Data de aprovação: 14/12/2021

A MODERNIZAÇÃO DOS CRIMES EM VIRTUDE DO CRESCIMENTO DA INTERNET

Raimundo Inácio da Silva Filho[1]
João Batista Machado Barbosa[2]

RESUMO

O presente estudo parte de uma análise da mudança da sociedade, devido ao desenvolvimento de tecnologias capazes de conectar várias pessoas de diferentes locais, em uma única rede mundial de computadores. Desse modo, a internet se demonstrou uma ferramenta essencial para o desenvolvimento dos seres humanos, visto que, barreiras foram quebradas devido à grande facilidade que o ambiente digital nos proporcionou, sendo possível em apenas alguns cliques o envio de mensagem para pessoas do outro lado do mundo, assim como, a transferência de dinheiro por meio da internet, e dentre várias outras mudanças que o ambiente digital nos proporcionou. Por se tratar de um ambiente aberto e diversificado, contribuiu para o desenvolvimento da sociedade, porém, existem pessoas que se utilizam dessa qualidade do ambiente digital para praticar crime. Nesse sentindo, o trabalho irá versar sobre o desenvolvimento do ambiente cibernético até o desenvolvimento das condutas práticas na Internet, além de demonstrar meios necessários para uma maior segurança no ambiente digital. Com isso, é necessário um aperfeiçoamento em determinados pontos do nosso ordenamento jurídico que tratam sobre os crimes cibernéticos, de modo que sejam um pouco mais severas, com a finalidade de inibir determinadas condutas delituosas que são praticadas no ambiente digital, de forma que a pena se enquadre ao dano causado a vítima, visto que, em determinados casos os danos causados no ambiente digital são superiores ao mundo físico.

Palavras-chaves: Crime Digital. Internet. Convenção de Budapeste. Globalização.

[1] Acadêmico do Curso de Direito do Centro Universitário do Rio Grande do Norte (UNI-RN). E-mail: raimundoinacio89@gmail.com
[2] Professor Mestre. Orientador do Curso de Direito do Centro Universitário do Rio Grande do Norte (UNI-RN). E-mail: jbmb@uol.com.br

THE MODERNIZATION OF CRIMES DUE TO THE GROWTH OF THE INTERNET

ABSTRACT

The present study starts from an analysis of the changes in society, due to the development of technologies capable of connecting several people from different places, in a single worldwide computer network. Thus, the internet has proven to be an essential tool for the development of human beings, since barriers have been broken due to the great ease that the digital environment has provided us, being possible in just a few clicks to send messages to people on the other side of the world, as well as to transfer money over the internet, and among several other changes that the digital environment has provided us with. Because it is an open and diverse environment, it has contributed to the development of society. However, there are people who use this quality of the digital environment to commit crimes. In this sense, the paper will focus on the development of the cybernetic environment until the development of the practical conducts on the Internet, and will also show the necessary means for a better security on the digital environment. Thus, it is necessary to improve certain points of our legal system that deal with cybercrime, so that they are a little more severe, with the purpose of inhibiting certain criminal conducts that are committed in the digital environment, so that the penalty fits the damage caused to the victim, since, in certain cases, the damage caused in the digital environment is greater than in the physical world.

Palavras-chaves: Digital crime. Internet. Budapest Convention. Globalization.

1. INTRODUÇÃO

No mundo cada dia mais tecnológico, devido à rápida e crescente evolução da informática e da globalização, à vida das pessoas acabaram sendo facilitadas, visto que, as relações entre os povos se tornaram mais comuns. Isso ocorre devido ao desenvolvimento de tecnologias capazes de reduzir a distância entre os povos fossem capazes de quebrar a barreira da distância, de modo que apenas com acesso a uma rede de internet e um único clique o usuário possa enviar uma mensagem para alguém do outro lado do globo terrestre.

Desse modo, o desenvolvimento da tecnologia colaborou para a população ter novos recursos que facilitam na vida dos usuários, como, a procura por informações, diversão, compras, vendas e até mesmo relações entre os povos, essas são as atividades mais comuns praticadas no ambiente digital. Nada obstante, alguns usuários se utilizam desses meios fornecidos pelo ambiente digital para praticarem atitudes delituosas.

Diante disso, surgiu uma nova área das relações sociais em que ocorreu a necessidade de os países atuarem, visto que, é um ambiente propício a relações de consumo, comunicação, divulgação, dentre outras coisas. Nesse sentido, surgiu a necessidade da legislação brasileira em geral, criar mecanismos para arguir sobre as demandas da internet, indo desde as relações normais dos seres humanos, como por exemplo, a compra e venda até os crimes praticados através da internet.

Dessa forma, ocorreram alterações no ordenamento jurídico brasileiro, com o objetivo de trazer uma segurança maior para os usuários da internet, porém, é perceptível que apesar das leis que trazem uma certa segurança para os indivíduos que se utilizam do meio digital, é algo novo e ainda falta um longo caminho para percorrer até que se tenha realmente uma segurança nos ambientes digitais. Isso se deve ao fato que a internet é um ambiente vasto e ainda muito novo, no qual, é de difícil acompanhamento por parte do ordenamento jurídico, visto que, este se desenvolve de modo lento, o qual dificulta em uma maior segurança jurídica para os usuários que se utilizam dos meios digitais para vendas, compras, relações pessoais, dentre outros...

A legislação ainda carece de segurança jurídica, mas como veremos no decorrer do presente trabalho, existem algumas leis e artigos que abordam sobre tal tema, embora não possuam eficiência necessária para punir os que praticam crimes no ambiente virtual.

Assim, o presente trabalho tem a seguinte problemática: a falta da segurança no ambiente cibernético devido à ineficácia da atual legislação em combater determinados crimes digitais.

Dessa forma, o presente trabalho tem como objetivo principal demonstrar a ineficácia da legislação em determinados crimes. No que se refere aos objetivos específicos, ateve-se aos seguintes: definir os crimes digitais, pontuar os principais crimes digitais, analisar a legislação que trata sobre os crimes cibernéticos, comparar a legislação de outros Estados.

Para isso, foi utilizado a pesquisa bibliográfica, visto que, se buscou investigar conhecimento técnico nessa nova área dos interesses sociais e jurídicos, também como, o posicionamento sobre este atual tema. A técnica de pesquisa utilizada foi a bibliográfica e documental, no qual, consiste na coleta de informações e análises de materiais que já foram produzidos a respeito desse atual tema, o qual, foi assumido como tema de pesquisa científica.

2. FORMAÇÃO DA SOCIEDADE DA ERA DIGITAL

Observa-se que, onde existem sociedades humanas, ocorre, no decorrer dos anos, uma verdadeira revolução cultural, social e econômica, de modo que transformou totalmente os conceitos de fronteiras entre telecomunicações, informações e meios de comunicações.

Desse modo, expõe Castel (2001), que o final do século XX foi um período em que teve a possibilidade de vislumbrar acontecimentos sistemáticos que, quando analisados em sua amplitude, penetrabilidade e alcance social, poderiam ser caracterizados como uma verdadeira revolução, tais quais ocorreram anteriormente na Revolução Industrial e no Renascimento, todavia, nestes tempos, a revolução teve por objeto principal um bem completamente distinto: a informação. Tal objeto passou a ser reconhecido como um bem com total centralidade nas sociedades humanas, de modo que, passaram a fluir com velocidade e em quantidades antes inimagináveis, assumindo valores sociais e econômicos jamais antes considerados.

Conforme explica Barreto Jr. (2007, p. 2):

> Convencionou-se nomear este novo ciclo histórico de Era da Informação, cuja mais distinta peculiaridade inerente às sociedades humanas vincula-se à existência de complexas redes profissionais e tecnológicas, voltadas à produção e ao uso da informação, que passa a ser considerado um bem valioso, utilizado para gerar conhecimento e riqueza.

2.1 SURGIMENTO DA INTERNET

A internet consiste em um sistema de redes de computadores que estão interconectados, com mais de 4 bilhões de usuários. Os computadores pessoais ou de escritório/locais, tem acesso à internet por meio de provedores de acesso, que se ligam a redes regionais que, por sua vez, se unem a redes nacionais e internacionais.

Desse modo, por existir um sistema que deixam todos os usuários conectados em uma grande e complexa rede, é possível enviar mensagens por meio dessas redes até chegar ao seu destino, independentemente dele está do outro lado do mundo em relação a sua localização. Isso devido à aparelhos chamados de roteadores, que são instalados em diversas partes da Rede, o qual, estão encarregados de determinar qual a rota mais adequada.

A internet atual, só foi ser idealizada por volta dos anos 60, de início, foi utilizado como uma ferramenta de comunicação militar, o qual, precisava de algo que resistisse a um conflito nuclear mundial. Desse modo, um grupo de programadores e engenheiros, contratados pelo Departamento de Defesa dos Estados Unidos, desenvolveu o conceito de uma rede sem nenhum tipo de controle central, por onde passariam as mensagens divididas em pequenas partes, o qual, foram nomeadas de ‘’pacotes’’. Nesse sentido, as informações teriam uma maior flexibilidade, segurança e rapidez, onde o computador seria apenas um ponto, visto que, independentemente daquele computador ser destruído não iriam causar um dano as informações passadas e nem futuras porque não iria interromper o fluxo das informações.

Apenas em 1969, por meio de uma comunicação entre a Universidade da Califórnia e um centro de pesquisa em Stanford, entrou em operação a ARPAnet (Advanced Research Projects Agency Network), de início conseguiram ligar quatro computadores, com o passar do tempo, mais computadores foram reunidos em um único sistema todos pertences a outras universidades, centros de pesquisas com a finalidade militar e das indústrias bélicas.

No ano de 1990, a ARPAnet foi transformada em NSFnet (National Science Foundation’s Network), se ligando a outras redes existente, de modo que, passaram a se interconectar centros de pesquisa e universidades de todo o mundo. Desse modo, formou a ‘’internet’’, o qual, foi anteriormente utilizada e criada para uso militar, agora poderia ser utilizada como uma ferramenta de troca de informação entre o meio acadêmico.

Em 1987, a internet foi liberada para o uso comercial, desse modo, este foi o ponto principal para o desenvolvimento desta tecnologia, visto que, mais usuários iriam ter acesso a internet, e devido a isso aumentaria o desenvolvimento dessa tecnologia, criando novos programas úteis para o cotidiano dos usuários. No ano de 1993, com o avanço da tecnologia, e graças a isso, ocorreu o desenvolvimento do

famoso World Wide Web, conhecido popularmente como www, o qual, se tornou de extrema importância para o desenvolvimento da internet.

2.2 WORLD WIDE WEB

É um sistema de documentos dispostos na Internet que servem para permitirem o acesso às informações apresentadas por meios de hipermídia. Esses documentos podem ser vídeos, hipertextos, sons, imagens. E para ter acesso a essas informações é necessário a utilização de um navegador para descarregar as informações (conhecidos como páginas ou documentos).

A ideia desse sistema surgiu em 1989, com Tim Berners-Lee, o qual, utilizou de um computador NeXTcube para ser o seu primeiro servidor, e também para escrever o primeiro navegador, o qual foi nomeado de WorldWideWeb em 1990.

No dia 6 de agosto de 1991, ele postou um resumo no grupo de notícias Alt.hypertext. Essa data foi de exímia importância, porque marca a data de estreia da Web como um serviço público na Internet

Desde então, o ambiente digital cresceu de modo rápido e acelerado, com mais usuários se conectando a cada dia. Devido ao grande aumento de usuários da internet por conta do popularmente conhecido www., ocorreu o surgimento de meios de comunicações eficientes para a toda a população, visto que, agora existem redes especializadas nos meios de comunicações, entretenimento, dentre outros... Isso corroborou para a crescente utilização do ambiente digital no Brasil, assim como, em todo o globo terrestre.

2.3 O DESENVOLVIMENTO DA INTERNET NO BRASIL

No Brasil, os primeiros passos dessa tecnologia ocorreram em 1988, quando a Rede Nacional de Pesquisa (RNP) e o Ministério da Ciência e Tecnologia começaram a investir na tecnologia. E apenas no ano de 1992, que ocorreram os primeiros pontos de pesquisas instalados em algumas universidades do País e, em 1995, foi liberada para o uso comercial, um ponto importante para o desenvolvimento da tecnologia no Brasil.

Com o passar do tempo, no ano de 1995 a internet começou a ser administrada por instituições não-governamentais, que se encarregavam de estabelece padrões de

infraestrutura, domínios, dentre outros. Ocorreu a atuação do governo federal no sentido de implantar infraestrutura necessária e definir os parâmetros para, posteriormente, ocorrer a operação de empresas privadas provedoras de acesso aos usuários. A partir desse momento que a internet no Brasil teve um crescimento gigantesco, visto que, nos anos 2000, a internet contava com aproximadamente 4,5 milhões de usuários, e no ano de 2020, segundo pesquisa do IBGE, já contava com mais de 134 milhões de usuários.

Apesar de todos os benefícios da internet, surgiram novos meios da violação de bens jurídicos protegidos pela Legislação da República Federativa do Brasil, no qual, passaram a ser realizado no plano virtual, um novo ambiente das relações sociais.

Conforme Colli (2009, p.07):

> Apesar de a internet facilitar e ampliar a intercomunicabilidade entre as pessoas, ela pode ter sua finalidade transformada em um meio para a prática e a organização de infrações penais. Dentre estas despontam os chamados crimes informáticos.

Desse modo, a internet pode ser um ambiente para as relações humanas e, também um ambiente propício para a consumação de crimes. E os primeiros crimes que aconteceram, por volta dos anos 1970, foi em sua maioria por usuários que tinham conhecimento técnico sobre o ambiente digital, e devido a isso, se aproveitou das falhas do sistema de segurança para obter vantagem em detrimento de outro.

2.4 SURGIMENTO DO DIREITO NO AMBIENTE DIGITAL

A sociedade vem sofrendo muitas mudanças no decorrer dos anos, dentre elas está o crescimento no número de usuários que utilizam a rede mundial de computadores, a internet.

Devido a essas transformações ocorrem o surgimento de novos ramos dos direitos, o qual, procuram-se adaptar em relação às mudanças e as novas realidades, de modo que as relações jurídicas não fiquem desprotegidas no ambiente digital. Nesse sentido, que surge os Direitos Digitais, de uma necessidade de regulamentar todas as relações entre os usuários no ambiente cibernético, incluindo-se nessa regulamentação, o combate aos crimes virtuais.

Essas mudanças ocorreram em vários ramos do Direito, visto que passaram a fazer parte do cotidiano, alterando as relações de compra e venda do ramo do direito civil e do direito do consumidor, por meio de contratos eletrônicos. Em relação ao Direito Penal e Processual penal, também ocorreram mudanças, sendo de extrema importância para esse ramo do direito, a criação de leis específicas sobre os crimes praticados no ambiente digital.

Diante dessas necessidades, foi indispensável uma adequação do Direito em relação ao regulamento das relações entre os usuários no ambiente virtual, diferenciando as condutas criminosas que passaram a ser praticadas no ambiente digital ou por meio dele.

3. REGULMENTAÇÃO DO AMBIENTE DIGITAL

A regulamentação da Internet se deu pelo Marco Civil da Internet, o qual, representa uma das primeiras iniciativas que estabeleceram preceitos gerais, diretrizes e princípios a serem aplicados em relação ao uso da Internet no Brasil. Nesse sentido, esta lei foi criada com a finalidade de beneficiar a sociedade, além de ser algo necessário, visto que, existia um novo ambiente para legislar sobre.

Devido a isso, a Internet teve uma grande expansão no Brasil, com a atuação de empresas provedores de serviços, com a facilidade de adquirir um aparelho eletrônico que possua internet e com a disseminação das famosas redes sociais, o qual, auxiliou a encontrar pessoas que não tinham contato há anos, e o melhor, para todas as camadas da sociedade. Diante disso, a regulamentação do Marco Civil com força de lei, se mostrou algo muito relevante e importante para o desenvolvimento do ambiente digital.

Portanto, devido a esta lei, o brasil se inseriu no cenário mundial em relação a discussões a respeito de como estabelecer marcos regulatórios e modelos de governança da internet que de certo modo protejam os bens jurídicos dos usuários, assim como, a proteção da intimidade, privacidade e a liberdade de expressão, e ao mesmo tempo em que possa reprimir os atos lesivos contra o direito digital dos internautas. Isso também auxiliou no crescimento da economia, visto que, nasceram novos empregos, novas formas de trabalhar, novas formas de trabalho, dentre muitas outras.

4. O MARCO CIVIL DA INTERNET

A lei 12.965/2014 estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, o qual, foi popularmente conhecida como Marco Civil da Internet. Em seu texto, estão resguardados direitos e deveres aos usuários que podem gerar responsabilidade para os usuários, caso venham a ser desrespeitado pelas empresas provedoras.

O órgão responsável pela regulamentação da Internet é o Comitê Gestor da Internet no Brasil (CGI.br). criado pela Portaria Interministerial nº 147, de 31 de maio de 1995 e alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003, para coordenar e integrar todas as iniciativas de serviços Internet no país, de modo que, tem por objetivo promover a qualidade técnica, a inovação e a disseminação dos serviços ofertados.

O CGI.br é composto por membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica, nomeados por meio de Portarias Interministeriais assinadas pela Casa Civil da Presidência da República, pelo Ministério das Comunicações e pelo Ministério da Ciência, Tecnologia e Inovação.

A composição do CGI.br representa um modelo de governança da Internet baseado nos princípios de multilateralidade, transparência e democracia (COMITÊ GESTOR DA INTERNET NO BRASIL, 2014).

A proposição para o projeto de lei do Marco Civil da Internet nasceu de uma iniciativa proveniente da Secretaria de Assuntos Legislativos do Ministério da Justiça, em conjunto com o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas, onde foi estabelecido um processo aberto e colaborativo para a formulação de um marco civil brasileiro para regulamentação do uso da Internet, tendo como elemento principal de inspiração a Resolução de 2009 do CGI.br, intitulada “Princípios para a governança e uso da Internet no Brasil”.

5. PERIGOS NO AMBIENTE CIBERNÉTICO

Segundo o que expõe o especialista em informática, Mitnick (2006), corriqueiramente existe uma facilidade ao acesso das notícias, principalmente, em tempo real, e isto também acontece em relação aos meios de conversas, visto que, podem ser por meio de texto, webcam, dentro outros meios de comunicação que a

era digital nos fornece. Desse modo, no ambiente cibernético, temos acesso a tudo em que o ambiente informático possa nos oferecer, como por exemplo, uma informação imediata, possuindo a liberdade para buscar por caminhos distintos; a princípio, com a devida segurança acessam sites de relacionamentos, trabalho, realizam pesquisas, dentre outros funcionamentos que a tecnologia nos proporciona. Pelo grande aumento de uso da internet, e devido, a sua facilidade pelas empresas, o qual, traz bastantes benefícios para o desenvolvimento das atividades diárias em que necessita o acesso imediato a informação e rapidez na comunicação, desse modo, facilitando o desempenho das empresas, de modo que, com a utilização de e-mail e busca de informações pela internet as empresas possuem uma facilidade de resolver negócios, correr atrás de informações, dentre outras. Mas com a utilização dessas ferramentas de modo inadequado podem acabar vulnerabilizando as organizações. (SHEMA, 2003).

Desse modo, para Shema (2003), as instituições que tem o acesso corporativo a internet, sempre se vem em situações no qual existe um certo riscos, devido à falta de limites nos caminhos da web. Nesse sentido, a utilização dos espaços virtuais e de suas facilidades para os fins corporativos, podem acarretar em significativo impacto em relação aos negócios e na imagem das empresas, refletindo diretamente para os clientes e no resultado econômico da mesma.

Os meios de utilização de modo inadequado ou indevido do ambiente digital e de suas facilidades podem acarretar em problemas jurídicas para as organizações. E aos usuários que possuem computadores em sua residência podem sofrer riscos ainda maiores do que em relação as empresas. Pois, é comum encontrar vários tipos de vírus, no qual, nenhum computador está totalmente seguro das ameaças de vírus que são softwares maliciosos com o objetivo de destruir ou obter informações (STARLINGS, 2003).

Em consonância com o raciocínio de Starlings (2003), as maiores organizações estão se esforçando muito para deixar a entrada ao ambiente digital mais protegido, de todo modo, esse termo não existe 100% de segurança, porque o que existe é uma possibilidade de um certo ‘’upgrade’’, no qual, irá ocorrer um aumento na proteção por meio de especialistas capacitados, e claro, com investimentos no setor de segurança.

6. OS CRIMES CIBERNÉTICOS

6.1 CONCEITOS INICIAIS

Antes de adentrarmos no assunto, é pertinente esclarecer as características que diferenciam o hacker e cracker. O hacker é um indivíduo que possui um conhecimento técnico em relação ao meio digital, o qual, se utiliza de tal conhecimento em favor da justiça, trabalhando em conjunto com a força policial no combate de rede de criminosos virtuais.

Já os crackers, estes são os usuários que se utilizam do seu conhecimento digital para a prática de crimes no ambiente cibernético. É bastante comum confundirem eles, porque os jornalistas de emissoras de televisão comunicam os fatos errados, alegando que o hacker é o responsável pelo dano causado, e é muito incomum relacionarem tal atitude em relação ao cracker, o qual, é o verdadeiro responsável pelos crimes.

Devido à grande propagação dos computadores e da facilidade ao acesso à internet, diante disso, ocorreu o surgimento de novos crimes e uma nova modalidade de criminosos com conhecimento técnico no ambiente digital e na computação, em todo o globo terrestre. Sendo assim, estes crimes são conhecidos como crimes digitais, virtuais, informáticos, telemáticos, dentre outros. (CRUZ; RODRIGUES, 2018).

É pertinente trazer conceitos de grandes estudiosos sobre o conceito do que seria considerado um crime virtual.

Expõe Colli (2010) que, os atos criminosos praticados nesse ambiente possuem como caracterização falta física de agente ativo, devido a isso, acabam ficando de forma usual com definição como crimes virtuais, isto é, delitos praticados pelo meio da internet possuem denominação de crimes virtuais, justamente, por causa dessa falta física dos seus autores.

Segundo o que expõe a doutrinadora Carla Araújo de Castro (2003, p. 9.), os crimes cibernéticos:

> Os crimes digitais podem ser conceituados como sendo às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros.

Conforme explica Crespo (2015), no ambiente online, os usuários são capazes de fomentar o preconceito étnico e de gênero, alimentar discursos racistas, divulgar propagandas de ódio e violência, extremismos políticos e ideológicos, comprar e vender substancias ilícitas, dentre outros crimes. Wendt e Jorge (2012) conceituam estas práticas, dizendo que, tais condutas, quando praticadas contra ou por intermédio de computadores, são denominadas como crimes cibernéticos.

De acordo com o pensamento de Cassanti (2014), traz a descrição do crime digital como um ato lesivo cometido por meio de um computador ou de um periférico (celular, tablets, dentre outros) na intenção de obter vantagem em detrimento de outro, e de forma indevida.

Seguindo a linha de raciocínio do autor, os crimes ou ações praticadas por meio do ambiente digital ou contra a internet, merecem serem observados, assim como, serem distinguidos para não ocorrer a aplicação de sanções majoradas ou diminuídas quando imputadas ao usuário que praticou o ilícito penal.

Os conceitos quanto aos crimes práticos no ambiente cibernético são diversos, não ocorrendo um consenso entre os doutrinadores sobre a melhor denominação para os delitos que são práticos com a tecnologia, delitos informáticos, abuso de computador, fraude informática, dentre vários outros. Esses conceitos não abrangem todos os crimes ligados à tecnologia, devido a isso, é necessário ficar atento quando está conceituando determinado crime, visto que, existem variadas situações complexas que ocorrem no ambiente virtual, de modo que o Código Penal Brasileiro tipificou apenas dois crimes virtuais, os quais são a invasão de dispositivo informáticos e interrupção de serviço telemático, o restante é considerado como crimes comuns cometidos com o auxílio da internet (LEONARDI, 2012).

6.2 O COMEÇO DOS CRIMES DIGITAIS.

Segundo o sistema de segurança Avast, embora a internet tenha apenas 30 anos, os especialistas em segurança consideram que uma fraude de 1834 foi o primeiro crime virtual da história. No qual, dois indivíduos mal intencionados se infiltraram no sistema francês de telégrafo e obtiveram acesso aos mercados financeiros, cometendo assim o roubo de dados. A maioria dos crimes nesse período era em relação aos mercados financeiros, visto que, muitos tinham o objetivo de obter vantagem financeira.

No ano de 1940 apareceu Rene Carmille, um especialista em informática que foi conhecido como o primeiro hacker ético do mundo, visto que, ele foi capaz de impedir as tentativas nazistas de registrar e rastrear judeus, de modo que conseguiu atrapalhar as atividades nazistas, salvando assim dezenas de milhares de judeus de campos de extermínio.

7. CRIMES DESPROPORCIONAIS A PENA APLICADA

Os danos causados pelos crimes digitais vão desde crimes praticados contra a honra, até aqueles em que o criminoso consegue infligir um dano financeiro para vítima. Dentre os crimes virtuais, podemos destacar esses, cujas práticas são comuns em nosso dia a dia, e devido ao dano causado à vítima.

7.1 CALÚNIA

Em relação ao crime de calúnia, assim como os demais crimes contra a honra e outros delitos nos quais o bem jurídico atingido não é a tecnologia propriamente dita, o qual, se enquadra no crime informático impróprio. Isso porque o bem jurídico atingido pela prática da calúnia é a honra, o qual, se encontra tutelada pela legislação vigente, ocorrendo que, no âmbito informático, a tecnologia da informação é a apenas um meio que foi utilizado para a prática do crime. (PACHECO, 2019)

Desse modo, a partir das facilidades proporcionadas pelo uso da internet, a rede mundial de computadores acaba se tornando um ambiente conveniente para a prática de crimes, até mesmo para aqueles que se utilizam do meio digital para causar dano à reputação de outros, em um contexto em que a própria investigação é dificultada devido a ausência de profissionais capacitados para tal tarefa. (PACHECO, 2019)

Nesse sentido, o crime de calúnia tem a classificação de crime digital impróprio, visto que, o meio digital foi utilizado como um meio para atingir a finalidade, a qual, era a prática de imputar um crime a alguém que não o cometeu. Pela prática do crime ter sido no ambiente digital, as proporções do crime tomam um rumo desproporcional e diferente.

Dito isso, é mais fácil identificar uma ofensa à honra que foi proferida por meio de um e-mail, sendo de um usuário ao outro. Porém, nos casos em que for tomado

como base o ambiente virtual, como por exemplo, o *Facebook*, o *Twitter*, o *Instagram*, entre outros redes sociais. Nesse sentido, por se tratar de uma rede social, essas redes propiciam uma nova forma de praticar o crime, que seria a permanência, de modo que, enquanto a postagem está inserida no ambiente virtual, está mensagem está sendo repetida à exaustão, fazendo com que mais e mais pessoas vejam e compartilhe tal publicação. (NUCCI, 2017)

Nesse caso, quanto mais pessoas compartilharem a publicação, estarão contribuindo em desfavor à honra do usuário que foi vítima do crime de calúnia. O artigo 138 do Código Penal, dispõe que:

> Artigo 138: Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena – detenção, de 6 (seis) meses a 2 (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.
> § 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 artigo 141;
> III: se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

Em relação a detenção é de apenas seis meses a dois anos, e multa, mas nos casos em que a conduta criminosa é praticada no ambiente digital, deveria ter uma pena maior. Isso devido ao fato de que no ambiente digital o dano causado pelo criminoso contra a honra da vítima é potencializado, visto que, um número indefinido de usuários poderá ter acesso àquela publicação de algum modo, e realmente acreditarem que a vítima fez aquele crime que foi imputado falsamente a ela.

Mesmo nos casos em que a postagem é excluída, ainda assim, ocorre o perigo daquela calúnia ser compartilhada em outros meios de comunicação, podendo causar um dano imenso à imagem do usuário na internet e no seu convívio social. Não podendo assim, ter um controle sobre o compartilhamento daquela publicação, que poderá ser vista até em outros estados, e até mesmo, em outros países.

Portanto, a calúnia no meio digital merece uma qualificadora devido aos danos que este crime possa vir a causar à honra, à imagem de uma determinada pessoa, visto que, o dano causado à vítima pode chegar a ter proporções indefinidas.

7.2 DIVULGAÇÃO DE IMAGENS ÍNTIMAS (NUDES)

Este crime se assemelha bastante com o outro, devido ao objetivo do crime, o qual, é causar dano a uma determinada pessoa. Apesar de não ter uma tipificação expressa, ele pode se encaixar nos crimes de difamação e injúria.

É importante abordarmos os textos destas leis, tipificam que:

> Artigo 139: Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.
> 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.

A pena do crime de injúria é menor do que ao crime de difamação, vejamos:

> 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.

É necessária uma tipificação para essa conduta criminosa que é praticada no ambiente virtual, em virtude dos danos causados por esta conduta. De modo que prejudicam muito além da honra e da imagem, visto que, muitas pessoas quando são expostas na internet dessa maneira acabam tendo a sua vida social abalada e o seu emocional afetado.

Isso se deve ao fato de ter suas imagens intimas vazadas, e pelo caráter de perpetuidade no ambiente digital, o qual, independente de excluírem todas as fotos que estão vinculadas aos sites, ainda assim, irá existir usuários que estarão de posse dessas imagens, e poderão faze-las circular novamente pelo ambiente digital.

Portanto, por se tratar de um dano irreparável ao indivíduo, esta conduta deveria ser tipificada, de modo que a pena fosse mais rígida, com o objetivo de inibir que ocorra novas condutas assim.

8. CLASSIFICAÇÃO DOS CRIMES DIGITAIS

É necessário classificar os crimes cibernéticos, apesar de que as classificações existentes para os crimes cibernéticos não serem eficazes, visto que, a evolução proporcionada pela internet é muito grande, assim como as novas formas de praticar crimes digitais. Portanto, as classificações se tornam ultrapassadas em pouco tempo.

De todo modo, existem duas classificações que mais estão presentes na doutrina. Sendo eles os crimes cibernéticos puros, mistos e comuns e crimes cibernéticos próprios e impróprios.

8.1 CRIMES DIGITAIS PUROS

É considerado crime digital puro, aquele em que o sujeito ativo tem como alvo o sistema de informática, até mesmo nas situações em que ocorrem atos de vandalismo contra a integridade física de determinado sistema, assim como, pelo acesso indevido aos dados contidos no computador atacado.

8.2 CRIMES DIGITAIS MISTOS

Nesta modalidade, o objeto tecnológico é um instrumento indispensável para a consumação da ação criminosa, sendo assim, apenas um meio de execução do crime.

É considerado misto, devido a violação das normas da lei penal comum e das normas da lei penal de informática, visto que, podem ser aplicados normas relacionadas aos crimes comuns em conjunto com uma norma por mau uso de equipamento e meio de informático. Desse modo, não seria apenas um delito comum, pois incide na penal de informático, tendo assim o concurso de normas. Como por exemplo, a retirada ilícita de valores monetários de contas bancárias via *homebanking*.

8.3 CRIMES CIBERNÉTICOS COMUNS

Os crimes informáticos comuns, são aqueles que se utilizam do ambiente digital apenas como um instrumento para a efetuação de um delito que já está tipificado no nosso Código Penal. Desse modo, a internet é apenas um meio para a realização de uma conduta delituosa, como por exemplo, a pornografia infantil, que era instrumentalizada por meio de vídeos e fotografias, mas no ambiente digital é por meio de páginas, grupos. Portanto, mudou apenas a forma, mas a essência do crime permanece a mesma.

8.4 CRIMES CIBERNÉTICOS PRÓPRIOS

Segundo Anderson Soares Furtado Oliveira (2009, p.33), o crime cibernético próprio é aquele em que:

> [...] só pode ser cometido no ciberespaço, ou seja, necessariamente, deve ser realizado no ambiente do ciberespaço, para que a conduta seja concretizada, tendo um tipo penal distinto do tradicional. Ademais, tanto a ação quanto o resultado da conduta ilícita consumam-se no ciberespaço.

Nessa classificação os crimes próprios são aqueles em que o sistema informático do sujeito passivo é o objeto e o meio do crime. Desse modo, entrariam aqui os crimes de invasão de sistema quanto de modificar, alterar, inserir dados falsos, ou seja, de modo que cause um dano diretamente ao software ou hardware do computador e deverá ser realizado por meio de um computador ou contra ele e seus periféricos.

8.5 CRIMES CIBERNÉTICOS IMPRÓPRIO

Aires José Rover (2009, p.3), expõe que:

> São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta para a perpetração de crime comum, tipificável na lei penal. Dessa forma, o sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta.

Ou seja, os crimes cibernéticos impróprios são aqueles em que atingem um bem jurídico comum, como por exemplo, o patrimônio, e se utilizam dos sistemas informáticos como um meio de execução, como por exemplo, no caso em que um cracker invade uma rede de computadores de um hospital e muda as prescrições médicas relativas a um determinado paciente, isso se caracterizaria como crime cibernético impróprio, visto que, foi utilizado da rede como uma ferramenta para a perpetração de um crime comum.

9. CRIMES DIGITAIS E A TIPIFICAÇÃO

Segundo Newton de Oliveira Lima (2009, p.15), O Direito Penal é a *última ratio*, em virtude que só poderá ser utilizado em último recurso, e devido a isso, sempre resguardou os bens jurídicos mais relevantes, já que:

> [...]com a difusão da tecnologia informática, tornando-se uma presença constante na maioria das relações sociais, o Direito deve cuidar de reconhecer valores penalmente relevantes, criando normas protetoras a fim de estabelecer a segurança dessas relações"

Desse modo o Direito Penal vigente possui uma missão árdua, em virtude que deverá ir à luta contra os crimes digitais, para evitar e punir os delitos e garantir os direitos inerentes à pessoa. Nesse sentido, passará pelo sistema da tipicidade, o qual, funciona como um critério de racionalidade do Direito Penal, em consonância com o princípio da Legalidade e da teoria do tipo penal. É evidente a importância da tipicidade aos crimes digitais, para tentar inibir futuras ações delituosas.

A proteção de bens jurídicos é o alicerce moderno da tipificação de novas condutas (SILVA, 2003, p.30-33). De fato, as condutas praticadas na internet geram perigo aos bem jurídicos valorados pelo Direito a partir de outras normas. Trata-se de condutas de perigo (SILVA, 2003, p.50)

10. PRINCIPAIS LEIS SOBRE OS CRIMES DIGITAIS

As ações criminosas praticadas no ambiente digital afetam a segurança e credibilidade necessários para realizar qualquer negócio jurídico. De modo que, ultrapassam esse limite interferindo no cotidiano de muitas pessoas, fazendo com que ocorra uma certa desconfiança nas relações sociais realizadas nesse novo ambiente.

Muitas condutas encontram-se sem a devida regulamentação. Nesse sentido, o ambiente digital se transformar em um verdadeiro paraíso para os criminosos desta área. Basso e Almeida (2007) explicam que em muitos casos, as leis existentes são também aplicáveis aos novos pressupostos do contexto virtual. Em outros, é necessária uma nova regulamentação para se ter uma maior segurança no emprego das ferramentas eletrônicas e maior certeza quanto a validade e eficácia das transações celebradas por meio eletrônico

O que existe atualmente é um conjunto reduzido de normas que tipificam somente algumas condutas. São tipos extremamente específicos, não sendo esse um óbice à produção de normas mais gerais. (MONTEIRO NETO, 2008, p. 93)

10.1 LEI CAROLINA DIECKMANN.

A Lei 12.737/2012, conhecida popularmente como Lei Carolina Dieckmann, teve a sua criação após a atriz ter sido vítima de um crime cibernético, onde os criminosos tiveram acesso ao seu dispositivo informático por meio de um e-mail enviado para atriz, o qual, continha um arquivo malicioso e ao ser aberto, liberou uma porta que permitiu a entrada dos crackers em seu dispositivo.

Após terem acesso ao seu computador, conseguiram imagens intimas da atriz e em seguida fizeram inúmeras chantagens, alegando que iriam divulgar tais fotografias na internet e só não divulgariam caso a vítima transferisse uma determinada quantia, a atriz não aceitou as chantagens feita pelos criminosos e por isso teve as suas fotos expostas em sites de conteúdo adulto. Devido a isso, houve uma grande comoção por parte da população, e o assunto passou a ser tratado em regime de urgência, e no mesmo ano do fato foi promulgada a Lei 12.737/2012.

Cabe, nessa oportunidade, ressaltar o que dispõe a Lei Carolina Dieckmann, a qual disciplina sobre a inviolabilidade do dispositivo informático:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (BRASIL, 2012, [s.p.]).

A nova lei também trouxe o artigo 154-B, o qual, dispõe que:

> Art. 154-B - Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime e cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (BRASIL, 2012, [s.p.]).

Esta lei trouxe modificações no Código Penal Brasileiro, acrescentando os artigos 154-A e 154-B, criando assim o tipo penal ‘’Invasão de dispositivo informático’’.

Nesse sentido, o bem jurídico, que está sendo amparado por esses artigos, é a inviolabilidade dos dados informáticos, visando assim, preservar a privacidade e a intimidade do usuário no ambiente cibernético, o qual, estes direitos estão protegidos no artigo 5º da Constituição Federal.

Vale ressaltar que ocorreram modificações em outros dispositivos do Código Penal Brasileiro, como por exemplo, no artigo 266 que acrescentou a interrupção ou perturbação de serviços telegráficos, telefônico, informático, telemático ou de informação de utilidade pública, e do mesmo modo modificou o artigo 298, o qual, estabelece que:

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena - reclusão, de um a cinco anos, e multa. Falsificação de cartão. Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

Segundo (JUNIOR, 2014), o texto legal tem a finalidade de incriminar a conduta do agente que invade, driblando os mecanismos de segurança, e obtém, adultera ou destrói a privacidade digital alheia, bem como a instalação de vulnerabilidade para obtenção de vantagem ilícita. Desse modo, para ocorrer o crime, tem a necessidade da existência de um mecanismo de segurança no sistema do aparelho, uma vez que esta lei condiciona a ocorrência do crime com a violação do sistema de segurança.

Nesse sentido, caso ocorra a invasão ao dispositivo informático que se der sem a violação do mecanismo de segurança pela inexistência deste será conduta atípica. Por essa razão que é necessário proteger bem o seu dispositivo, utilizando de ferramentas que impeçam que o seu aparelho eletrônico seja violado, como por exemplo, a utilização de firewall, antivírus e senhas.

10.2 LEI AZEREDO

Em consonância com o pensamento de (CRESPO, 2015), esta lei enquanto seu projeto foi apelidado de ‘’AI-5 digital’’ devido aos pontos polêmicos que continha, em especial, os referentes à guarda dos logs de acesso dos usuários pelos provedores. Por este motivo, o projeto foi esvaziado e se tornou uma lei com poucas e frágeis disposições.

Nesse sentido, é necessário expor o que está determinada a Lei 12.735/2012, disciplina em seu art.4º que: ‘’Os órgãos da polícia judiciária estruturarão, nos termos

de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.''

Dessa maneira, o texto determina que os órgãos da polícia judiciária deverão criar delegacias especializadas no combate aos crimes digitais. Mas essa especialização depende do Poder Público, visto que, é necessário investir na especialização da Polícia com treinamentos e equipamentos.

10.3 LEI 14.155/2021

Esta lei alterou o Código Penal com a finalidade de agravar algumas condutas criminosas praticadas no ambiente informático, como por exemplo, nos crimes em que ocorre a violação de dispositivo informativo, furto e estelionato cometidos de forma eletrônica ou pela internet, além de ter definido uma competência em modalidades de estelionato através do Código de Processo Penal

Desse modo a Lei 14.155/2021, trouxe mudanças na Lei Carolina Dieckmann, o qual disciplina que:

> Art. 1º O Decreto-Lei nº 2.848, dede dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
> (...)
> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (BRASIL, 2021, [s.p.])

Nesse sentido, a lei ficou mais abrangente devido a remoção do termo ''mediante violação indevida de mecanismo de segurança'', sendo assim, só era possível ocorre a consumação do crime caso o criminoso tivesse quebrado alguma senha ou burlado algum tipo de barreira digital. Porém, devido a retirada desse trecho da lei, ela se tornou mais abrangente.

Vale ressaltar que na redação anterior falava em ''dispositivo informático alheio'', e nessa nova redação foi utilizada a expressão ''dispositivo informativo de uso alheio'', ou seja, o crime poderá se configurar ainda que o sujeito ativo viole o seu próprio dispositivo, no caso em que esteja utilizada pela vítima, como por exemplo, no caso de empréstimo. Desse modo, o sujeito ativo será o próprio dono do dispositivo.

Apenas com a invasão de dispositivo já é ilegal, incriminando o indivíduo que obtém acesso ao computador ou algum aparelho eletrônico alheio por meio de alguma

engenharia social, como por exemplo, convencendo uma pessoa a compartilhar sua senha. Além de ter aumentado a pena, que agora é possível chegar aos 4 anos de reclusão, além da multa.

Ocorreu a alteração do crime de furto que está previsto no art. 155 do Código Penal, o qual, foi alterado pela Lei n. 14.155, de 27 de maio de 2021, que introduziu, nos §§ 4º-B e 4º-C, a figura do ‘’furto mediante fraude por meio de dispositivo eletrônico ou informático’’.

Essa alteração trouxe uma nova tipificação penal em relação aos crimes digitais, o qual dispõe no Art. 155 do Código Penal, que:

> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

Esta ‘’novatio legis’’ foi criada devido ao aumento expressivo de fraudes virtuais durante o período de pandemia, visto que, ocorreu um distanciamento social e o ambiente digital teve uma maior realização de atividades pessoais e profissionais contribuído para o incremento desse resultado.

Nesse sentido, a lei está tentando inibir crimes que não eram tipificados anteriormente, como por exemplo, as práticas de clonagem de *whatsapp*, nos casos em que não ocorreram prejuízo financeiro ao outrem, e em relação a prática do crime de *phising*, quando se utiliza de uma fraude para obter os dados de usuários, como por exemplo, em relação a falsificação de um site.

No caso da fraude eletrônico, sem a necessidade do furto, também houve uma alteração, o qual está expressa no Art. 171, que:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

Portanto, esta iniciativa legislativa, criminalizou mais severamente as fraudes virtuais, com penas mais rigorosas e uma melhor descrição em relação a Lei Carolina Dickmann. De fato, esta norma é algo benéfico para a sociedade brasileira, mas ainda não podemos tirar uma conclusão sobre, visto que, ainda é algo muito recente. De todo modo, ainda se faz necessário a alteração em algumas normas penais.

11. DIREITO COMPARADO

O avanço tecnológico acontece no mundo todo, e devido a isso, ocorre uma evolução no tratamento dos crimes digitais por parte da grande maioria dos Estados, visando sempre proteger e tutelar os bens jurídicos importantes.

Nesse sentido, é necessário expormos um pouco sobre o tratamento dos crimes digitais em outros Estados. Dito isso, será exposto a convenção de Budapeste que trata sobre os crimes digitais e, que foi aceita por vários países.

11.1 CONVENÇÃO DE BUDAPESTE

A convenção foi criada em 2001, e é o único tratado internacional sobre crimes cibernéticos, com normas de direito penal e processual penal, ela é voltada a definir estratégias em conjunto com os demais países membros para a tipificação e o enfrentando dessas condutas delituosas praticadas no ambiente digital. Sendo em sua maioria membros da União Europeia, todavia, existem membros de outros continentes, como por exemplo, os Estados Unidos, Canada, Japão, além de países vizinhos do Brasil, como, Argentina, Paraguai, Chile e Colômbia.

O tratado da Convenção sobre o Cibercrime, prioriza em seu preâmbulo ‘’uma política criminal comum, com o objetivo de protege a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional’’ e reconhece ‘’a necessidade de uma cooperação entre os Estados e a indústria privada’’.

Desse modo, o tratado é necessário, visto que, para ter um bom desenvolvimento em relação aos crimes digitais, tem que ocorrer a cooperação internacional para que seja possível coibir as práticas ilícitas nos ambientes digitais, além facilitação das informações fornecidas com a ajuda das empresas privadas.

Além disso, Castells (2007, p.205) explica que: ‘’a internacionalização das atividades criminosas faz com que o crime organizado (...) estabeleça alianças estratégicas para cooperar com as transações pertinentes a cada organização, em vez de lutar entre si’’. Ou seja, no ambiente digital tem-se a possibilidade de crimes que já eram praticados no ambiente físico, também pudessem ser praticados na Internet, e de formas cada vez mais sofisticadas, podendo ocorrer em um crime a participação de muitos autores de diferentes nacionalidades, e em locais distintos do globo terrestre.

O tratado possui ao todo quatro capítulos (Terminologia, Medidas a Tomar em Nível Nacional, Cooperação Internacional e Disposições Finais) e 48 artigos. A convenção tipifica os crimes cibernéticos como: infrações contra sistemas e dados informáticos; infrações relacionadas com computadores; infrações relacionadas com o conteúdo; pornografia infantil e infrações relacionadas com a violação de direitos autorais.

Vale ressaltar que os países signatários poderão adaptar suas próprias legislações nacionais buscando criminalizar tais condutas delituosas. Outro ponto importante se deve à sugestão de adotarem medidas legislativas cabíveis para punir aqueles crimes que foram tentados, assim como, adotar medidas cabíveis para a responsabilização da pessoa jurídica cometidas por seus funcionários.

> Como se verificou, muito embora a convenção exija de seus membros que sigam alguns princípios fundamentais e regras estabelecidas em convenções anteriores, sua aplicabilidade é bastante relativizada, buscando amoldar-se de acordo com a legislação pátria de cada país signatário, objetivando, sobretudo, apontar caminhos e não propor soluções enrijecidas e únicas para a resolução dos problemas apontados, o que, em tese, facilitaria o ingresso do Brasil na adesão à referida convenção, mas até o presente momento, o país não aderiu ao tratado. (COLTRO e WALDMAN, 2020, p.112)

O Ministério Público Federal, já se manifestou favorável em relação a adesão, e salientou que poderia auxiliar ao combate da criminalidade virtual no país, visto que, existe uma falta de legislação moderna e específica para o combate aos crimes digitais no Brasil. Até o presente momento está ocorrendo discussões sobre o ingresso do país no determinado tratado, mas nada decidido.

Vale ressaltar que, o Brasil não foi convidado para à Resolução, e para fazer parte dela, demandaria receber um convite de um dos Estados membros. Porém, isso não seria algo difícil, visto que, o Brasil mantém relações diplomáticas com países que atualmente fazem parte do grupo fundador.

12. CONCLUSÃO

A internet é uma ferramenta de grande valor para todos os povos, visto que, é capaz de ligar pessoas nos mais remotos cantos do mundo em uma questão de segundos, além de suas facilidades nos dia-a-dia da população, como por exemplo, a compra, venda, contratos, dentre outros. Devido a isso está ferramenta se tornou uma febre na maioria das sociedades, pelas facilidades que ela nos proporciona.

Apesar de representar um avanço gigantesco em todas as sociedades, a internet apresentou outros risco para a sociedade, visto que, em seu início não existia legislação para regular o comportamento dos usuários no ambiente digital. E devido a essa falta de regulação, causou um grande crescimento nos crimes praticados no ambiente digital.

Diante disso surgiu a necessidade da legislação em regulamentar essas condutas criminosas práticas no ambiente digital, para tentar inibir que tais ações delituosas sejam praticadas na internet.

Com o passar do tempo, aumentou-se a necessidade de uma legislação específica em determinados crimes, como foi o caso da criação da lei Carolina Dieckmann, e que teve a sua motivação devido ao compartilhamento de dados pessoais da atriz Carolina Dickmann, devido a isso que a Lei leva o seu nome. Nesse sentido, a lei tipifica a conduta de invadir dispositivo sem o consentimento da pessoa como um crime cibernético. No mesmo ano ocorreu a criação da Lei 12.735/2012, de modo que estabeleceu que os órgãos da polícia judiciárias deverão estruturar setores especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação, dentre outros.

A mais recente legislação sobre os crimes praticados no ambiente digital é a Lei 14.155/2021 trouxe modificações na conduta criminosa tipificada na Lei Carolina Dickmann, modificando esse dispositivo para deixa-lo mais abrangente, e com uma maior pena para os crimes de invasão de dispositivo informativo. Além de ter criado a lei de estelionato mediante fraude, tipificando assim, a conduta criminosa de clonar whatsapp, o qual, não era previsto anteriormente, apenas era enquadrado no caso de estelionato caso houvesse algum dano financeiro para a vítima que teve o seu whatsapp clonado.

Porém, em determinadas leis possuem uma pena branda e sem suficiência para coibir a prática dessas condutas criminosas, de modo que, o dano causado à vítima é muitas vezes superior à pena aplicada ao culpado pelo delito informático.

Isso ocorre em muitos crimes contra à honra, como por exemplo, no crime de calúnia, onde é imputado um crime a uma determinada pessoa que é inocente. E por conta de a internet ser um ambiente de fácil acesso é uma potencializadora da divulgação destes crimes, visto que, a grande maioria das pessoas compartilhem entre si determinada noticia acreditando que aquilo é um fato verídico, de modo que, o dano causado à vítima do crime é irreparável devido a internet ter o seu caráter de perpetuidade.

Para inibir determinadas atitude maldosas no ambiente digital, seria necessário alterar algumas penas da legislação, com a finalidade de um ambiente digital mais seguro. Uma punição proporcional ao crime cometido é uma maneira de fazer com que as práticas desses delitos sejam cada vez menos comum.

Por fim, uma opção boa e fácil para combatermos essas práticas delituosas, seria aderir a Convenção de Budapeste. Que se demonstra algo bastante propicio no combate à criminalidade no mundo, em virtude da colaboração entre os países, e as empresas privadas.

O Ministério Público Federal, se manifestou a favor da adesão do país ao trato, o que sem sombra de dúvidas seria benéfico e contribuiria para melhorar a segurança do ambiente digital, tanto para as empresas que se utilizam dela, como, para as pessoas físicas, que diariamente utilizam-se dos meios digitais para relações econômicas e sociais.

REFERÊNCIAS

ARAUJO, Cláudio Rodrigues. Análise da aplicação do direito penal nos crimes virtuais. **Pensar Acadêmico**, Manhuaçu, v. 19, n. 2, p. 494-511, maio-setembro, 2021. Disponível em: <ANÁLISE DA APLICAÇÃO DO DIREITO PENAL NOS CRIMES VIRTUAIS | Araujo | Pensar Acadêmico (unifacig.edu.br)>. Acesso em 15/11/2021

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

BRASIL. **Lei 12.735 de 30 de novembro de 2012**. 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. Disponível em: <L12735 (planalto.gov.br)>Acesso em 10/10/2021

BRASIL. **Lei 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: <L12737 (planalto.gov.br)> Acesso em 15/10/2021.

BRASIL. **Lei 14.155 de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em:< L14155 (planalto.gov.br)>Acesso em 12/11/2021

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

CASTELLS, Manuel. **A Era da Informação**: economia, sociedade e cultura. Volume I, a sociedade em rede. 5. ed., São Paulo: Paz e Terra, 2001.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. Rio de Janeiro, Lumen Juris, 2003.

COLLI, Maciel. **Cibercrimes**: Limites e Perspectivas a investigação policial de crimes cibernéticos. São Paulo: Juruá, 2010.

COLTRO, Rafael Khalil; WALDMAN, Ricardo Libel. CRIMINALIDADE DIGITAL NO BRASIL: A PROBLEMÁTICA E A APLICABILIDADE DA CONVENÇÃO DE BUDAPESTE. **Revista Em Tempo**, [S.l.], v. 21, n. 1, p. 104-123, aug. 2021. ISSN 1984-7858. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3247>. Acesso em: 15 nov. 2021.

COMITÊ GESTOR DA INTERNET NO BRASIL. **O CGI.br e o Marco Civil da Internet**. 2014. Disponível em: <CGI.br - O CGI.br e o Marco Civil da Internet>. Acesso em 22/10/2021

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

CRESPO, Marcelo. **Deep Web: o submundo do crime**. Canal Ciências Criminais, 2015. Disponível em: https://canalcienciascriminais.jusbrasil.com.br/noticias/211380741/deep-webo-submundo-do-crime. Acesso em 6/11/2021

CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. **Revista Científica Eletrônica do Curso de Direito**, 13. ed., janeiro, 2018.

LATTO, Nica. **O que é crime virtual?**. Avast. Disponível em: <O que é o crime virtual? | Definição e exemplos | Avast> Acesso em 16/10/2021

LIMA, Newton de Oliveira. **Cultura e direito na pós-modernidade**: análise sob um enfoque atualizador da teoria dos valores de Gustav Radbruch. Disponível em: <27002 (diritto.it)> . Acesso em 22/10/2021

MATSUYAMA, Keniche Guimarães; LIMA, João Ademar de Andrade. **CRIMES CIBERNÉTICOS:**: atipicidade dos delitos. 2017. 10 f. TCC - Curso de Direito, Unifacisa, Campina Grande, 2021. Disponível em: http://www.joaoademar.qlix.com.br/3cbpj.pdf. Acesso em: 23 out. 2021.

MITNICK, Kevin David; SIMON, Wiliam. **A Arte de Enganar: Ataques de Hackers**: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education do Brasil, 2006.

MONTEIRO, CESAR MACEDO. **Classificações dos Crimes de informática ainda sem rodapé**, 2013, 68 f. (Profissional Jurídico) Disponível em: <https://pt.slideshare.net/cmacedomonteiro/classificao-dos-crimes-de-informatica-ainda-sem-nota-de-rodap/RK=1/RS=k7f6jhy2UgBPimvHDKWeCYI0cp0->Acesso em 07/11/2021.

NUCCI, Guilherme de Souza. **Código Penal comentado**. 15 ed. rev., atual. e ampl. Rio de Janeiro: Forense, 2015.

PACHECO, Juliana Andricópolo. **A prática do crime de calúnia em meio cibernético**. 2019. 59 f. Monografia (Especialização) - Curso de Direito, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2019. Disponível em: <001101230.pdf (ufrgs.br)> Acesso em 12/10/2021

SHEMA, Mike. Hack notes: **Segurança na Web**: referência rápida. Rio de janeiro: Campus, 2003. 182 p

SILVA, Ângelo Roberto Ilha da. Dos crimes de perigo abstrato em face da Constituição. São Paulo: Editora **Revista dos Tribunais**, 2003.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012.