PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

CRIMES CIBERNÉTICOS: A INEFICÁCIA DA LEGISLAÇÃO BRASILEIRA.

ORIENTANDO (A): SARAH PEREIRA FERREIRA
ORIENTADOR (A): PROF. (A) ME. CARMEN DA SILVA MARTINS

GOIÂNIA-GO

2021

SARAH PEREIRA FERREIRA

CRIMES CIBERNÉTICOS: A INEFICÁCIA DA LEGISLAÇÃO BRASILEIRA

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof. (a) Orientador (a): ME. CARMEN DA SILVA MARTINS.

GOIÂNIA-GO

2021

SARAH PEREIRA FERREIRA

CRIMES CIBERNÉTICOS: A INEFICÁCIA DA LEGISLAÇÃO BRASILEIRA

Data da Defesa: 26 de Maio de 2021

BANCA EXAMINADORA

Orientador (a): Prof. (a): Orientadora Carmen da Silva Martins.
Nota

Examinador (a) Convidado (a): Prof. (a) : Prof. Me. Marcelo Di Rezende

Nota

Dedico este trabalho aos meus pais. Sem eles nada seria possível. Os dois maiores incentivadores das realizações dos meus sonhos. Muito obrigado.

Agradecimentos

Agradeço primeiramente a Deus, pois sem a sua graça não seria capaz de alcançar a conclusão deste trabalho. Meus sinceros agradecimentos aos meus pais Antônia Pereira e Edicio Neto que sempre estiveram ao meu lado me apoiando ao longo de toda a minha trajetória.

Toda a minha gratidão a minha orientadora Ma. Carmen da Silva Martins por todo incentivo e apoio tão importantes. Sem sua ajuda e ensino nada disso seria possível.

Em um mundo que muda rapidamente, a única forma garantida de falhar é não correr riscos. –Mark Zuckerberg.

SUMÁRIO

CRIMES CIBERNÉTICOS: A INEFICÁCIA DA LEGISLAÇÃO BRASILEIRA

Sarah Pereira Ferreira[1]

RESUMO

As tecnologias evoluem de modo acelerado em torno do mundo. Juntamente com esta evolução se faz presente o aparecimento dos crimes cibernéticos, passa a criar novas formas de lesar o usuário, sendo estas, novidades para a legislação. O presente estudo tem como objetivo explanar sobre o meio cibernético, demonstrar a legislação vigente no Brasil.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. Sendo que a Lei nº 12.737/2012 causou interpretações dúbias que facilitaram a impunidade dos crimes, tendo pouca eficácia para punir, juntamente com as lacunas que impossibilitam a aplicação aos delitos cometidos pelos agentes.
Palavras-Chave: Crimes cibernéticos. Internet. Legislação.

ABSTRACT

Technologies are evolving rapidly around the world. Along with this evolution, the emergence of cyber crimes is present, it starts to create new ways of damage the user, and these are new to the legislation. The present study aims to explain and cybernetic environment, to demonstrate the current legislation in Brazil.The study will focus mainly on the most recent legislation on the subject, Law nº. 12,735 / 2012 and Law nº 12,737 / 2012, which deal primarily with the invasion of devices and the exposure of intimate photos and videos, recurrent crimes in the current context of the internet. Since Law nº 12,737 / 2012 caused dubious interpretations that facilitated the impunity of crimes, having little efficacy to punish, together with the gaps that make it impossible to apply to the crimes committed by the agents.

KeyWords: Cyber Crimes. Internet. Legislation.

[1] Acadêmica de Direito da Pontifícia Universidade Católica de Goiás.

INTRODUÇÃO

No presente artigo traz a intenção de estudar os crimes cometidos pelo mundo da internet, tendo em vista com as revoluções tecnológicas. O estudo será executado por meio de pesquisas bibliográficas e com o apoio de artigos da Internet.

Diante do crescimento do uso de sistemas informáticos e da internet no Brasil, nota-se que o ordenamento jurídico não tem acompanhado a dinâmica evolução digital. Torna-se inegável que essas lacunas legais geram insegurança e a impressão de que a impunidade está instalada nos meios digitais.

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

Com o avanço da internet e um dever que o Direito possa acompanhar essa evolução nas relações cibernéticas. A ausência de punibilidade pelo Estado é uma realidade, existe atualmente uma infinidade de crimes virtuais, todavia, em muitos casos ainda não há uma definição especificamente quanto à regulamentação destes crimes, a falta de lei específica para a tipificação dos crimes.

Surgiu a Lei nº 12.737/12 também chamada de Lei Carolina Dieckman, em razão do vazamento das fotos íntimas da atriz. que traz em sua lei a tipificação do crime denominado “Invasão de dispositivo informático”. Entretanto na época houve grande pressão social para que a lei fosse aprovada o mais rápido possível logo percebe-se que não houve grande estudo para a formulação da mesma possuindo , vícios que deixam brechas para impunibilidade.

Logo em seguida 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 sobre os crimes virtuais definiu de forma clara direitos, garantias e responsabilidades para que nos meios digitais. Todavia por mais que pareça ser eficaz ao tratar dos direitos do usuário deixa a desejar.

1.INFORMÁTICA NO MUNDO MODERNO: INTERNET E CRIMES VIRTUAIS

1.1 CARACTERIZANDO A INTERNET

A Internet nasceu de um projeto de pesquisa militar (ARPA: Advanced Research Projects Agency), no período da guerra fria, no final dos anos cinqüenta e início dos anos sessenta.

De acordo com Lima (2000), este projeto surgiu como resposta do governo americano ao lançamento do Sputnik pela ex-União Soviética. Inicialmente a idéia era conectar os mais importantes centros universitários de pesquisa americanos com o Pentágono para permitir não só a troca de informações rápidas e protegidas, mas também para instrumentalizar o país como uma tecnologia que possibilitasse a sobrevivência de canais de informação no caso de uma guerra nuclear.

Conforme Moherdaui (2002, p. 19) diz que: “A internet é um conjunto de recursos tecnológicos que coloca à disposição de qualquer cidadão que possui computador, um modem e uma linha telefônica uma enorme quantidade de informação e possibilidades de acesso a serviços diversificados”.

Nos dias atuais, é impossível pensar no mundo sem a Internet. Ela tomou parte dos lares de pessoas do mundo todo. Estar conectado na rede mundial passou a ser uma necessidade de extrema importância

Atualmente, 4,1 bilhões de pessoas utilizam a rede mundial. O número de usuários corresponde a 53,6% da população de todos o mundo. Sendo que o número de usuários de internet no Brasil em 2019 chegou a 134 milhões, ou 74% da população acima de 10 anos de idade, com 71% dos domicílios com acesso à rede, segundo a pesquisa TIC Domicílios, do Comitê Gestor da Internet (CGI.br).

Conforme a lei 12.965 de 23 de abril de 2014 , que define o que é Internet:

> I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes. A Internet é a tecnologia que permite a comunicação entre pessoas de todos os lugares em tempo real. É a transmissão de dados entre os dispositivos que não estejam necessariamente conectados,

> portanto é possível identificar que a Internet facilita a vida do indivíduo que pretende praticar condutas delituosas.

1.2 CONCEITO E CLASSIFICAÇÃO DE CRIMES VIRTUAIS

Inicialmente, vale destacar que, com os avanços tecnológicos no âmbito da informática, surgiram os nomeados crimes virtuais. Contudo, não existe uma denominação concreta para os crimes dessa espécie, assim, esses delitos são conhecidos também de crimes cibernéticos, crimes de informática, crimes tecnológicos, crimes cometidos por meio eletrônico, crimes digitais entre outros. Nessa perspectiva, assevera Silva:

> [...]que não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. De uma forma ou de outra o que muda é só o nome atribuído a esses crimes, posto que devem ser observados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda deve a conduta ser típica, antijurídica e culpável. (DA SILVA, 2015, p.39).

Para Maia os crimes ciberneticos:

> 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).

O cibe crime nada mais é que todo ato em que o computador ou meios de tecnologia de informação serve para atingir um ato criminoso ou em que o computador ou meios de tecnologia de informação é objeto de um crime. O cibe crime está associado ao fenômeno da criminalidade informacional de condutas violadoras de direitos fundamentais, seja por meio da utilização da informática para a prática do crime ou como elemento de tipo legal de crime. Cosoante a isso no mesmo sentido, destaca 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)

Conclui-se, que crime virtual é a conduta típica, ilícita e culpável que preenche os pressupostos de crime ou de contravenção penal, ocorrida com dolo ou culpa, perpetrada por pessoa física ou jurídica por meio da informática, seja na Rede Mundial de Computadores ou não, e que vai de encontro à segurança do sistema informático, o qual deve observar a integridade, desimpedimento e a privacidade de indivíduos e entidades.

1.3 CRIMES CIBERNÉTICOS PRÓPRIOS E IMPRÓPRIOS

Os crimes virtuais podem ser classificados em crimes próprios e impróprios. Segundo Malaquias:

> [...] Os crimes próprios: são aqueles que necessitam da internet para ser praticado, ou seja está diretamente relacionado com a utilização da tecnologia da informática e comunicação. Para facilitar a compreensão, temse como exemplos enquadrados neste grupo, a criação e disseminação de vírus e outros códigos maliciosos, a negação de serviços, a invasão e a distribuição de dados (público ou privado) e tantos outros atos ilícitos. Os crimes impróprios: são aqueles em que o computador ou a estação de trabalho transforma-se em instrumento para a pratica do delito. Nesse grupo estão inseridos, a título de exemplo, os tipos penais comuns como a calunia, a injuria, a difamação, o furto, o estelionato, a produção, a divulgação e a publicação de fotografias ou imagens contendo pornografia ou cenas de sexo explícito envolvendo crianças ou adolescentes e todos os demais delitos preceituados no código penal e nas leis especiais, possíveis de serem praticados com a utilização dessa citada ferramenta e das novas tecnologias..(MALAQUIAS, 2012, p. 60)

Crimes próprios e aqueles praticados exclusivamente por meio de computadores. 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. Corroborando com esse conceito, valiosas são as lições de Jesus:

> 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. (Jesus apud CARNEIRO, 2012, p 156):

Crimes impróprios utilizado pelo computador e da internet onde o crime se consome no meio virtual mas que produz resultado no mundo físico**.** Do mesmo modo afirma o jurista Jesus:

> 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. (Jesus apud CARNEIRO, 2012, [n.p.]):

1.4 CRIMES CIBERNÉTICOS PURO, MISTO E COMUM

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. O alvo não é o computador, mas os bens da vítima, ou seja, a internet é utilizada como meio para realizar o crime, como, por exemplo, transferências ilícitas de bens e/ou valores. Exemplo*,* cita-se a retirada ilícita de valores monetários de contas bancárias via homebanking.*,*

Tipificado no Código Penal, caracterizando a modalidade de crime cibernético comum que e o acesso a internet e um instrumento para prática de outro delito. Os crimes cibernéticos comuns podem ser cometidos por qualquer pessoa, portanto, são aqueles que utilizam a Internet apenas como instrumento para a realização de um delito já tipificado pela lei penal. (CAPEZ, 2009; SCHMIDT, 2014).
Os crimes contra a honra que no passado se materializavam-se por outros meios, hoje pode se concretizar através da utilização da Internet, sobretudo por meio das redes sociais.

Nos crimes puro o agente criminoso tem a intenção de atingir diretamente o sistema de informação ou os dados de informação inseridas dentro do computador. Para Crespo a distinção fica nítida. Os conceitos de cada um, mesmo antes da lei Carolina Dieckmann já tinha contornos bem definidos:

> crimes digitais próprios ou puros (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (hacking), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas; e crimes digitais impróprios ou mistos (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc.). São exemplos de crimes digitais impróprios os contra a honra praticados na Internet, as condutas que as condutas ilícitas passíveis de penas que se voltem contra os sistemas informatizados e os dados envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil, o estelionato e até mesmo o homicídio. (Crespo,2015,online)

Conforme foi citado acima pode-se dizer que os crimes digitais são tanto os crimes tradicionais, já previstos na legislação, praticados com ajuda da mais moderna tecnologia a internet.

1.5 AGENTES HACKERS E CRACKERS

.

De origem na língua inglesa, o termo *hacker* surgiu por volta de 1990 com a popularização da internet, e significa aquele que se dedica a conhecer e modificar aspectos internos de aplicativos, programas e redes de computadores. Muitos *hackers* são contratados por grandes empresas para testar seus dispositivos de segurança informática.

Os termos "hacker" e "cracker", basicamente, servem para designar indivíduos que possuem habilidades com computadores, porém com finalidades diferentes. Enquanto os hackers elaboram e alteram hardwares e softwares de computadores sem causar prejuízos, os crackers utilizam seus conhecimentos para praticar o cracking, ou seja, quebrando um sistema de segurança.

Os hackres são indivíduos com a capacidade de criar funcionalidades e aplicações para computadores, dispositivos móveis e internet. Eles modificam softwares, hardwares e aplicam seus conhecimentos para desenvolver soluções de segurança, criar ou adaptar novos sistemas. Se definem como indivíduos que utilizam melhorando e desenvolvendo funcionalidades para softwares. A intenção de seus atos nunca é provocar danos, já que seu trabalho é feito de forma legal. Dentro desse grupo estão os profissionais de Tecnologia da Informação (TI), analistas de sistema e outros cargos na área de informática.

Os crackers Também possuem grade conhecimento em códigos, computadores, informática, hardware e software. A diferença entre o cracker e o hacker está no fato de o primeiro utilizar todo conhecimento que possuem para realizar alguma ação maléfica. Esses indivíduos invadem sistemas de segurança de grandes empresas, bancos ou computadores de celebridades com o objetivo de obter informações, dinheiro ou fama. Em alguns casos, os sites das instituições invadidas ficam por várias horas fora do ar.

Costumam quebrar códigos de seguranças de programas, o que faz com que eles se tornem “crackeados”. Já o termo "crack" é usado para se referir a

alguma ferramenta (como aplicativos, links e programas) utilizada por crackers para obter acesso a chaves de registro e licenças de produtos pagos.

Conforme entendimento de Viana, os Crackers possuem distintas classificações, sendo elas:

> Cracker de Sistemas – piratas que invadem computadores ligados em rede.
> Cracker de programas – piratas que quebram proteções de softwer cedidos a título de demonstração para usálos por tempo indeterminado, como se fossem cópias legítimas.
> Phreakers – piratas especialistas em telefonia móvel ou fixa.
> Desenvolvedores de Vírus, Worms e Trojans – programadores que criam pequenos softwares que causam algum dano ao usuário.
> Piratas de Progamas – indivíduos que clonam programas, fraudando direitos autorais.
> Distribuidores de Warez – webmasters que disponibilizam em suas páginas softwares sem autorização dos detentores dos direitos autorais.(Vianna,2001, p 60)

2. CRIMES CIBERNÉTICOS

2.1 CRIMES CONTRA HONRA

Essa modalidade de crime ocorre com mais frequência nos dias de hoje, pois os criminosos são incentivados pela grande possibilidade de anonimato na internet. Isso acontece porque as redes sociais e sites estão em constantes mudanças onde, além de haver a possibilidade de qualquer um utilizar esses meios, ainda há a possibilidade de não se identificar corretamente utilizando-se de nomes fictícios.

O Código Penal brasileiro em seu Capítulo V, Título I da Parte Especial dispõe sobre: ‘‘Os Crimes Contra a Honra’’. Tem como garantia fundamental pela Constituição da República Federativa do Brasil, que em seu artigo 5.º, inciso X, instituiu que “são invioláveis a intimidade, a vida privada, a honra é a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Honra é, portanto, um direito fundamental do ser humano, protegido constitucionalmente e penalmente. Segundo Nucci (2014 p.3) ‘‘honra “é a faculdade de apreciação ou o senso que se faz acerca da autoridade moral de uma pessoa, consistente na sua honestidade, no seu bom comportamento, na sua respeitabilidade no seio social, na sua correção moral”.

Divide-se em dois aspectos, o subjetivo e o objetivo conforme ensina Luis Regis Prado(2015, p 764 – 765)

> A honra, do ponto de vista objetivo, seria a reputação que o indivíduo desfruta em determinado meio social, a estima que lhe é conferida; subjetivamente, a honra seria o sentimento da própria dignidade ou decoro. A calúnia e a difamação atingiriam a honra no sentido objetivo (reputação, estima social, bom nome); já a injúria ofenderia a honra subjetiva (dignidade, decoro).

A honra constitui um bem jurídico e deve ser protegida, inclusive no âmbito do Direito Penal. Dentre os crimes contra a honra, pode-se destacar os principais: a calúnia, difamação e injúria.

Essas condutas podem ser praticadas por meios diversos, inclusive com a utilização da rede mundial de computadores. Atualmente, as redes sociais são o espaço mais fértil para que esse tipo de ataque ofensivo aconteça. Isso porque a internet traz a falsa sensação ao agressor ou criminoso de que as ofensas não serão reconhecidas, dada a possibilidade de anonimato da rede. A realidade, felizmente, é outra.

O dolo configura-se como elemento subjetivo dós Crimes Contra Honra, podendo ocorrer em quaisquer de suas modalidades seja ele direto ou mesmo eventual. Há necessidade, portanto, da intenção do agente em atingir a honra objetiva (calúnia e difamação), ou a honra subjetiva (injúria).Não há previsão portanto da modalidade culposa neste delito.

Crimes que violam a honra são elencados no código pelo código penal em três modalidades: a calúnia (art. 138 CP) a difamação (art. 139 CP)e a injúria (art.140 CP)

A calúnia caracteriza-se no ato de um a pessoa imputar, atribuir a outrem um a conduta criminosa que este não tenha cometido.

Calúnia está prevista no art. 138 do Código Penal que diz:

> **Art. 138** - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> **§ 1º** - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> **§ 2º** - É punível a calúnia contra os mortos.
> Exceção da verdade
> **§ 3º** - Admite-se a prova da verdade, salvo:

> **I** - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
> **II** - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;
> **III** - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

O crime ocorre quando a conduta típica de imputar, de forma falsa e dolosa, a prática de um fato determinado, definido com o crime, a alguém, maculando a imagem dessa pessoa perante a sociedade.

Crime de difamação é o simples fato de imputar qualquer adjetivo que ofenda a reputação de individuo determinado. Este crime ofende a honra objetiva do individuo por meio de um terceiro, que é o sujeito ativo do crime, sendo que este terceiro macula a reputação do individuo perante a sociedade.

A difamação esta tipificada no código penal no art. 139 que dispõe:

> **Art. 139** - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
> Exceção da verdade
> **Parágrafo único** - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

Injúria atinge a honra subjetiva, ou seja, ofende a dignidade e o decoro íntimo do indivíduo, fato este que não precisa levar em conta se um terceiro tom ou conhecimento ou não, basta que o ofendido tenha se sentido menosprezado, ultrajado por quem proferiu esta ação

A injúria esta tipificada no art. 140 do CP:

> **Art. 140** - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.
> **§ 1º** - O juiz pode deixar de aplicar a pena:
> **I** - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
> **II** - no caso de retorsão imediata, que consista em outra injúria.
> **§ 2º** - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
> Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.
> Pena - reclusão de um a três anos e multa.

A dignidade da pessoa quando é ofendida pela injúria ocorre sempre com os valores morais sendo atingidos, e quando ocorre um a ofensa ao decoro nada mais é do que a estrutura física e intelectual do injuriado.

2.2 INVASÕES INFORMATICA

O tipo penal de “Invasão de Dispositivo Informático”, previsto no art. 154-A e 150-B do Código Penal, inserido no capítulo VI, Dos Delitos contra a Liberdade Individual, na seção IV, Dos Crimes contra a Inviolabilidade dos Segredos, descreve como conduta ilícita:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com 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.

Qualquer pessoa pode praticar o crime de invasão de dispositivo informático, uma vez que o delito não exige nenhuma condição especial. Já o sujeito passivo pode ser o proprietário do aparelho informático invadido ou qualquer outra pessoa que tenha inserido informação ou dados neste dispositivo.

A conduta necessária para a configuração do delito consiste no ato de ‘’invadir’’ que significa ingressar virtualmente, sem a concordância expressa ou tácita do proprietário do dispositivo. O objeto material do crime é o dispositivo informático alheio que pode ser um computador, notebook, tablet, smartphone, pen drive.

Conforme Sydow a princípio parecem ter sido descritas as seguintes 4 (quatro) condutas típicas, no caput:

> Devassar dispositivo informático alheio - conectado ou não à rede de computadores — mediante violação indevida de mecanismo de segurança, com o fim de obter dados ou informações sem autoriza- do titular do dispositivo;
> Devassar dispositivo informático alheio - conectado ou não à rede de computadores — mediante violação indevida de mecanismo de segurança, com o fim de adulterar dados ou informações sem autorizaçâo do titular do dispositivo;
> Devassar dispositivo informático alheio - conectado ou não à rede de computadores — mediante violação indevida de mecanismo de segurança, com o fim de destruir dados ou informações sem autorizaçâo do titular do dispositivo;
> Devassar dispositivo informático alheio - conectado ou não à rede de computadores — mediante violação indevida de mecanismo de segurança, com o fim de instalar vulnerabilidades para obter Vantagem ilícita; OU simplesmente instalar vulnerabilidades para obter vantagem ilícita.(SYDOW,2021, p 441)

Nesse ponto de vista Sydow relata que em suma há duas categorias de delito, classificada de acordo com diferentes finalidades tipificadas sendo: a Invasão de dispositivo informático com a finalidade de obtenção, adulteração ou destruição

de dados ou sistema de informações. Invasão de dispositivo informático com a finalidade de instalar vulnerabilidade para obter vantagem ilicíta.

2.3 PORNOGRAFIA INFANTO JUVENIL

Pedofilia e uma espécie de parafilia estão entre as doenças classificadas pela Organização Mundial de Saúde (OMS) entre os transtornos da preferência sexual. Pedófilos são pessoas adultas (homens e mulheres) que têm preferência sexual por crianças geralmente pré-púberes (que ainda não atingiram a puberdade) ou no início da puberdade, de acordo com a OMS. Conforme o Dicionário Aurélio, pedofilia é a ‘‘parafilia representante por desejo forte e repetido por praticas sexuais e de fantasias sexuais com crianças pre-púberes; perversão sexual que visa á criança’’.

A legislação brasileira não possui nenhum dispositivo que traga como típica a conduta de desejo forte e repetido, nem de fantasias sexuais com crianças, considerados atos internos não puníveis, mas tão somente outra figura mais específica prevista no Estatuto da Criança e do Adolescente, estes atos exteriorizados.

O fato por si só de ser pedófilo não gera tipicidade penal, já que não existe qualquer tipo de previsão legal. A tipificação penal ocorre quando exterioriza o seu desejo vindo a consumar os crimes de abuso sexual ou apresentar imagens com pornografia ou cena de sexo envolvendo crianças ou adolescentes conforme o art. 241 do ECA.

A criminalização do acesso e do download de imagens contendo pornografia infanto-juvenil não se encontram configuradas como tipo penal, o que inibe a ação persecutória no que tange a determinados atos preparatórios, mas de outro lado quando o agente conclui o download ele transforma em posse, não havendo imediata destruição, concretiza-se o tipo descrito no art. 241-A do Estatuto da Criança e do Adolescente.

Pornografia infantil é crime no Brasil, passível de pena de prisão de dois a seis anos e multa. Segundo o art. 241, do Estatuto da Criança e do Adolescente (Lei nº 8.069/90):

> Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores (internet),

> fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente.

O código penal, em seu artigo 234, versa:

> Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno: Pena – detenção, de 6 (seis) meses a 2 (dois) anos, ou multa. Parágrafo único. Incorre na mesma pena quem: I – vende, distribui ou expõe à venda ou ao público qualquer dos objetos referidos neste artigo; II – realiza, em lugar público ou acessível ao público, representação teatral, ou exibição cinematográfica de caráter obsceno, ou qualquer outro espetáculo, que tenha o mesmo caráter; III – realiza, em lugar público ou acessível ao público, ou pelo rádio, audição ou recitação de caráter obsceno.

Tal raciocínio segundo jurista Sydow leva a conclusão de que 5 são as espécies de atores envolvidos com o crime de pornografia infantil de nossa legislação penal:

> 1, O distribuidor de material relacionado a crianças e adolescentes em cenas de pornografia explícita, mas que não tem interesse no consumo do material e também não o produz; (DISTRIBUIDOR-NÃO CONSUMIDOR-NÃO PRODUTOR).
> 2. O distribuidor de material relacionado a crianças e adolescentes em cenas de pornografia explícita, que tem interesse no consumo do material mas não 0 produz; (DISTRIBUIDOR-CONSUMIDOR-NÃO PRODUTOR).
> 3. O distribuidor de material relacionado a crianças e adolescentes em cenas de pornografia explícita, que tem interesse no consumo do material e 0 produz; (DISTRIBUIDOR-CONSUMIDOR-PRODUTOR).
> 4, O produtor de material relacionado a crianças e adolescentes em cena de pornografia explícita mas que não o distribui. (NÃO DISTRIBUIDOR-CONSUMIDOR-PRODUTOR).
> 5. O consumidor de material relacionado a crianças e adolescentes em cena de pornografia explícita que não tem interesse em distribuí-lo e não 0 produz. (NÃO DISTRIBUIDOR-CONSUMIDOR-NÃO PRODUTOR).(SYDOW,2021,p 589)

Para a lei Brasileira, todas as formas acima possuem tipificação penal. Entretanto ainda há uma situação de impunidade que a possibilidade de haver o consumo sem armazenamento.

O marco jurídico de proteção e reconhecimento dos direitos das crianças e adolescentes surgiu com a Constituição Federal de 1988, que trata os menores com prioridade por estes apresentarem pouca ou nenhuma capacidade de defesa. A Lei 8.069/90 do Estatuto da Criança e do Adolescente (ECA) reforça tal princípio constitucional no sentido de abordar os seus direitos e garantias fundamentais e

considerá-los como sujeitos de direitos para que eles não sejam tratados como seres inferiores pela sua condição de dependência. Visando prevenir ainda mais os menores, surgiu também a Lei 10.764/03 que modifica o art. 241 do ECA. Observando a grande incidência do crime ainda com tais avanços jurídicos, foi sancionada a Lei 11.829/2008 (resultado da CPI da pedofilia) que intensificou a proteção infantil visando aprimorar o combate à produção, venda e distribuição de pornografia infantil, criminalizando a aquisição do material e várias condutas de pedofilia na Internet. A identificação do endereço IP do usuário do computador, que realizou as operações criminosas na web, vai contribuir para se buscar a identidade do agente.

2.4 EXPOSIÇÃO DA INTIMIDADE SEXUAL

Conforme Danielly Dias Fernandes diz a lei 13.772, é de origem da Câmera dos Deputados, de autoria do Deputado João Arruda, e trata-se da evolução do PCL nº 18 de 2017. Alterou o Código Penal inserindo uma letra B no artigo 216 e criou o tipo penal de “Exposição de Intimidade Sexual”, além de criar um capitulo 1-A. Alterou também a lei Maria da Penha, em seu artigo 7º, incluindo a violação de intimidade sexual como violência psicológica.

A divulgação de imagens íntimas de alguém sem autorização, também chamada de pornografia não consensual, tornou-se um problema importante nos últimos anos. Isso porque inúmeras mulheres já sofreram com as suas consequências, tendo-se notícia, inclusive, de suicídios decorrentes dessa exposição difamatória. Assim, cyber revenge, revenge porn, pornografia de revanche e pornografia de vingança são as nomenclaturas mais utilizadas atualmente para se referir à prática de divulgação de imagens (fotos e vídeos) de pessoas em situações eróticas e/ou sexuais, sem o consentimento das mesmas.

A prática inclui a divulgação por meio da Internet tanto de imagens obtidas sem o conhecimento da vítima como de imagens obtidas consensualmente ou mesmo produzidas pela própria vítima, no âmbito de uma relação íntima anterior entre vítima e agressor, em redes sociais, sites específicos de publicação de imagens íntimas sem consentimento e mediante o compartilhamento em serviços de mensagens instantânea

Publicar foto ou vídeo intima sem consentimento conteúdo por qualquer meio de comunicação se tornou crime com a Lei nº 13.719/18 e prevê pena de um a cinco anos de reclusão, podendo ser aumentada.

2.5 ESTELIONATO

Não existe no ordenamento jurídico no qual o estelionato praticado por meio virtual diferente do estelionato comum. Agindo no virtual usando de armadilhas e golpes com intuito de obter vantagem patrimonial. A internet facilitou o acesso à informação e consequentemente a obtenção de informações, que atualmente são usadas para cometer delitos.

O estelionato é uma das práticas de crime mais popular, o número de pessoas que tentam adquirir para si ou para outras vantagens ilícitas, aumenta tanto com o uso da internet quanto fora dela. As condutas variam conforme os meios eletrônicos disponíveis. O código penal em seu artigo 171 assevera que:

> Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.

O estelionato é consumado quando há o alcance da vantagem ilícita, havendo prejuízo alheio, frisando-se a última parte, que é necessário haver o prejuízo alheio.

Outro golpe é o truque de confiança os golpista fazem esquemas específicos que geram uma credibilidade segundo Spencer ideia é convencer o internauta de que aquele site ou aquela mensagem enviada trata de um assunto verdadeiro é que há necessidade de atenção por parte do leitor. Tais ardis buscam convencer o usuário a ser vitimizado de acordo com uma série de argumentos, dentre eles:

> a)Fatos tristes: como em casos de mensagens que contem relatos de pessoas doentes, precisando de tratamento, fotos de crianças com deformidades que teoricamente precisam de operação ou remédios caros e que, portanto, precisam de doações em dinheiro;
> b) Oportunidade única para o usuário - é o caso dos denominados gold bricks schemes ou estelionatos económicos em que a pessoa recebe uma

> oferta de compra de açóes, produtos, serviços, vouchers etc que precisam ser completadas nas próximas horas ou a vítima perderá a chance.
> c) Fatos de utilidade pública: identifica-se um programa ou açao governamental e utiliza-se tal pretexto para convocar pessoas a se inscreverem ou pagarem antecipadamente para usufruir da vantagem.
> d) Fatos geradores de curiosidade: busca-se um fenómeno ocorrido recentemente como um acidente ou uma catástrofe e convida-se o usuário para clicar para ver as fotos ou contribuir com instituições de amparo e salvaguarda.
> e)Instituições confiáveis: apresenta-se ao usuário como instituição confiável ou marca conhecida e apresenta-se uma situação como necessidade de confiança de senha, dividida não paga, cadastramento de dados ou um problema.

Com o objetivo convencer a pagar um boleto, fazer deposito ou transferir valores, ceda senha e dados bancários ou de cartão de credito, clique em link que instala um dispositivo espião.

3. LEGISLAÇÃO APLICÁVEL AOS CRIMES CIBERNÉTICOS

3.1 ANALISE DA LEI 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. 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

Lei 12.737 de 30 de novembro de 2012, também conhecida popularmente como ‘‘Lei Carolina Dieckmann’’, *que* deu origem ao crime de invasão de dispositivo informático a qual se encontra prevista no art. 154-A do CPB. Sendo a primeira lei a dispor de modo específico sobre crimes cibernéticos. trouxe 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:32
> 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)

Com o fim de tutelar os crimes informáticos puros, no entanto esta lei é deficiente em alguns pontos, especialmente por não preverem forma de violência moral nas condutas praticadas pelos crimes cibernéticos.

Com o caso da atriz Carolina Dieckmann estando com grande pressão na mídia, sociedade acabou mobilizando para que lei fosse aprovada rapidamente. Podendo perceber que este e um dos motivos da lei apresentar tantas falhas, deixando a população desprotegida em relação a crimes virtuais sendo que era necessária uma elaboração mais panejada por juristas e especialistas desta mesma área.

Nota-se que grande parte da ineficácia da lei 12.737/2012 está na previsão que o art. 154-A do Código Penal faz ao retratar que só existirá crime se houver violação de dispositivo de segurança. Ou seja, quando a vítima não possuir antivírus, firewalls ou qualquer outro meio que torne seguro seu dispositivo eletrônico e mesmo assim este for violado virtualmente, tal ato não será enquadrado como invasão de dispositivo informático, pois se faz necessário ter ultrapassado algum tipo de mecanismo de segurança.

Como exemplo desta situação tem-se a vítima que tiver um computador desprovido de senha, caso ela tenha seus dados invadidos, o autor desta ação não poderá ser punido por meio da referida lei, visto que, não existiu a violação do mecanismo de segurança necessário para caracterizar o crime.

Outro fato que não se considera como crime do artigo 154-A do Código Penal, ocorre quando um colega de trabalho compartilha o computador com outro e descobre informações ou fotos deste e as divulga. Nessa situação, mesmo que existisse o mecanismo de segurança no computador do trabalho, o agente não teve que ultrapassá-lo, descaracterizando a figura do crime.

Diversas são as formas que podem ocorrer a invasão de dispositivo eletrônico sem que o indivíduo responsável seja penalizado. Sendo dessa forma não são penalizados , por pura deficiência do texto de lei. Outro ponto e que os delitos de natureza cibernética necessitam de provas, mais especificamente de perícia, uma vez que não há como conseguir testemunha para esse tipo de crime.

Logo depois houve 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.

3.2 MARCO CIVIL DA INTERNET

O Marco Civil foi apresentado como um Projeto de Lei à Câmara dos Deputados, em 2011, sob o número PL 2.126/2011, apensado ao PL 5.403/2001. Foi fruto de sugestões da sociedade por consulta pública do Ministério da Justiça. Sua sanção se deu após um dia de sua aprovação no Senado Federal, durante a abertura do Encontro Multissetorial Global sobre o Futuro da Governança da Internet – NETmundial, que reuniu representantes de mais de 80 países em São Paulo, e

ganhou repercussão positiva em várias partes do mundo. Por fim, em 23 de abril de 2014, a Lei nº 12.965 foi aprovada, estabelecendo princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Também conhecida como Constituição da Internet Brasileira, a lei tem por objetivo central disciplinar a relação entre empresas operadoras de produtos ou serviços associados à internet e os seus respectivos usuários dentro do território nacional.

O texto normativo do Marco Civil da Internet estabelece que sejam respeitados princípios como a liberdade de expressão, pluralidade, diversidade, abertura, colaboração, exercício de cidadania, proteção à privacidade, dados pessoais, livre iniciativa, livre concorrência e defesa do consumidor. Em contraposição, por serem objeto de outras normas especificas, não trata diretamente de temas como cibercrimes, comércio eletrônico, direito autoral, expansão da banda larga e regulamentação setorial das telecomunicações.

Esta lei foi criada com o objetivo de preencher as lacunas existentes no sistema jurídico em relação aos crimes virtuais, abordando primeiramente e enumerando todos os direitos do usuário, tratando de todos os tipos de assuntos como solicitar os arquivos pessoais de navegação, bem como solicitar a atuação do pode público perante estes crimes, garantindo ao cidadão o direito de usar a internet de maneira autônoma sem ter nenhum tipo de prejuízo estando protegido a todo tempo.

A Lei n° 12.965/14, mais conhecida como o Marco Civil da Internet, veio a ratificar as garantias constitucionais, não vindo a tipificar qualquer conduta criminosa, apenas tendo a ideia que a mesma seja a Constituinte da Internet Brasileira e possui em seu conteúdo ampla gama de pontos relevantes referentes aos direitos e garantias, como descreve Cassanti (2014, p. 91-92):

> Remoção de conteúdo: Segundo o Marco Civil, os provedores de conexão à internet não serão civilmente responsáveis por danos relacionados ao conteúdo gerado por terceiros (essas empresas não responderão na Justiça pelo conteúdo publicado por seus usuários. Isso só acontecerá, após ordem judicial, a empresa não tome as providências para tornar o conteúdo indisponível. Dados pessoais: O Marco Civil assegura ao internauta o direito ao sigilo de suas comunicações via internet (salvo por ordem judicial); informações claras e completas dos contratos de prestação de serviço; não fornecimento a terceiros de seus registros (...) Neutralidade da rede: Este item propõe que o responsável pela transmissão do conteúdo deve tratar de forma igual quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino. É a chamada neutralidade da rede

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 conforme no artigo 13 e 15.

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).

O Marco Civil deixa a desejar, por mais que pareça ser eficaz ao tratar dos direitos do usuário. O ato de introduzir ferramentas judiciais do mundo físico como a obtenção de ordem judicial, no mundo virtual é contra produtivo, uma vez que as velocidades entre os dois mundos são incompatíveis, enquanto o primeiro é muito devagar, o segundo requer cada vez mais agilidade. Desta maneira, reforça-se ainda mais a urgência em uma inovação jurídica na legislação, no que conduz os crimes cibernéticos.

3.3 LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados Pessoais (LGPD) um complemento ao marco civil da internet no que tange tratamento de dados pessoais, atende necessidades atuais de segurança e proteção de dados on-line e off-line, indicando

figuras envolvidas, suas responsabilidades e penalidades, tendo como impacto maior também.

Ela foi inspirada na GDPR (General Data Protection Regulation), que entrou em vigência em 2018 na União Europeia, trazendo grandes impactos para empresas e consumidores.

Lei 13.709, de 14 de agosto de 2018, entra em vigor em agosto de 2020 tem como objetivo regulamentar dados dos brasileiros como são tratados, armazenados e protegidos pelas empresas, uma vez que os dados pessoais ganharam grande importância na economia moderna, pois permitem fazer predições, analisar perfis de consumo, opinião, entre outras atividades. Prevendo punições para descumprimento em caso de vazamentos, ou outras irregularidades.

A LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Tem como objetivos: Proteção à privacidade; liberdade de expressão, informação, comunicação e opinião; Inviolabilidade da intimidade honra e da imagem; desenvolvimento econômico, tecnológico e inovação; livre iniciativa, livre concorrência e a defesa do consumidor; direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania.

Os agentes de tratamento, âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois agentes de tratamento, o controlador e o operador. O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Já o operador é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

A mesma protege dados pessoais são aqueles em que possível identificar diretamente ou indiretamente um individuo vivo: nome, RG, CPF, gênero, data de nascimento entre outros.

Endereço de IP do usuário, assim como dados como cookies e informações sobre o hábito de consumo que o usuário tenha vinculado aos seus perfis on-line são classificados como dados pessoais.

CONCLUSÃO

As novas tecnologias exigem que os operadores do Direito se preparem para as novas realidades, que demandam aberturas de pensamentos é decisões capazes de conciliar os interesses em jogo, sobretudo diante da evolução tecnológica que ocorre em velocidade surpreendente, sem a correspondente evolução da legislação e do pensamento jurídico.

Todo dia surge um dispositivo novo, uma possibilidade nova de crime a ser cometido através da internet, e isso é um grande problema, pois não se pode punir alguém sem lei anterior que defina o crime que foi praticado, portanto, se for uma conduta nova o usuário se torna impune, pois não existe regulamentação sobre o ocorrido.

O Brasil encontra-se atrasado no âmbito jurídico, mas em evolução nas criminalidades executadas por meios virtuais, necessitando-se se igualar as nações que já possuem legislação especial voltada aos crimes virtuais.

Poucas normas específicas que versem sobre a proteção contra os crimes virtuais dificultam a ação do Estado que 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.

Assim, a partir das observações efetuadas ao longo deste trabalho, constatou-se a falta de uma legislação específica aos crimes cibernéticos no Brasil traz, em muitos casos, a impunidade dos criminosos, logo que determinadas condutas não são tipificadas é as que são, tal como a lei nº 12.737/12, traz lacunas é dúbias interpretações que facilitaram a impunidade dos crimes. Com o grande avanço tecnológico e o aumento usuários, é indispensável a criação de uma lei que defina as condutas criminosas praticadas no meio virtual, com penas destinadas aos seus agentes proporcionais aos resultados delituosos que estes produzem.

A nova legislação precisava ser mais aprimorada para que se diminuísse a incidência dos crimes cibernéticos, para garantir a segurança virtual junto com a tutela do direito penal brasileiro. Evitando assim novas brechas, não deixando a impunidades dos infratores de crimes virtuais.

REFERÊNCIAS

ANTÔNIO, Roberto Darós Malaquias. **Crimes cibernéticos e prova: a investigação criminal em busca da verdade**. Curitiba: Juruá, 2012, p. 60.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília,DF,23 abr,2014 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 03 de abril de 2021.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.**Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em: 04 de abril de 2021.

BRIGATTO, Gustavo**. Acesso à internet cresce no Brasil, mas 28% dos domicílios não estão conectados**. 27 maio, 2020. Disponivel em: https://nic.br/noticia/na-midia/acesso-a-internet-cresce-no-brasil-mas-28-dos-domicilios-nao-estao-conectados. Acesso em: 11 de outubro de 2020.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. Âmbito Jurídico, Rio Grande, XV, n.99, abr. 2012. Disponível em:<http://www.ambitojuridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17>. Acesso em: 12 de outubro de 2020.

CASTRO, Aldemario Araujo. **A internet e os tipos penais que reclamam ação criminosa em público**. Disponível em: http://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf. Acesso em: 13 de outubro de 2020.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. 1. ed. Rio de Janeiro: Brasport, 2014.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.90.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais: do que estamos falando?**. Diaponivel em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/. Acesso em: 14 de outubro de 2020.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Três em cada quatro brasileiros já utilizam a Internet, aponta pesquisa TIC Domicílios 2019**. Disponivel em : https://cgi.br/noticia/releases/tres-em-cada-quatro-brasileiros-ja-utilizam-a-internet-aponta-pesquisa-tic-domicilios-2019/. Acesso em: 10 de outubro de 2020.

DA SILVA, Patrícia Santos. **Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais**. Brasília: Vestnik, 2015.

FERNANDES, Danielly Dias .**Aplicabilidade da Lei 13.772/2018 no Ordenamento Jurídico Brasileiro.** Disponível em : https://daniellydiasfernandesadv.jusbrasil.com.br/artigos/1139747475/aplicabilidade-da-lei-13772-2018-no-ordenamento-juridico-brasileiro. Acesso em: 5 de fevereiro de 2021.

JESUS, Damásio de Milagre, Celso Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva. 2016. Pag. 49

MOHERDAUI, Luciana. **Guia de estilo web produção e edição de notícias on-line.** 2. ed. rev.e ampl. São Paulo: Editora SENAC São Paulo, 2002.

NUCCI, Guilherme de Souza**. Código Penal comentado**. 14. ed. Rio de Janeiro: Forense, 2014.

ONU NEWS. **Estudo da ONU revela que mundo tem abismo digital de gênero.** Disponivel em: https://news.un.org/pt/story/2019/11/1693711. Acesso em: 11 de outubro de 2020.

PRADO, Luiz Regis. **Curso de direito penal brasileiro**. 14. ed. São Paulo: Revista dos Tribunais, 2015, p. 764-765.

PINHEIRO, Patrícia Peck. **Direito digital**. 4. ed. São Paulo: Saraiva, 2010.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático**. 2 ed. Salvador: Editora JusPodvim, 2021.

VIANNA, Túlio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos de Direito Penal Infórmatico.** Belo Horizonte. 2001.