lei nº 9.609/98, que discorria sobre a proteção de programas de computadores, tipificado suas violações como crime.

> Art. 35. Violar direitos de autor de programas de computador:
> Pena – Detenção, de 6 (seis) meses a 2 (dois) anos e multa.
> Art. 37. Importar, expor, manter em depósito, para fins de comercialização, programas de computador de origem externa não cadastrados:

Pena – Detenção, de 1 (um) a 4 (quatro) anos e multa. (BRASIL, 1998).

Além disso, o STJ já firmou o entendimento de que os crimes de pedofilia e divulgação de pornografia infantil por meios eletrônicos, que estão descritos na legislação especial que proíbe crimes impróprios, cujo exemplo é o ECA, Lei nº 8.069/90, que na sua atualização em 2008 tipificou o armazenamento ou distribuição de fotos pornográficas envolvendo crianças e adolescentes, como crime:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (BRASIL, 2019).

A Corte entendeu que apenas o envio de fotos pornográficas através da internet já constitui crime.

Outro caso que já foi devidamente enquadrado pela Corte foram os casos de furto e estelionato virtual, onde a Terceira Seção do STJ estabeleceu que a apropriação de valores de conta corrente de maneira fraudulenta via internet sem o consentimento da vítima, configura furto qualificado por fraude; decidiu também que a competência para julgar tal crime é do juízo do laco da consumação do delito de furto, local cujo o bem é subtraído da vítima.

Como crimes próprios, a Lei nº 9.983/00 serve como exemplo, o qual tipificou condutas como inserção de dados falsos em sistemas e informações ou alterações não autorizadas:

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:

> Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado. (BRASIL, 2019).

Em 2012, foram publicadas duas Leis, que alteraram o CP para tratam especificamente de crimes cibernéticos: A Lei 12.735/12, que tipifica condutas realizadas no meio digital, que sejam praticadas contra sistemas informatizados, e essa norma traz que a polícia judiciária terá que estruturar e formar equipes especializadas no combate à ação delituosa em rede de computadores e dispositivos de comunicação.

> Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. (BRASIL, 2019).

E a Lei 12.737/12 que passa a criminalizar a invasão de computadores, e o furto de senhas e arquivos, cuja pena prevista é de 3 meses a 1 ano para agentes que invadir dispositivo informático alheio, podendo estar conectado ou não à rede de computadores.

> 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.
> [...] (BRASIL, 2019).

Mais tarde, a regulação da internet no Brasil foi se aperfeiçoando com o Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, que estabelece os princípios, garantias, direitos e deveres para o uso da internet no Brasil. Mas se engana quem pensa que a ex-presidente Dilma Rousseff apressou o projeto do Marco Civil da Internet por estar preocupada com a sociedade civil brasileira e com a adequação do Brasil com a informação na internet; lamentavelmente ela fez isso para tutelas um objetivo pessoal, devido ao fato de estar sendo vigiada pela inteligência dos Estados Unidos durante o governo Obama em alguma relação com a estatal Petrobrás e questões de lavagem de dinheiro.

Os princípios para o uso da internet no Brasil são enunciados pelo Art. 3º da referida Lei:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (BRASIL, 2019).

Um outro ponto relevante do Marco Civil são os direitos e Garantias dos usuários, que trata no art 7º, da referida norma:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

> [...]
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> [...]
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet. (BRASIL, 2019).

O Marco estabelece que os provedores têm o dever de manter os registros pelo tempo de um ano, e permite que a autoridade policial ou administrativa e/ou o Ministérios Público possam requerer a guarda dos registros por mais tempo. Estabelece também que o tempo presumido para a guarda em provedores de aplicações são de seis meses:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
> [...]
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
> § 3º Na hipótese do § 2º a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.
> § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.
> [...]
> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos temos do regulamento.[...] (BRASIL, 2019).

A nova Lei traz também que a natureza de ação penal, nos crimes contra a dignidade sexual passa a ser incondicionada.

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que

> contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia:
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave. (BRASIL, 2019).

Por fim, veio a Lei 13.718/18, que introduz modificações no campo dos crimes contra a dignidade sexual. Sua ementa “Tipifica os crimes de importunação sexual e de divulgação de cena de estupro; altera para pública incondicionada a natureza da ação penal dos crimes contra a dignidade sexual; estabelece causas de aumento de pena para esses crimes; cria causa de aumento de pena referente ao estupro coletivo e corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais).

4.1 POSIÇÃO JURISPRUDENCIAL E DOUTRINÁRIA SOBRE A LEI Nº 12.737/2012

Em 2012 a atriz global Carolina Dieckmann foi vítima de exposição íntima na internet, o que a princípio afirmaram foi que o fato ocorreu após ela levar seu computador para assistência técnica, onde continha fotos de seu corpo e suas intimidades, as quais foram furtadas e divulgadas em massa, o que logo após foi desmentido a história. Posteriormente, verificou-se que o infrator enviou um *e-mail*, que a induzia abrir um anexo, que através da mensagem teria um código malicioso, onde deixaria o computador vulnerável; ou seja, ela foi vítima de invasão de dispositivo informático, logo após, o furto das imagens, e por fim, o infrator ameaçando expor tais fotos na internet caso ela não pagasse a quantia solicitada. Como a atriz não cedeu às exigências do infrator, o mesmo divulgou asa fotos conforme ameaçado. Seus direitos foram atendidos rapidamente, visto a fama da atriz. O infrator foi indiciado por extorsão conforme o artigo 158 do Código Penal:

> Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa:
> Pena - reclusão, de quatro a dez anos, e multa.
> [...] (BRASIL, 2019).

Com base nesse famoso caso, o projeto de Lei 2.793/2011 do Deputado Paulo Teixeira (PT-SP), voltou a ser cotado e foi sancionado em 02 de dezembro de 2012,

a fim de dar uma previsão legal para tais crimes informáticos, tipificando os delitos praticados através do meio eletrônico. E assim, como na Lei Maria da Penha, a atriz cedeu seu nome à Lei 12.737/2012, que trouxe alterações ao Código Penal Brasileiro, preceituando acerca da tipificação criminal de crimes informáticos.

Após o fato descrito acima, quando a vítima foi uma atriz famosa, e que a vulnerabilidade veio a público, que o Brasil viu que algo precisava ser feito. O que nos leva a questão da criação do Marco Civil da Internet, onde apenas dois anos separam a Lei 12.737/2012 do Marco 12.965/2014, que mostra uma modificação conjunta nas áreas penal e civil, buscando uma proteção no ambiente digital.

A Lei nº 12.737 de 30 de novembro de 2012, dispõe sobre a tipificação criminal de delitos informáticos, alterando o Decreto-Lei nº 2.848 de 07 de dezembro de 1940 – Código Penal. Essa Lei trouxe para o ordenamento jurídico o crime de invasão de dispositivos informáticos, que consiste em invadir dispositivos alheios, independentemente de estar conectado ou não à rede de computadores, com a intenção de adulterar, destruir ou apenas obter dados sem autorização expressa do usuário titular para adquirir vantagem ilícita. Serviu de grande referência de debates após anos de ineficiência jurídica, sendo a primeira lei criada tão somente para a tipificação de crimes cibernético, que antes disso não havia outra opção senão a impunidade.

A Lei 12.737 de 2012 trouxa uma grande inovação em que introduziu um novo tipo penal sendo o delito de invasão de disposto informático nos seguintes termos:

> 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.”(BRASIL, 2019)

O crime de invasão informática pode causar sérios prejuízos à vítima, por ser um crime que expõe a pessoa por meio de roubos de informações pessoais e até mesmo sigilosas. A pena prevista é de detenção de 3 meses a um ano e multa, havendo qualificação e aumentos de pena, conforme o artigo acima.

Na generalidade, é um crime de ação pública condicionada, ou seja, dependerá da representação do lesionado ou de quem tiver qualidade para representa-lo, exceto em crimes cometidos contra o patrimônio da administração pública direta ou indireta e a qualquer dos Poderes da União, Estados, Distrito Federal e Municípios, tornando-se assim de ação pública incondicionada, que é o que traz o artigo 154-B da referida Lei.

Além disso, a referida lei alterou também os artigos 266 e 298 do Código Penal, conforme exposto a seguir:

> 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) (BRASIL, 2019)

Percebe-se que de acordo com o artigo 3º acima da lei alterou também o conceito de crime de interrupção de serviço informático, o qual é bastante praticado no dia a dia, sendo por meio de araques que pretendem reduzir ou até mesmo inutilizar a capacidade de um serviço na rede de computador, causando assim prejuízos no provedor de serviço.

A eficiência da Lei 12.737 é questionável, pelos operados do direito, já que a ótica da Lei Carolina Dieckmann abrange em grande parte, apenas o desfalque patrimonial sofrido pela vítima, sendo que deveria englobar a lesão às garantias individuais, como a honra, imagem, dignidade.

No Brasil, existe um número muito grande de casos de publicações de fotos intimas sem o consentimento da vítima e que ocorrem por meio de invasão computacional; pesquisas apontam que as mulheres são vítimas habituais de tal conduta. Dados da policial civil, pontam que, em Minas, 111 infrações contra a dignidade sexual na web foram registradas no primeiro trimestre de 2019, um crescimento de 122% em relação ao mesmo período de 2018.

Na atualidade o popularmente conhecido “nudes”, onde casais trocam fotos, sem vestimentas, por se sentir confortável com seu parceiro, mas que ao término da relação pode se transformar em instrumento de vingança, e acabar por ser divulgado tais fotos comprometedoras, o que pode trazer danos psicológicos e prejuízos irreparáveis à pessoa exposta. E apesar de haver tipificação para esse tipo de conduta, o agente sofre as punições, mas não são suficientes para reprimir o criminoso, a prática vem aumentando a cada ano, e acaba que é sempre a vítima quem sofre as maiores consequências, que na maior parte as vezes, ela nem reage a esse ataque, e posterior ao dano, muitas vítimas passam a desenvolver transtornos de ansiedade, síndrome do pânico, estresse pós-traumático, entre outros; e o prejuízo, quase nunca é reparado totalmente, vez que o material divulgado será armazenado por novas pessoas, podendo vir à tona a qualquer momento

A pouco tempo tivemos o caso da jovem que aos 14 anos de idade se relacionou com um rapaz de 17 anos, e que a ameaçou com fotos tiradas pelo mesmo, as quais ela não tinha conhecimento, e a jovem acabou se enforcando, por receio de tais fotos serem divulgadas. O que nos mostra que esse tipo de crime não atinge apenas o computador, mas pode trazer danos irreversíveis para as vítimas, e que por muitas vezes os aparelhos eletrônicos são usados por pessoas sem o mínimo de

moral, o que é fundamental meios mais eficazes para assegurar a proteção da sua intimidade e vida privada, como traz na CF, em seu artigo 5º, V.

Outro exemplo que teve bastante repercussão na mídia, foi o caso do jogador Neymar, onde após ser acusado de estupro por uma mulher, divulgou imagens intimas da mesma.

Antes da edição da lei, os crimes como furto e estelionato eletrônicos não tinham necessidade de legislação específica conforme julgamento abaixo:

> "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.(BRASIL, 2019).

Conforme julgado acima do Supremo Tribunal Federal é nítido na possibilidade de interpretação extensiva da lei, assim crimes como o estelionato pode acontecer de forma virtual, não sendo necessário de lei que versa necessariamente de modo virtual.

Nessa mesma linha, segue jurisprudência do Supremo Tribunal Federal em que dispõe da não necessidade de lei especifica para crimes virtuais antes da Lei nº 12.737 de 2012:

> PENAL. PROCESSO PENAL. CONFLITO DE JURISDIÇÃO. INQUÉRITO POLICIAL. FRAUDE BANCÁRIA. CAIXA ECONÔMICA FEDERAL. TRANSFERÊNCIA DE VALORES POR MEIO ELETRÔNICO (INTERNET). FURTO MEDIANTE FRAUDE. (ART. [155], § 4º, INC. II, CP). FORO DA CONSUMAÇÃO DO DELITO.

> LUGAR ONDE SITUADA A AGÊNCIA EM QUE MANTIDA A CONTA-CORRENTE LESADA. PRECEDENTES (STJ E TRF4).
> 1. **Consolidou-se o entendimento de que a subtração de valores de conta-corrente ou conta-poupança - sem a autorização do titular e por meio de expediente eletrônico fraudulento (Internet) - configura o crime de furto mediante fraude** (art. 155, § 4º, inc. II, CP).
> 2. Considerando que **o delito de furto se consuma no momento em que a coisa móvel é retirada da esfera de disponibilidade da vítima e colocada em poder do agente**, competente para apreciar o feito é o juízo do lugar onde situada a agência da CEF em que mantida a conta corrente lesada.
> 3. Precedentes do Superior Tribunal de Justiça e deste Tribunal. (grifos nossos).(BRASIL, 2019).

Salienta-se, portanto, que há doutrinadores que entendem que não há necessidade de lei específica para dirimir os crimes virtuais, em que o Código Penal Brasileiro já consegue proteger tais delitos.

Desta forma, segue entendimento de Patrícia Peck Pinheiro:

> não há sociedade saudável sem que estejam claros os valores que são protegidos e sanção para quem as descumpra. Entretanto, tem-se que penalizar o infrator digital com uma pena que impacte sua esfera virtual, não apenas física, pois, segundo ela, de nada adianta colocar o criminoso eletrônico em uma cela na cadeia e ele continuar acessando a internet via celular, o que fará com que ele continue praticando o crime.(PINHEIRO, 2011, p. 61).

Nesse sentido pela desnecessidade de lei que regula crimes virtuais dispõe Dooun:

> Direito Penal para as relações virtuais deve ser um direito penal mínimo, não havendo necessidade de uma legislação nova, deve-se usar direito penal minimamente, usando os outros ramos do direito para coibir as situações praticadas no ambiente eletrônico. Deve o Direito Penal ser guardado e resguardado para situações extremas. Faz crítica o criminalista quanto à compulsividade de legislar, de criar lei penal, sob o argumento de que o Direito penal é o instrumento do direito mais drástico que se tem, pois, segundo ele, pagar indenização é uma coisa, perder a liberdade é outra. A criação demasiada de lei gera faz com que esse ramo do perca sua credibilidade. (DOOUN, 2012, p.11).

Verifica-se que para estes doutrinadores acima, que o entendimento é que não há necessidade de lei específica para dirimir os conflitos no âmbito virtual, em que os crimes como exemplo, furto e estelionato praticados por meio eletrônico são perfeitamente protegidos e sujeitos a sanção penal pelo Código Penal Brasileiro.

Por outro lado, Tulio Lima Vianna explica sobre a necessidade de lei específica:

> a elaboração de uma legislação penal moderna que verse sobre crimes informáticos facilitaria e muito o trabalho dos operadores do direito, considerando por ideal que o tema fosse regulado por um tratado internacional, aos moldes da Convenção de Genebra, posto que a internet é um fenômeno transnacional. Ocorre que, conforme opinião do referido autor, a morosidade com que se aprovam as leis no Brasil é fato notório, por esse motivo, prefere o “desafio da análise cuidadosa de nossa legislação penal, que, (...), já tipifica muitas das modernas condutas delituosas realizadas pela interne (VIANA, 2013, p. 5).

Por fim, verifica-se que apesar de poucas normas especificas referente aos crimes cibernéticos, já constituem um aparato normativo pelo Estado contra as condutas criminosas digitais. Sendo, portanto, suficiente juntos com o Código Penal para coibir ações em face do mundo cibernético.

CONSIDERAÇÕES FINAIS

Os crimes cibernéticos são um fenômeno jurídico recente, devido a isso o ordenamento jurídico brasileiro ainda não o acompanhou, levando assim às lacunas legislativas perigosas que precisam ser sanadas.

A criminalidade virtual vem crescendo a cada dia mais, nos quais as condutas são dotadas de características específicas em que o direito penal não consegue tutelar o bem jurídico diante da alta lesividade.

Por este fato foi criada a Lei conhecida como Lei Carolina Dieckmann com o fim de tutelar os crimes informáticos puros, no entanto esta lei conforme visto é deficiente em alguns pontos, especialmente por não preverem forma de violência moral nas condutas praticadas pelos crimes cibernéticos.

No ano de 2014, foi sancionada a Lei nº 12.965, intitulada “Marco Civil da Internet”. Esta foi produzida com o intuito de preencher as lacunas de nosso sistema jurídico no tocante aos crimes virtuais. Inicialmente, trata dos fundamentos e conceitos, elencando os direitos dos usufruidores. Tipifica princípios, tais como liberdade, neutralidade e privacidade, além de determinar garantias, direitos e deveres no ambiente virtual. Um destaque se dá ao direito e garantia a inviolabilidade da intimidade e da vida privada.

Contudo, sabe-se que no momento de punição ao desrespeito de tais princípios as penas são plácidas e não atingem um resultado satisfatório. Além disto, para requisições de informações privadas é necessária ordem judicial, não podendo o provedor da internet fornecer dados como IP, senha e login dos criminosos, deixando o trabalho de investigação moroso. Por mais válida que seja a tipificação de garantias e direitos, tais artigos não abarcam por completo o campo de atividade dos criminosos virtuais, ficando as lacunas a mercê de suprimento advindo de outras legislações, como por exemplo, casos de compras on-line, que são regulamentadas pelo CDC (Código de Defesa do Consumidor).

No presente trabalho traz a intenção de estudar os crimes cometidos pelo mundo da internet, tendo em vista com as revoluções tecnológicas as pessoas interagem bastante por meio do mundo virtual, através de redes sociais, compras virtuais, acesso mais prático em contas bancárias e dentre outros exemplos e para

resguardar o sigilo e o acesso de informações. Sendo assim foi analisado se é considerável ou não a implementação de legislação específica sobre os crimes cibernéticos.

Assim sendo, verifica-se o número crescente de pessoas lesadas por meio do mundo virtual, em que são ofendidos, lesados ou até mesmo agredidos por meio de algum dano. Portanto, se faz necessário que o Estado tenta coibir a prática dos crimes digitais.

Porém, diante da existência de poucas normas específicas que versem sobre a proteção contra os crimes virtuais dificulta a ação do Estado na esfera digital, e para não permanecer inerte verifica-se que o Estado vem aplicando a legislação brasileira especificamente o Código Penal por analogia para coibir e proteger contra as práticas de condutas delituosas para não gerar impunidade.

Salienta-se também que conforme o estudo as vezes o agente criminoso pratica a conduta não com a intenção de praticar um crime digital, mas sim o acesso indevido ao sistema de informação é um meio da prática de um delito comum previsto no ordenamento jurídico, configurando os chamados crimes impróprios. Já os crimes próprios seriam aqueles que a conduta tem a intenção de ser cometidos contra o sistema informacional.

Contudo a lei nº 12.737 de 2012 é de suma importância no combate dos crimes cibernéticos, contudo é ainda insuficiente para tutela do direito.

Diante da intervenção mínima do direito penal na tutela de bens jurídicos, conforme foi estudado anteriormente em que a intervenção da proteção pela esfera penal é somente em ultimo caso quando as outras áreas não conseguirem proteger o direito lesado verifica-se que a legislação específica é insuficiente para a tutela dos crimes informáticos. Sendo necessário a tutela pelo direito penal por meio da interpretação extensiva.

Por fim, para essa nova realidade de crimes cibernéticos necessita de uma rápida resposta estatal no combate dos crimes, assim a existência e efetivação de uma legislação específica no resguardo dos direitos dos cidadãos para garantir a segurança virtual junto com a tutela do direito penal brasileiro.

Pois um dos maiores obstáculos do Estado no que refere a proteção dos crimes digitais, se dá pelo fato de o Estado sempre aplicar por analogia o ordenamento jurídico brasileiro nas ações punitivas contra crimes digitais, em que muita das vezes

a lei penal permanece omissa, sendo necessário uma adaptação criando mais leis específicas para evitar verdadeiras brechas contra a impunidades dos infratores de crimes virtuais.

REFERÊNCIAS BIBLIOGRÁFICAS

_____Supremo Tribunal Federal. **Habeas Corpus** nº 76689 PB. Partes: Wilson Furtado Roberto; Luiz Alberto Leite Filho; Antonio Carlos Monteiro E Outro; Tribunal De Justiça Do Estado Da Paraíba. Relator: Sepúlveda Pertence. Julgado Em: 21/09/1998.Disponívelem:<Http://Stf.Jusbrasil.Com.Br/Jurisprudencia/740355/Habeas-Corpus-Hc-76689-Pb> Acesso em: 5 dez. 2019

ARTIGO 19. **Direito ao Compartilhamento: Princípios sobre a Liberdade de Expressão e Direitos Autorais na Era Digital**. 2013. Disponível em: <http://www.article19.org/data/files/medialibrary/3716/13-04-23-right-to-share-PO.pdf> Acesso em: 22 out 2013.

ASCENSAO, José de Oliveira. **Direito da Internet e da Sociedade da Informação**. ed. Rio de Janeiro: ed. Forense, 2002.

BARRETO JUNIOR, Irineu Francisco. Atualidade do conceito Sociedade da Informação para a pesquisa jurídica. In: PAESANI, Liliana Minardi (Coord.). **O Direito na Sociedade da Informação**. São Paulo: Atlas, 2007, p. 59.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**: Parte geral, I. 19ª ed. rev., ampl. e atual. São Paulo: Saraiva, 2013, p. 54.

BOFF, Salete Oro e DIAS, Felipe da Veiga. **O acesso à informação no campo digital**: Uma análise entre a sociedade da informação e a sociedade de risco. **Revista de Estados Jurídicos**, ano 16, n.23, 2012

BRITO, Auriney Uchôa de. **O bem jurídico-penal dos delitos informáticos**. **Boletim Ibccrim**, São Paulo, v. 199, n. 17, p.14-15, jun. 2009. Disponível em: <https://www.ibccrim.org.br/boletim_artigos/236-199-Junho-2009>. Acesso em: 05 jun. 2019.

BRASIL. Lei nº 17.718, de 24 de setembro de 2018. **Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).** Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 05 jun. 2019.

BRASIL. Lei nº 12.737/2012, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos.** Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 05 jun. 2019.

CÂMARA DOS DEPUTADOS. **CPI - Crimes Cibernéticos.** 2016. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos>. Acesso em: 04 nov. 2019.

CARNEIRO. Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema da tipificação.** Disponível em: < http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529> Acesso em: 06 nov. 2019

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

CAPEZ, Fernando. **Curso de Processo Penal**. 15. ed. rev. e atual. São Paulo: Saraiva, 2012.

COLARES, Rodrigo Guimarães. **Cibercrimes**: os crimes na era da informática. **Revista Consultor Jurídico**, Meio Eletrônico, 26 jul. 2002. Disponível em: <https://www.conjur.com.br/2002-jul-26/crimes_informatica>. Acesso em: 05 jun. 2019

COSTA, Marco Aurélio Rodrigues. **Crimes de informática**. Disponível em: Revista Eletrônica Jus Navigandi. Site: http://www.jus.com.br/doutrina/crinfo.html. 1997. Acesso em: 14 de nov de 2019

DAOUN, Alexandre Jean *apud* ROSSETTO, Marcela. Direito penal mínimo na web. **Visão jurídica**. São Paulo: Escola, ano V, edição 62, Junho/2011

FORBES. Compras online somaram R$ 166,2 bi no Brasil. **Forbes.** São Paulo, p. 1-1. 12 set. 2018. Disponível em: <https://forbes.uol.com.br/colunas/2018/09/compras-online-somaram-r-1662-bi-no-brasil/>. Acesso em: 03 jun. 2019.

GLOBO. Polícia encontra hackers que roubaram fotos de Carolina Dieckmann. **G1**, Rio de Janeiro, 13 maio 2012. Disponível em: <http://g1.globo.com/fantastico/noticia/2012/05/policia-encontra-hackers-que-roubaram-fotos-de-carolina-dieckmann.html>. Acesso em: 01 jun. 2019.

PECK PINHEIRO, Patricia. Direito penal mínimo na web. **Visão jurídica**. São Paulo: Escola, ano V, edição 62, Junho/2011

PINHEIRO, Patrícia Peck**. Direito digital**. 5. Ed. São Paulo: Saraiva, 2013.

REIS, Alexandre Cebrian Araújo. **Direito processual penal esquematizado** / Alexandre Cebrian Araújo Reis e Victor Eduardo Rios Gonçalves ; coordenador Pedro Lenza. – São Paulo : Saraiva, 2012

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos:** Ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2013.

VELLOSO, Jean Pablo Barbosa. **Crimes Informáticos e Criminalidade Contemporânea**. Out. 2015. Disponível em: Acesso em: 15 DE nov. de 2019.

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos.** Belo Horizonte: Fórum, 2013.

CAIADO, Felipe B.; CAIADO, Marcelo. **Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse**. In: FEDERAL, Ministério Público. **Crimes cibernéticos.** Brasília: Minstério Público Federal, 2018.

ROSA, Fabrízio. **Crimes de Informática**. Campinas: Bookseller, 2002.

FELIZARDO, Aloma Ribeiro. **Cyberbullying Difamação na Velocidade da Luz**. São Paulo: Willem Books, 2010.

REDAÇÃO GALILEU. **Foto de um buraco negro é revelada pela primeira vez na história**: No anúncio, cientistas disseram que o feito só foi possível a partir do sonho de Albert Einstein, há 100 anos. **Galileu**, São Paulo, 10 abr. 2019. Disponível em: <https://revistagalileu.globo.com/Ciencia/Espaco/noticia/2019/04/foto-de-um-buraco-negro-e-revelada-pela-primeira-vez-na-historia.html>. Acesso em: 01 jun. 2019.

LELIS, Acácia Gardênia Santos; CAVALCANTE, Vivianne Albuquerque Pereira. Revenge Porn: **A Nova Modalidade de Violência de Gênero**. **Derecho y Cambio Social**, 2016. Disponível em: < https://www.derechoycambiosocial.com/revista045/REVENGE_PORN.pdf>. Acesso em: 25 jun. 2019.

VIANA, Tulio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013