STRONG BUSINESS SCHOOL CURSO DE DIREITO

Nicolas Oliveira Araújo

TÍTULO: A TIPICIDADE DOS CRIMES CIBERNÉTICOS NO BRASIL

SANTO ANDRÉ
2023

NICOLAS OLIVEIRA ARAÚJO

A TIPICIDADE DOS CRIMES CIBERNÉTICOS NO BRASIL

Projeto de Pesquisa apresentado como requisito parcial para obtenção do título de Bacharel em Direito, pelo Curso de Direito da STRONG BUSINESS SCHOOL.

SANTO ANDRÉ
2023

RESUMO

Neste projeto, foi estabelecido como problemática, a tipificação adequada para os ilícitos penais virtuais. Dessa forma foi estabelecido como objetivo geral verificar as vertentes penais e protetivas, aplicáveis em cada tipo de crime para combater e diminuir tais ilícitos penais. Destarte, foi utilizado a metodologia de revisão de literatura, pesquisa descritiva e bibliográfica, portanto foi realizado o entendimento penal e doutrinário em relação às mudanças da legislação Brasileira sobre o tema e quais as principais normas aplicáveis para os casos que ocorrem no País. Para isso foram aplicados artigos, sites, trabalhos acadêmicos, leis e doutrinas que remetem aos crimes digitais. Com exceção das leis, os conteúdos coletados são entre os anos de 2000 a 2023 no Brasil. O tema abordado, refere -se a constância de ilícitos que vem ocorrendo através de golpes virtuais, tendo como base aumento no índice de casos brasileiros.

No cenário atual, há poucas leis para cada crime no setor virtual e baixa penalização.

Portanto, este estudo mostra a profundidade de cada crime cibernético e a característica de cada um deles com base na necessidade da criação penal sobre a Lei Carolina Dieckmann e LGPD que por vez, tem como tentativa de minimizar a quantidade destes atos, junta a aprovação da Lei 14.155/2021 que tem como principal intuito alterar o tempo de sanção aos criminosos, o que era de apenas três meses a um ano, passou a ser de quatro anos até oito anos de reclusão.

Palavras-chave: Ilícitos penais ; Legislação; Lei Carolina Dieckmann; LGPD - Lei geral de proteção de dados virtuais.

ABSTRAT

In this project, the appropriate classification for virtual criminal offenses was established as a problem. Therefore, the general objective was to verify the criminal and protective aspects applicable to each type of crime to combat and reduce such criminal offenses. Therefore, the methodology of literature review, descriptive and bibliographical research was used, therefore a criminal and doctrinal understanding was carried out in relation to the changes in Brazilian legislation on the subject and which are the main applicable standards for cases that occur in the country. To achieve this articles, websites, academic works, laws and doctrines that refer to digital crimes were applied. With the exception of laws, the content collected is between the years 2000 and 2023 in Brazil. The topic addressed refers to the constancy of illicit acts that have been occurring through virtual scams, based on an increase in the rate of Brazilian cases.

In the current scenario, there are few laws for each crime in the virtual sector and low penalties.

Therefore, this study shows the depth of each cybercrime and the characteristics of each of them based on the need for criminal creation under the Carolina Dieckmann Law and LGPD which, in turn, attempts to minimize the number of these acts, together with the approval of the Law 14,155/2021, whose main purpose is to change the sanction time for criminals, which was from just three months to one year, now from four years to eight years of imprisonment.

Keywords: Criminal offenses; Legislation; Carolina Dieckmann Law; LGPD - General virtual data protection law.

Sumário

1. Introdução

Os crimes informáticos (de informação) ocorrem desde muito antes do surgimento da internet. Com o avanço da tecnologia e o advento da internet, surgiram novos meios de comunicação e como tal, também está sujeito a marginalização e criminalidade, ao mesmo tempo que teve impacto positivo na vida das pessoas, também ocorreu impactos negativos, os principais delitos oriundos do meio digital são: Homicídio, Estupro Virtual, Estelionato, Furto Qualificado, Injúria, Calúnia, Difamação, Invasão de dispositivo informático, Pedofilia, Violação de segredo entre outros.

A cibercriminalidade é uma ação criminosa realizada por meio de um computador, uma rede de computadores ou um dispositivo conectado à rede, que tem como objetivo gerar invasões de sistema, disseminação de vírus, roubo de dados pessoais, falsidade ideológica e acesso a informações confidenciais. Atualmente as pessoas têm facilidade ao acesso da internet, portanto a educação digital é muito importante para não serem alvos de crimes digitais destacados anteriormente e até mesmo para não cometerem nenhum tipo de injúria ou difamação na rede, pois tais são comuns em plataformas como Facebook e Instagram.

Em seu aspecto metodológico, o método de pesquisa empregado é revisão de literatura, pesquisa descritiva e bibliográfica, portanto será viável realizar o entendimento penal e doutrinários sobre as mudanças da legislação apoiando-se em técnicas de coleta de dados, materiais que levam à análises e reflexões, Jurisprudências, sobre a delimitação será em tratar dos principais tipos de crimes digitais que vem ocorrendo atualmente na vida das pessoas no Brasil.

O presente projeto tem o objetivo inicial, destacar os principais tipos de crimes digitais desenvolvidos atualmente dentro da sociedade Brasileira, com o intuito de demonstrar a importância de saber manusear os meios digitais. O ordenamento jurídico concedeu a tipificação de crime virtual e fixou a punição aos criminosos, mesmo assim a porcentagem de crimes usando a rede mundial de computadores teve grande aumento, de modo que gerou consigo prejuízos sociais e econômicos, trazendo a sensação de medo e insegurança nas pessoas.

A Lei nº 12.737/2012, publicada em dezembro de 2012, popularmente conhecida como “Lei Carolina Dieckmann”, em homenagem à atriz que teve suas fotos íntimas divulgadas. A norma incluiu no Código Penal os Arts. 154-A e 154-B, dando origem ao crime de invasão de dispositivo informático e alterando ainda os Arts. 266 e 298, do mesmo código (CRESPO,2013).

Nessa vertente o intuito principal é destrinchar sobre as mudanças que ocorreram na legislação Brasileira, no período entre os anos de 2012 até 2023 e abordar casos que houve grande repercussão nacional decorrentes de crimes cibernéticos, na maioria dos casos, tem como finalidade obter vantagens pecuniárias, espalhar informações falsas (Fake News) ou para ter acesso às informações confidenciais e sigilosas tanto de pessoas físicas ou jurídicas. Sendo assim, antes do ano de 2012 no Brasil não havia uma lei para aplicar nos crimes ocorridos no mundo digital, o que tornava a internet como “terra sem lei" posto isso surge o questionamento. Qual a tipificação adequada para os ilícitos penais virtuais?

Por fim o direito é uma matéria dinâmica que deve se adequar às mudanças que ocorrem na sociedade, diante ao advento da tecnologia, as pessoas passaram a ter novas necessidades, sendo assim é evidente que ao longo dos anos a lei deve se adequar e ocorrer mudanças com o intuito de resguardar todos os direitos e deveres no mundo digital. No período da pandemia da COVID-19, onde ocorreu o isolamento social , obrigou a muitos que não faziam o uso da internet a utilizá la, no seu cotidiano, para o trabalho home-office, para pagamentos e transações financeiras, diante esse caso fortuito foi registrado um índice maior da criminalidade na internet, onde os delinquentes teve a percepção de oportunidade para cometerem mais “golpes”.

2. Capítulo I

2.1. Dos crimes virtuais

Este capítulo, abordará as características sobre os crimes digitais e como são tipificados, desta forma o leitor estará apto para entender os aspectos de cada tipo e exemplo de crime como: Homicídio, Estupro Virtual, Estelionato,

Furto Qualificado, Injúria, Calúnia, Difamação, Invasão de dispositivo informático, Pedofilia e Violação de segredo. E compreender como as leis são criadas para alcançar as lacunas que existiam sobre o tema, portanto o capítulo descreve o que é os crimes virtuais no contexto geral e no Brasil, quais os principais tipos de crimes cometidos atualmente, abordamento sobre o marco da Lei Carolina Dieckmann (LEI N. 12.737/12), qual o possível perfil dos delinquentes que o praticam e os principais crimes cometidos no Brasil de grande repercussão nacional e sua relevância para que as normas destinadas ao combate sejam criadas e desenvolvidas para proteção de todos na sociedade.

Emeline Piva Pinheiro (2006), conceituando crimes virtuais, observou que são aquelas infrações penais (crimes ou contravenções penais) praticadas no ambiente virtual, ou seja, em redes sociais, sítios eletrônicos, em redes de compartilhamento ou através de caixa postal eletrônica, ou até mesmo as praticadas fora desses ambientes, porém mediante o uso de dispositivo de informática.

Nesse sentido, Patrícia Peck Pinheiro considera crimes virtuais como:

> [...] condutas de acesso não autorizados a sistemas de informática, resultando em ações destrutivas, afetando sistemas de comunicação, alteração de dados, violação a direitos autorais, todos tipo de ofensas, descriminações e demonstração de ódio e intolerância, exposição de pornografia infantil, terrorismo e muito mais (2013, p.46).

Crimes virtuais são aqueles praticados em ambiente virtual com denominações diversas, não havendo até o presente um consenso de qual seria a melhor definição para os delitos relacionados à tecnologia. Desde modo acredita-se 23 que os conceitos ainda não abarcam todos os crimes ligados a tecnologia por serem inúmeras e de grande multiplicidade as situações envolvendo o ambiente virtual (CRESPO,2013). Sobre esse conceito Augusto Eduardo de Souza Rossini afirma o seguinte:

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

Alan Moreira Lopes (2012) também argumenta que existem vários conceitos e terminologias dadas ao crime cometido por intermédio de computador e seu utilizando a internet. Constatando-se, que o crime de informática é toda ação típica, antijurídica e culpável contra ou pela utilização de processamento automático ou eletrônico de dados ou mesmo pela sua transmissão.

2.2. Os crimes virtuais no contexto geral

O crime cibernético, também conhecido como crime virtual, refere-se às ações ilegais cometidas por meio da tecnologia ou por meio de recursos informáticos. Trata-se de um comportamento ilegal onde o autor recorre a um computador, celular, ou qualquer outro aparelho de informática ou que pode ser conectado à internet, justamente pela aplicação ser realizada em ambiente.

Entretanto, a progressiva mutação tecnológica dificulta o combate a esses crimes, que estão em constante alinhamento com as novas tecnologias. Assim, com o uso incontido e indiscriminado da internet, virtual (JORGE; MILAGRE, 2016).alguns indivíduos com conhecimento em informática passaram a se aprimorar e utilizar esses conhecimentos para roubar informações criptografadas, como já havia sido feito há muito tempo, para obter proveito econômico ou ainda, por mera diversão. (JORGE; MILAGRE, 2016)

Na doutrina, os crimes cibernéticos são divididos em crimes próprios e crimes impróprios. A qualificação como crime próprio ocorre quando as ações do autor do crime visam prejudicar um sistema ou infringir dados, como por exemplo, invasão de sistemas para destruir ou impedir o funcionamento de um servidor de um site ou de uma empresa. A qualificação como crimes impróprios ocorre quando se trata de um crime que também pode ser realizado fora da internet, como por exemplo o estelionato (AZEVEDO; CARDOSO, 2021).

Nos crimes impróprios, destacam-se como mais comum na internet o discurso de ódio. Neste caso, por mais que a liberdade de expressão seja um direito garantido por lei, ela não pode ultrapassar os limites dos direitos de terceiros e se opor à imagem, privacidade, honra, intimidade, etc. porque pode se figurar em crimes contra a honra, assédio ou difamação (AZEVEDO; CARDOSO, 2021).

Sobre o perfil do autor dos crimes, as pessoas imaginam que sejam pessoas com conhecimentos avançados sobre o uso de ferramentas tecnológicas, porém tal percepção é equivocada, pois qualquer pessoas que tem o mínimo de discernimento sobre tal ferramenta pode cometer tais tipos de crimes, portanto a atenção deverá ser redobrada para que não seja prejudicado até mesmo por pessoas conhecidas.

O Superior Tribunal de Justiça publicou levantamento no dia (17/06/2018) sobre precedentes que julgaram crimes cibernéticos no Brasil. Esse tipo de delito afeta anualmente 62 milhões de pessoas e causa prejuízo de US$22 bilhões, de acordo com estudo divulgado no início de 2018 pela empresa de segurança virtual Symantec.

Conforme o Superior Tribunal de justiça:

> O uso cada vez mais intenso e diversificado da internet vem abrindo caminhos para a prática de novas fraudes, ou para novas formas de cometimento de velhos crimes, em casos nem sempre fáceis de enquadrar no ordenamento jurídico. O STJ tem interpretado normas infraconstitucionais em relação aos ilícitos praticados pela rede. O tribunal, por exemplo, decidiu manter preso preventivamente um homem que usou a internet para obter fotos e vídeos com conteúdo erótico e depois extorquiu mulheres para não divulgar as imagens.

Desta forma com a polarização do uso da internet, os criminosos tiveram a percepção que poderiam aplicar golpes e fraudes nas transações comerciais, pois a população tem realizado inúmeras compras pela internet, desse modo, os estelionatários criaram diversos sites clandestinos de vendas de produtos falsificados, enganando o usuário, pois a facilidade de comprar sem sair de casa é o motivo de ter aumentado esses crimes, a população Brasileira abraçaram esse novo tipo de mercado.

2.3. A tipicidade dos principais ilícitos penais cibernéticos.

A análise da tipicidade dos principais ilícitos penais cibernéticos ocorridos atualmente no Brasil, quais as possíveis sanções punitivas aos infratores, características e consequências que causam na vida das vítimas, apontando a importância da conscientização e responsabilidade para não se tornarem alvo de tais ilícitos.

À medida que a tecnologia se torna cada vez mais segura e eficiente para os humanos, essa prática se torna mais comum porque não necessita que o próprio criminoso invada o celular da vítima, pelo contrário, é a vítima que acaba passando seus dados sem perceber. Essa relação entre a prática do crime e a estratégia utilizada parece difícil de entender, porém, trata-se de uma estratégia de ponte para um crime maior, seja roubo de informações pessoais, fotos privadas, clonagem de cartões, informações confidenciais da empresa, etc. (SILVA et al., 2021).

2.4. Estupro Virtual

De acordo com Mireya Suárez (1995, p. 05), entende-se o crime sexual como sendo um “tipo específico de violência que se configura quando alguém força outro a praticar qualquer tipo de ato sexual”. Ou seja, configura-se crime sexual quando o ato sexual é realizado sem o consentimento da vítima e contra sua vontade, decorrendo assim, danos físicos e/ou emocionais.

Diversos doutrinadores, dentre eles destaca-se Jorio (2019), tratando de crimes sexuais virtuais como a violação da liberdade sexual e o desrespeito e indocilidade ao princípio da dignidade da pessoa humana, assegurado a todos pela Constituição Federal brasileira.

A liberdade sexual pressupõe as escolhas livres e conscientes concernentes às práticas sexuais e à vida sexual em geral. Dispor de liberdade sexual implica em manter o poder de decisão sobre como, quando e com quem serão praticados atos de cunho sexual. Proteger a liberdade sexual, diante disso, significa assegurar o direito de que o titular desse bem jurídico possa determinar livremente sua sexualidade e seu comportamento sexual desde que, com suas opções, não ofenda bens jurídicos alheios. (JORIO et al., 2019, p.43)

O estupro virtual é constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso, portanto o ato de chantachear ou oferecer dinheiro em troca de fotos de nudes, videos ou até mesmo para ter conjunção carnal através da internet poderá ser sancionado perante a lei.

De acordo com o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, passa a vigorar:

> Art. 217-B. Assediar, instigar ou constranger, por qualquer meio de comunicação, menor de 14 (catorze) anos a se exibir de forma pornográfica ou sexualmente explícita:
> Pena – reclusão, de 4 (quatro) a 12 (doze) anos.
> Parágrafo único. Incorre na mesma pena quem pratica as ações descritas no caput com alguém que, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato."

Os indivíduos tentam ludibriar a vítima, por meio da telecomunicação para obterem alguma vantagem seja sexualmente ou em pecúnia, infelizmente as crianças acabam sendo o alvo maior dos criminosos, portanto a educação digital é importante para não se prejudicarem ao navegarem. Até mesmo em aplicativos de jogos online, existe a possibilidade de troca de mensagens, portanto os responsáveis deverão ficarem atentos aos smartphones e computadores de seus dependentes.

Como o nome mesmo diz "estrupo virtual", é toda ação ilícita que o criminoso comete com o intuito de violar a integridade sexual de outrem, portanto o ato ilícito não se configura através da conjunção carnal, mas na tentativa ou dolo de adquirir fotos, vídeos, com o intuito de chantagear ou expor a vítima.

Para exemplificar esse tipo de crime, tem-se a seguinte situação:

> […] Determinada pessoa passa a conhecer alguém em uma rede social. A partir disso, se inicia um flerte e a troca de nudes. Em determinado momento, se inicia o recebimento de ameaças e que as imagens serão expostas. Para que isso não ocorra, a pessoa é "obrigada" a se despir e a se masturbar durante uma chamada de vídeo. Atenção: isso é um estupro virtual (DUARTE, 2020, p. 02).

Pode-se entender de maneira geral, que o "estupro é um ato criminoso que atenta contra a liberdade de escolha sexual da vítima" (OLIVEIRA, 2010, p. 15). Segundo Oliveira (2010, p 20) ´´A sua prática decorre dos animais, que muitas vezes praticam atos sexuais contra as fêmeas, agredindo-as em quase todos os casos. Assim, pode-se afirmar que o estupro é uma ação que viola a disponibilidade do indivíduo, com uma atitude primitiva e selvagem, como nos animais``.

O "estupro virtual" pode ter a sua ocorrência de várias maneiras. A título de exemplo ele pode ser vislumbrado quando um indivíduo através de alguma

rede social (WhatsApp, Facebook, por exemplo) intenciona constranger, envergonhar ou ameaçar outrem a tirar a roupa na frente de uma webcam, praticar masturbação ou se fotografar nu (GOMES, 2017).

Discorrendo sobre essa questão Camargo (2019) explica que no caso do estupro físico existe o uso da força bruta como forma de dominação da vítima e posteriormente realizar o ato sexual. No caso do estupro virtual ele se configura na base do domínio psicológico, onde o estuprador(a) age por meio de ameaças, chantagem, constrangimento, etc. Por não haver o consentimento da vítima, entendese que houve o crime de estupro.

2.5. Estelionato

O chamado “crime de estelionato” é aquele que o autor é pratica golpes com o intuito de enganar a vítima para obter algum tipo de vantagem, na maioria dos casos em pecúnia, com novas formas de fazer o pagamento atualmente, o chamado “PIX” (pagamento instantâneo brasileiro), tem milhares de casos de pessoas sofreram prejuízos por serem enganadas e realizarem transações erradas.

DE acordo com o DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940, Código penal:

> 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 um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

O estelionato, conforme previsto no artigo 171 do Código Penal Brasileiro, é um dos delitos que mais desafia a aplicação da lei no campo do Direito Penal. Ficou claro que o estelionato não se limita a uma mera fraude financeira, mas envolve uma série de fatores complexos, incluindo o dolo, a confiança da vítima e a obtenção de vantagem indevida.

A lei 14.155/21 também alterou o artigo 70 do Código de Processo Penal, tratando da competência para o julgamento de algumas das modalidades do crime de estelionato. O §4° do referido artigo foi incluído com a seguinte redação:

> § 4º Nos crimes previstos no art. 171 do Decreto-lei 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante

> depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção (BRASIL, 2021).

Os infratores buscam vítimas na internet para obter dados pessoais ou bancários das pessoas, visto que a todo instante as pessoas compartilham e acessam diversos aplicativos na rede, destarte podem ser enganadas e sofrerem algum tipo de prejuízo financeiro. Atualmente o número do boletim de ocorrência em decorrência de fraude de Pix, o pagamento instantâneo tem aumentado, pois as pessoas se tornam alvo do estelionatário, pessoa que causa fraude a terceiros.

O termo estelionato, caracteriza o uso de falsa identidade, portanto no direito brasileiro, uma garantia e proteção à imagem de cada sujeito, de forma com que cada atitude pode ter uma implicação, seja em âmbito civil ou penal. O crime de falsa identidade é um delito formal, conforme ensina Fernando Capez:

> Consuma-se o crime com o ato de atribuir-se ou atribuir a outrem falsa identidade. Trata-se de crime formal, de maneira que o delito se perfaz 8 independentemente da obtenção da vantagem ou da produção de dano a terceiro (CAPEZ, 2020, s.p.).

Sendo assim, ao utilizar a rede de computadores, para criar perfis falsos com o intuito de adquirir vantagem indevida ou causar dano a outrem, pode responder pelo crime de falsa identidade e não é necessário que a vantagem seja alcançada, portanto a mera tentativa se caracteriza como crime.

2.5.1. Caso de estelionato no Brasil, o crime mais recorrente em 2023

De acordo com a matéria publicada no dia 22/07/2023 pela câmara de notícias, está ficando cada vez mais recorrente em Mato Grosso do Sul, os golpes que são realizados na internet, são os crimes virtuais mais denunciados em ocorrências no Estado. De janeiro a junho deste ano, segundo a Secretaria de Estado de Segurança Pública (Sejusp), 38,08% dos casos registrados se tratam de estelionato, seguido por preservação de direito 11,04%, e de fraude eletrônica 9,39% das ocorrências.

Conforme informado pela Sejusp, em 2022, foram registrados 1.801 crimes em Mato Grosso do Sul entre os delitos mais praticados na internet Os dados foram disponibilizados ao Correio do Estado pela Sejusp, por meio da Superintendência de Inteligência em Segurança Pública de Mato Grosso do Sul. De acordo com as informações foram registrados 1.197 crimes no interior e 604 crimes cometidos virtualmente na Capital.

O crime de estelionato virtual tem se destacado como um dos mais praticados no país devido a uma série de fatores que facilitam sua ocorrência e dificultam a identificação e punição dos infratores. Um dos pontos importante de destacar é a facilidade de acesso à tecnologia pois devido o aumento do acesso à internet e o uso massivo de dispositivos eletrônicos, mais pessoas estão conectadas, tornando-se potenciais alvos para os criminosos virtuais. Muitas pessoas ainda não têm pleno conhecimento sobre medidas de segurança cibernética, o que os torna vulneráveis a técnicas sofisticadas aos golpes virtuais, pois os criminosos virtuais muitas vezes operam de forma anônima ou por trás de uma rede complexa de computadores, tornando difícil a identificação de sua verdadeira identidade ou localização.

2.6. Furto qualificado

De acordo com Código Penal o agravante do furto qualificado por meio eletrônico, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento similar. Nesse caso, a pena será de reclusão de quatro a oito anos e multa.
Para começar a análise, transcrevo o dispositivo legal a ser analisado:

> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel: Pena - reclusão, de um a quatro anos, e multa.
> § 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.

O dispositivo legal dispõe que caso o crime for praticado contra idoso ou vulnerável, a pena aumenta de um terço ao dobro. E, se for praticado com o uso de servidor de informática mantido fora do país, o aumento da pena pode ir de

um terço a dois terços, portanto houve algumas mudanças legislativas relevantes para diminuir o número de crimes ocorridos no país.

A atualização do Código Penal foi fundamental pois, com o avanço do acesso a internet, revelaram novas formas de furto que não eram previstas na norma anterior. Atualmente, é possível cometer um furto sem precisar invadir a casa da pessoa, através de uma porta ou janela, usando apenas um dispositivo eletrônico ou informático. Esse tipo de crime é realizado de forma virtual porém é difícil de detectar o infrator.

O furto qualificado por meio eletrônico envolve a subtração de bens ou valores utilizando-se de meios digitais, sem a autorização do titular ou responsável pelos ativos. A legislação brasileira, especialmente o Código Penal, não possui uma tipificação específica para crimes cibernéticos, incluindo o furto qualificado por meio eletrônico. No entanto, esse tipo de delito pode ser enquadrado em disposições legais preexistentes.

O artigo 155 do Código Penal, que trata do crime de furto, pode ser aplicado ao contexto dos crimes cibernéticos. Em sua forma qualificada, prevista no § 4º do mesmo artigo, o furto é agravado quando há destruição ou rompimento de obstáculo à subtração da coisa, quando o agente comete o crime com abuso de confiança, mediante fraude, escalada ou destreza, ou com emprego de chave falsa. Esses elementos podem ser adaptados à realidade digital.

Dentro do âmbito cibernético, o furto qualificado se manifesta quando indivíduos utilizam métodos como invasão de sistemas, engenharia social (como o phishing), subtração de senhas e outras artimanhas fraudulentas para ilegalmente apropriar-se de ativos eletrônicos, sejam eles bens ou valores. Agravantes, como a utilização de software malicioso (malware) ou a execução do ato criminoso de forma coordenada, desempenham um papel fundamental na determinação do caráter qualificado do furto.

É importante discorrer sobre tal crime de furto pois é considerado um dos mais frequentes no país e que a atualização do artigo 155 do Código Penal é de extrema importância para todos, pois garante maior proteção para as vítimas de crimes cibernéticos e para a população mais vulnerável.

2.7. Dos crimes contra a honra

A honra é classificada como o conjunto de qualidades intelectuais, físicas ou morais de um indivíduo, pois aponta seu valor social, sua rejeição ou aprovação em meio a sociedade que está inserido. Tal elemento é indispensável para o convívio social e desenvolvimento pessoal, portanto há proteção legal conforme a legislação vigente.

Segundo Magalhães Noronha 1 , conceitua-se honra "[...] como o complexo ou conjunto de predicados ou condições da pessoa que lhe conferem consideração social e estima própria".

Para Guilherme de Souza Nucci2 a honra pode ser traduzida da seguinte forma:

> Conceito de 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; enfim, na sua postura calcada nos bons costumes. Essa apreciação envolve sempre aspectos positivos ou virtudes do ser humano, sendo incompatível com defeitos e más posturas, embora não se trate de um conceito absoluto, ou seja, uma pessoa, por pior conduta que possua em determinado aspecto, pode manter-se honrada em outras facetas da sua vida. Honra não pode ser, pois, um conceito fechado, mas sempre dependente do caso concreto e do ângulo que se está adotando. Não é demais ressaltar que sua importância está vinculada à estima de que gozam as pessoas dignas e probas no seio da comunidade onde vivem.

Destaque-se, ainda, o entendimento de Nelson Hungria 3 , para o qual a honra deve ser entendida da seguinte forma:

> [...] quer como o sentimento de nossa dignidade própria (honra interna, honra subjetiva), quer como o apreço e respeito de que somos objetos ou nos tornamos merecedores perante os nossos concidadãos (honra externa, honra objetiva, reputação, boa fama)

Diante desse recente entendimento sobre o conceito de honra, percebemos que é possível examinar a honra de duas maneiras distintas: a perspectiva objetiva e a perspectiva subjetiva. Isso representa a tradicional divisão na doutrina da honra em duas categorias separadas, nomeadamente, a honra objetiva e a honra subjetiva.

Nesse sentido giza Castelo Branco4:

> A honra subjetiva é o sentimento de cada um a respeito de seus atributos físicos, intelectuais, morais e demais dotes da pessoa humana. É o apreço próprio, a autoestima em relação a tais atributos. A honra objetiva é a reputação, a boa fama, o respeito e a consideração de que o cidadão se torna merecedor perante a sociedade. É o sentimento alheio sobre os atributos da pessoa.

É importante destacar que a proteção da honra é uma necessidade crucial, uma vez que a importância de preservar a honra não se restringe apenas ao indivíduo, mas se estende a toda a sociedade, pois é essencial para a convivência na comunidade.

Incontestavelmente, é um fato que todos possuem o direito à honra, uma vez que ela está inserida nos direitos da personalidade, que também são chamados de "direitos sobre a própria pessoa" ou "direitos individuais". A honra, conforme estipulado no artigo 5º, inciso X, da Constituição Federal de 1988, é um bem considerado constitucionalmente inviolável. Referido dispositivo constitucional assevera o seguinte:

Art. 5º - Omissis: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

No entanto, a proteção legal da honra não se limita à previsão constitucional mencionada anteriormente, A honra possui proteção e legitimidade também no Código Penal Brasileiro, tendo disposições legais e figuras típicas que representam ao crime contra a honra que abordaremos em sequência.

2.8. Calúnia

Caluniar é dizer de forma mentirosa que alguém cometeu crime. Para a ocorrência do crime de calúnia é essencial que haja atribuição falsa de crime. Ex: dizer que fulano furtou o dinheiro do caixa, sabendo que não foi ele, ou que o dinheiro não foi furtado.

> 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.

O crime de calúnia por meio eletrônico não difere substancialmente do crime de calúnia tradicional previsto no Código Penal. Ambos os tipos de calúnia envolvem a imputação falsa de fatos criminosos a alguém, e as sanções legais se aplicam igualmente a ambos os contextos.

A jurisprudência e a legislação brasileira têm demonstrado um compromisso em lidar com os crimes cibernéticos, incluindo a calúnia por meio eletrônico, a fim de proteger a honra e a reputação das pessoas no ambiente digital. No entanto, é essencial que o sistema legal continue a evoluir para enfrentar os desafios em constante evolução apresentados pelo mundo digital e pelos crimes cibernéticos.

A calúnia virtual, também conhecida como difamação online, é uma conduta criminosa que ocorre no ambiente digital, caracterizada por disseminar informações falsas, difamatórias ou prejudiciais sobre uma pessoa, empresa ou entidade, com o intuito de prejudicar a reputação da vítima.

Tal crime envolve a publicação de informações falsas, seja por meio de textos, imagens, vídeos ou outros meios digitais, tais delitos ocorrem por meio de plataformas onlines e instantâneas: sites, e mails, blogs mensagens instantâneas entre outros, com o objetivo de prejudicar a honra e moral da vítima.

É importante lembrar que, embora a liberdade de expressão seja um direito fundamental em muitas jurisdições, essa liberdade não dá a ninguém o direito de difamar, caluniar ou prejudicar a reputação de outras pessoas de forma injusta ou maliciosa. Portanto, é essencial que os usuários da internet ajam com responsabilidade e respeitem as leis locais ao interagir online. Além disso, as vítimas de calúnia virtual podem buscar apoio da justiça para defender seus direitos e buscar reparação pelos danos causados.

2.9. Difamação

Difamação é a imputação ofensiva atribuída contra a honra e dignidade de alguém com a intenção de desacreditá-lo na sociedade em que vive, e provocar contra ele desprezo ou menosprezo público. Difamar é tirar a boa fama ou o crédito, desacreditar publicamente atribuindo a alguém um fato específico negativo, para ocorrer o crime de difamação o fato atribuído não pode ser considerado crime. Exemplo: Dizer para os demais colegas que determinado funcionário costuma trabalhar embriagado. Vejamos a aplicação no código penal:

> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:

Pena - detenção, de três meses a um ano, e multa.

A difamação, nos termos do Código Penal brasileiro, está prevista no artigo 139 e consiste em imputar a alguém, falsamente, fato ofensivo à sua reputação. A característica fundamental da difamação é a divulgação de informações que prejudiquem a imagem ou honra de uma pessoa.

No contexto dos crimes cibernéticos, a difamação por meio eletrônico ocorre quando alguém utiliza dispositivos ou meios digitais, como redes sociais, blogs, mensagens eletrônicas, ou outras formas de comunicação online, para disseminar informações difamatórias a respeito de outra pessoa.

A legislação brasileira não diferencia a difamação tradicional da difamação por meio eletrônico. Ambas são enquadradas nas disposições do Código Penal e sujeitas às mesmas sanções legais. O meio eletrônico não isenta o autor do crime de responsabilidade legal, e as mesmas regras que se aplicam à difamação offline também se aplicam à difamação online.

Tal delito atinge diretamente a honra objetiva da vítima, de maneira semelhante à difamação, requer que seja atribuído um fato a alguém. No entanto, não é necessário que esse fato seja consumado, basta que tenha o potencial de manchar a reputação da pessoa, independentemente de ser verdadeiro ou falso.

O infrator deve mencionar um evento com detalhes específicos, incluindo o momento, o local e as pessoas envolvidas. Se o autor, por exemplo, apenas acusar a vítima de ser alcoólatra, estará cometendo o crime de injúria. No entanto, se ele descrever em detalhes que a vítima estava cambaleando nas ruas, visivelmente embriagada, então estará configurado o crime de difamação.

2.10. Injúria

A Injúria consiste em aplicar palavras ou qualidades ofensivas a alguém, exibir defeitos ou opinião que desqualifique a pessoa, atingindo sua honra e moral. O exemplo mais comum que ocorre frequentemente todos os dias são os xingamentos, palavras de baixo calão para ofender outrem.

No que diz respeito à injúria, Jesus (2011, p. 261) a conceitua da seguinte forma: “ofensa à dignidade ou decoro de outrem”, estando prevista no Código Penal em seu art. 140:

> Artigo 140. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena – detenção, de 1 (um) a 6 (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 consistia em outra injúria. § 2º Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se consideram aviltantes: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa, além da pena correspondente à violência. § 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência; Pena – reclusão de 1 (um) a 3 (três) anos e multa..

Diferentemente da calúnia e da difamação, a injúria diz respeito à honra subjetiva, que relaciona-se ao sentimento próprio de cada indivíduo no que tange aos seus aspectos morais, intelectuais ou físicos (CAPEZ, 2011).

Nos crimes de injúria o elemento subjetivo é o dano, o qual tem fundamento em atribuir a outra pessoa qualidade negativa, ou até mesmo a vontade de injuriar alguém. Para Jesus (2011), a injúria consuma-se a partir do momento em que o ofendido toma ciência da qualidade negativa que lhe foi atribuída.

Assim, Bittencourt (2011) complementa que diferentemente da calúnia e da difamação, no caso da injúria basta que somente a vítima tome ciência da ofensa, uma vez que não se trata do aspecto externo da honra, mas sim a auto estima, o aspecto interno.

Capez (2011) ainda afirma que a injúria não precisa ser pronunciada na presença do ofendido, é necessário apenas que o mesmo tome conhecimento da ofensa, ou através de terceiros, por correspondência, ou qualquer outro meio.

2.11. Invasão de dispositivo informático

É um dos delitos que tipifica o termo do cibercrime, muitas empresas e pessoas já sofreram prejuízos decorrente esse crime, destarte, a legislação traz fundamentos para que seja sancionado tais ilícitos, vejamos de acordo com o Código Penal - Decreto -Lei nº 2.848, de 7 de dezembro de 1940.

> 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.

A invasão de dispositivo informático é um crime cibernético grave, tipificado no Código Penal brasileiro e regulamentado por outras normativas relacionadas à proteção de dados pessoais. A legislação e a jurisprudência brasileiras estão alinhadas com a necessidade de combater eficazmente os crimes cibernéticos, incluindo a invasão de dispositivos informáticos.

2.12. Pedofilia

A pedofilia Virtual corresponde em produzir, publicar, vender ou armazenar conteudos pornograficos de crianças ou seja de pessoas incapazes pela rede mundial de computadores, através de sites de bate papos e salas virtuais, alguns casos os juvenis são manipulados para enviarem fotos e se exibir- se para os criminosos. a Lei n. 11.829/2008 proporcionou ao alterar o Estatuto da Criança e do Adolescente (ECA), a fim de combater as condutas relacionadas à pedofilia na internet.

A Lei n. 13.718/2018 acrescentou ao Código Penal o artigo 218-C, com a seguinte redação:

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave [...] (BRASIL, 2019,p. 542).

A erradicação da pedofilia virtual exige um esforço conjunto das autoridades, da sociedade civil, das empresas de tecnologia e de todos os cidadãos. É fundamental que o sistema legal e as políticas públicas estejam em constante evolução para enfrentar esse desafio em constante mutação e, assim, proteger as crianças e adolescentes contra essa forma horrenda de exploração.

A luta contra a pedofilia virtual é uma responsabilidade coletiva e uma prioridade urgente, e todos devem se empenhar para criar um ambiente virtual seguro para as gerações futuras.

3. Capítulo III

3.1. Legislação e marco regulatório

Neste capítulo, irei abordar as principais regulamentações que tratam de crimes cibernéticos no Brasil. Isso envolverá uma análise aprofundada do Marco Civil da Internet, a Lei Carolina Dieckmann e outras legislações relevantes que estabelecem responsabilidades e penalidades para criminosos cibernéticos.

No Brasil, houve aprimoramentos na legislação relacionada aos delitos cometidos na internet, como resultado de casos amplamente divulgados pela mídia. Isso levou a um aumento da preocupação com o tema, resultando na implementação de medidas punitivas mais eficazes para crimes virtuais.

3.2. Lei Carolina Dieckmann (LEI N. 12.737/12)

Essa lei foi um avanço fundamental na legislação para combate aos crimes informatizados, e diminuir as lacunas existentes sobre os casos cibernéticos. O caso da atriz Carolina Dieckmann foi um crime cibernético, exemplo de atentado. A autora teve sua caixa de e-mail hackeada e seu conteúdo pessoal publicado online. A princípio, os infratores tentaram extorquir a atriz, ameaçando-a de publicar na web todas as imagens íntimas as quais tiveram acesso, mas quando a mesma se recusou a pagar a quantia exigida e levou o caso às autoridades, os infratores divulgaram as referidas imagens na internet.

É interessante observar que as leis que surgiram a partir de 2012, que versam sobre a temática de cibercrime, foram resultado de pressão da mídia sobre o poder legislativo. Nesse cenário, cita-se as Leis nº 12.735/12 e 12.737/12, sendo que a primeira trouxe alteração legislativa do Código Penal, do Código Penal Militar e da Lei de Preconceito, tipificando os crimes realizados na internet, e a segunda dispõe a respeito da tipificação dos crimes informáticos, além de alterar o Código Penal (CRUZ; RODRIGUES, 2018).

A Lei Ordinária 12.735/12 se tratou da transformação do projeto de lei 84/99, e foi nomeado de “Lei Azeredo”, trazendo as primeiras disposições sobre crimes, penas e outras providências cometidos por meio virtual, que alterou

somente o inciso II do parágrafo 3° do art. 20 da Lei n° 7.716/89 (Lei do Crime Racial), para proibir conteúdos discriminatórios na rádio, televisão ou internet, e por qualquer forma possível, a pedido do juiz, e para combater as atividades criminosas praticadas através da Internet ou de sistemas informáticos, determinou também que a Polícia Judiciária tenha o responsabilidade de estabelecer delegacias especiais de polícia (BRASIL, 2012a).

Porém, essa lei ainda não atribuía a proteção aos objetos jurídicos sobre a liberdade pessoal de usuários de equipamentos de informática, devido a essa "lacuna", ocorreu o escândalo midiático da divulgação de fotos íntimas da atriz Carolina Dieckmann, tornando presente o problema em questão, e levando a sanções urgentes contra a referida do caso, sendo criada a Lei nº 12.737/2012.

Caetano (2015), destaca como a pressão da mídia contribuiu consideravelmente, uma vez que o caso ganhou repercussão nacional, dessa forma, a lei permitiu a tipificação criminal de delitos informáticos, alterando o Código Penal ao acrescentar dois artigos, o art. 154-A e 154-B.

> 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, 2012b).

No artigo 154-B, conforme os crimes tipificados no artigo acima, é praticado somente por intermédio de órgão, a menos que o crime seja cometido contra órgão da administração pública direta ou indireta de qualquer poder da União, seja Estadual, do Distrito Federal ou Municipal (BRASIL, 2012b).

Além da alteração descrita anteriormente, a Lei n° 12.737/2012, também alterou o artigo 266 e 298 do Código Penal, incluindo no crime de interrupção de serviço, os serviços telemáticos ou de informação de utilidade pública; e nos crimes de falsificação de documentos foi incluído a falsificação de cartões de crédito/débito (BRASIL, 2012b).

Um dos principais problemas também destacados desta lei remete a, que ao ser considerado culpado, pode levar entre 3 meses a 1 ano de reclusão e multa. Situação que levou a inúmeras críticas, pois ao passar pouco tempo de reclusão, não torna a lei totalmente preventiva de que os responsáveis pela

prática do crime não vão continuar cometendo-os, ressaltando a alta taxa de golpes sofridos pelos brasileiros anualmente. (BARROS, MATHEUS - Página 22 - 2021)

3.3. Marco civil da Internet (LEI N. 12.965/14)

A Lei n.º 12.965/14 foi submetida à Assembleia Nacional em 2011 pelo chefe do Poder Executivo, transformando-a na Lei n.º 2.126/2011. Assim, foi publicado em 23 de abril de 2014. Seu principal objetivo é estabelecer princípios, garantias e obrigações para o uso da Internet no Brasil.

A Lei n° 12.965/14, popularmente conhecida como Marco Civil da Internet certifica um procedimento mais ágil para a remoção de mídias íntimas que foram expostas no ambiente virtual, e a Lei nº 13.718/2018, que trouxe um novo delito no art. 218-C, do Código Penal:

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave. (BRASIL, 2018).

Devido a crescente funcionalidade que a internet foi adquirindo e seu acesso foi se tornando essencial à vida das pessoas, a lei foi criada com intuito de regularizar essas utilizações e eliminar a ideia de que a internet é uma “terra sem lei”. Nascimento (2019) explica que o Marco Civil da Internet ficou popularmente conhecido como a Constituição da 22 Internet Brasileira e é composto de 10 (dez) princípios elaborados pelo Comitê Gestor da Internet brasileira.

Os 10 (dez) princípios previstos na Lei do Marco Civil são:

> liberdade, privacidade e direitos humanos; governança democrática e colaborativa; universalidade; diversidade; inovação; neutralidade da rede; inimputabilidade da rede; funcionalidade, segurança e estabilidade; padronização e interoperabilidade; e ambiente legal e regulatório.

Seguindo esses princípios, a lei também permitiu a tipificação de diversos termos informáticos, como registro de conexão, sendo o conjunto de dados sobre a hora inicial e final do acesso à internet. E os registros de acesso a aplicações de internet, constando os dados de acessos realizados, sendo descrito a hora e data, a partir de determinada aplicação (BRASIL, 2014).

3.4. Cyberbullyng (LEI N. 13.185/15)

O “cyberbullying” (Assédio virtual) refere se a prática de agressão moral e manifestação de práticas hostis via plataformas digitais para atingir determinadas pessoas, Esse crime, bullying virtual tem o intuito de ridicularizar, assediar e/ou perseguir alguém, tal delito é praticado na maioria das vezes por perfis falsos para expor ou mostrar informações sobre outrem, com o intuito de prejudicá-lo, os adolescentes são o público alvo desse tipo de delito, e pode causar diversos traumas, ansiedade e depressão.

Para evitar esse perigo dos jovens serem manipulados, e assediados no meio digital, a educação virtual deveria se tornar uma matéria obrigatória nas escolas, a orientação e vigilância dos pais são fundamentais e importantes para que seus filhos não se prejudiquem por falta de informação.

De acordo com a lei Nº 13.185 - Parágrafo único:

> Há intimidação sistemática na rede mundial de computadores (**cyberbullying**), quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial.

O agressor tem a sensação de segurança no momento que está cometendo o delito, porém ele pode ser punido. O cyberbullying é passível de punição através do Código Penal, pois quando se configura crimes contra a honra, são eles: calúnia, difamação e injúria que iremos abordar posteriormente, infringem o artigo 138 do Código Penal vigente. Já os crimes de injúria racial e ataques racista infringem o artigo 140 do Código Penal e ao expor imagens de conteúdo íntimo de outrem transgride o artigo 2018-C do Código penal incluído pela lei 13.718, de 2018.

Em todos os casos a vítima tem proteção jurídica estatal de acordo com as punições previstas na legislação. A pena pode chegar a quatro anos de

reclusão. Na esfera Civil dependendo do caso em questão o agressor pode ser condenado a pagar indenizações por danos morais, porém há uma regra específica para infratores menores de idade, os responsáveis respondem subsidiariamente diante ao tribunal e podem ser condenados ao ressarcimento de indenização à vítima.

3.5. Lei Geral de Proteção de Dados Pessoais- LGPD (LEI N. 13.709/18)

Foi sancionada a lei nº 13.709 em 14 de agosto de 2018, que ficou conhecida como Lei Geral de Proteção de Dados (LGPD), baseada nas normas europeias de proteção de dados. Desta forma, essa lei buscou a autodeterminação informativa para fundamentar as principais questões sobre a proteção dos dados (art. 2º, inciso II). Com ela, ocorreram mudanças em relação ao entendimento do acesso às informações em banco de dados privados (LARA, 2019).

Para compreender a LGPD, é preciso analisar os seus princípios e bases legais. Por conseguinte, quando trata de dados pessoais a lei tem como base: a finalidade de tratá-los de forma específica, legítima, explícita e informada; a adequação à coerência do uso da informação solicitada; a necessidade do uso, limitado de dados essenciais para a finalidade apresentada; o livre acesso de consulta da pessoa titular; a qualidade dos dados, garantia da veracidade e atualidade deles; a transparência, ao titular, do uso dos dados; a segurança para impedir a invasão, destruição, perda ou difusão destes; a prevenção, a fim de evitar danos em razão do tratamento; a não discriminação, ou seja, não é permitido descriminar ou promover abusos conta os seus titulares; a responsabilidade e prestação de contas das empresas para comprovar que estão agindo de acordo com a lei (BRASIL, 2018).

3.6. Mudanças legislativas

No contexto do Direito Penal, é crucial que a legislação evolua periodicamente para garantir a prevenção e a repressão eficaz da criminalidade

por meio da aplicação justa das penas. Nesse sentido, é necessário explorar o conceito e algumas características peculiares do crime, que vai além de ser apenas um evento social, mas sim um episódio na trajetória de um indivíduo. Portanto, não se deve abordar o crime de forma isolada, desvinculada das circunstâncias que o envolvem e das implicações que ele tem na vida do acusado.

Com toda essa evolução, a humanidade se depara com novas necessidades e alcançar novos objetivos, resultando em transformações que ocorrem em 26 em todas as áreas do conhecimento, inclusive as ciências jurídicas. Sendo assim, pode-se dizer que o direito é dinâmico e acompanha a sociedade em sua evolução (PINHEIRO, 2013).

Com a necessidade de endurecer as penas e de tornar a lei aplicável em mais casos tipificados foi sancionada a Lei 14.155 de 27 de maio de 2021, trazendo consigo endurecimento das penas em seus Artigos:

> Art. 1º O Decreto-Lei nº 2.848, de 7 de 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:
> § 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 12 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. Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resultar prejuízo econômico. Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

O especialista em direito digital Dr. Luiz Augusto D'Urso, advogado do escritório D'Urso e Borges Advogados Associados, avaliou a importância da alteração, pois houve um crescimento exorbitante das invasões e golpes pela Internet, principalmente durante a pandemia. Segundo o próprio advogado:

> "O problema é que muitas invasões causavam prejuízos gigantescos, até com vazamentos de dados acessados, sendo que as penas para estas invasões eram de apenas 3 meses a 1 ano. Agora, com este aumento, nota- se uma resposta penal muito mais proporcional, com penas de reclusão de 1 a 4 anos, podendo chegar em até 5 anos, se houver obtenção de conteúdos sigilosos."

Tais alterações no ordenamento jurídico é vista como ponto positivo, pois houve aumento para o crime citado anteriormente o “estelionato” por meios digitais, com pena de reclusão de 4 a 8 anos e o aumento de 1/3 ao dobro da pena se o crime é praticado contra idoso ou vulnerável, esperando assim que haja efeito imediato na inibição da prática delituosa. A função de tais mudanças é para inibir e diminuir esses delitos e melhorar a vida de todos nós.

Assim como dispõe Matsuyama e Lima (2017) , o princípio da legalidade consiste em um dos mais importantes do ordenamento penal brasileiro. Ele encontra-se positivado no art. 5º, inciso XXXIX da Constituição Federal de 1988: “Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”, também é perceptível a menção ao referido princípio no art. 1º do Código Penal. Nesse sentido, Rogério Greco (2015) define:

> É o princípio da legalidade, sem dúvida alguma, o mais importante do Direito Penal. Conforme se extrai do art. 1º do Código Penal, bem como do inciso XXXIX do art. 5º da Constituição Federal, não se fala na existência de crime se não houver uma lei definindo-o como tal. A lei é a única fonte do Direito Penal quando se quer proibir ou impor condutas sob a ameaça de sanção. Tudo o que não for expressamente proibido é lícito em Direito Penal. (GRECO, 2015, p.144).

Conforme estabelece a própria Lei Maior, no ordenamento jurídico brasileiro, não se concebe que um fato seja considerado como crime sem que exista lei anterior que descreva tal conduta como delituosa. A legislação consiste na única fonte capaz de impor punição à prática de atos que ela mesma caracteriza como sendo ilícitos, configurando na limitação ao poder do Estado de interferir na esfera de liberdades dos indivíduos. O autor Cleber Masson (2015), entende que o princípio em questão, versa pela:

> [...] exclusividade da lei para a criação de delitos (e contravenções penais) e cominação de penas, possuindo indiscutível dimensão democrática, pois revela a aceitação pelo povo, representado pelo Congresso Nacional, da opção legislativa no âmbito criminal. De fato, não há crime sem lei que o defina, nem pena sem cominação legal (nullum crimen nulla poena sine lege). (MASSON, 2015, p.82).

4. Capítulo IV

4.1. Classificação dos Crimes Virtuais e seus sujeitos

Neste capítulo, será abordada a classificação dos crimes virtuais no Brasil, distinguido entre crimes virtuais próprios e impróprios. Os crimes virtuais próprios são aqueles que são perpetrados exclusivamente no ambiente digital, enquanto os crimes virtuais impróprios estão relacionados a atividades ilegais que têm conexões tanto online quanto offline. Essa distinção é crucial para entender a complexidade dos cibercrimes e sua aplicação legal.

Os Crimes virtuais podem ser classificados em próprios ou puros e, ainda, em impróprios ou impuros, vejamos:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial. (FERREIRA apud CARNEIRO, 2012, [n.p.]).

A classificação dos crimes virtuais em próprios e impróprios é fundamental para compreender a complexidade desse fenômeno em constante evolução. À medida que a sociedade se torna cada vez mais digital, é crucial que o sistema legal esteja preparado para lidar com uma ampla variedade de atividades criminosas que ocorrem no ambiente digital e que frequentemente transcendem as fronteiras físicas.

4.2. Crimes virtuais próprios

Os crimes virtuais próprios envolvem ações que são intrinsecamente ilegais no ambiente digital. Estes crimes são cometidos diretamente no espaço cibernético e geralmente não requerem ação fora da internet para serem perpetrados.

Os crimes virtuais próprios são aqueles em que o sujeito ativo utiliza o sistema informático do sujeito passivo, no qual o computador como sistema tecnológico é usado como objeto e meio para execução do crime.

Nessa categoria de crimes está, não só a invasão de dados não autorizados, mas toda a interferência em dados informatizados como, por exemplo, invasão de dados armazenados em computador seja no intuito de modificar, alterar, inserir dados falsos, ou seja, que atinjam diretamente o software ou hardware do computador e só podem ser concretizados pelo computador ou contra ele e seus periféricos.

Para alguns doutrinadores, como Marco Túlio Viana, crimes virtuais próprios: “são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)” (VIANA, 2003 apud CARNEIRO, 2012)

Alguns elementos que classificam os cibercrimes próprios são: Meio Digital: A infração ocorre inteiramente na internet, em redes sociais, websites, e-mails, aplicativos ou outros canais online. Falta de Manifestação Física: Não há um componente físico substancial associado ao crime, como o roubo de um objeto físico.Uso de Tecnologia: Geralmente, os cibercriminosos fazem uso de tecnologia avançada, como malware, phishing ou engenharia social, para cometer suas ações.Lesão ou Prejuízo: O crime resulta em lesão, prejuízo ou violação de direitos, sejam eles financeiros, de privacidade, honra ou outros.

4.3. Crimes virtuais Impróprios

Os crimes virtuais impróprios, por outro lado, são atividades ilegais que são cometidas utilizando a internet como meio, mas não são diretamente relacionadas ao ambiente digital. Eles envolvem o uso da internet para facilitar a prática de crimes tradicionais ou para ocultar a identidade dos criminosos.

Os crimes virtuais impróprios são aqueles que possuem elementos tanto online quanto offline. Eles se distinguem dos crimes virtuais próprios, que ocorrem exclusivamente no ambiente digital. Esta categoria de crimes engloba uma variedade de atividades ilegais, algumas são: Extorsão com Uso da Internet: Envolvendo ameaças ou chantagem online para obter vantagens financeiras ou outros benefícios. Tráfico de Drogas e Armas pela Internet: A compra, venda e

distribuição de substâncias ilícitas ou armas através da internet. Terrorismo Virtual: O uso da internet para planejar, promover ou executar atos terroristas. Exploração Sexual de Menores Online: Atividades relacionadas à pornografia infantil, tráfico de menores e abuso sexual de crianças na internet.

A categoria de delitos envolve atividades ilegais que ocorrem tanto no ambiente digital quanto no mundo físico. Estes crimes representam uma adversidade ao sistema jurídico, pois há dificuldades para identificar quem foi o sujeito que cometeu tais ilícitos.

Os delitos virtuais impróprios representam um desafio significativo para o sistema legal, exigindo a aplicação de leis tradicionais em conjunto com estratégias de combate aos cibercrimes. É crucial que as autoridades jurídicas estejam preparadas para lidar com esses crimes complexos, garantindo a segurança pública e a justiça na era digital.

4.4. Sujeito Ativo

Analisando alguns delitos ocorridos atualmente a idade dos sujeitos que cometem crimes são entre 17 à 30 anos de idade, tanto do gênero masculino quanto do gênero feminino, o acesso às informações e oportunidades de acesso à rede são fatores que influenciam na composição de tais sujeitos.

A imputação objetiva ao autor do crime e sua comprovação é extremamente difícil frente à ausência física do sujeito ativo. Ocorre que, frente à importância da identificação do autor do crime e a dificuldade desta identificação, surgiu a necessidade de se traçar um perfil denominado grupos que praticam determinados crimes virtuais.

Os hackers e os crackers geralmente são muito parecidos em relação ao vasto conhecimento aprofundado em informática, sendo que a principal distinção é a finalidade que suas práticas resultam, posto que os hackers realizam atividades positivas, não criminosas, enquanto a motivação dos crackers é criminosa em sua essência, agindo, normalmente e premeditadamente, com objetivo criminoso de obter vantagens ilícitas.

4.5. Hackers

Os Hackers são indivíduos que possuem um profundo conhecimento em informática e computação, e atuam na criação e alteração de software e hardware de computadores, não obrigatoriamente com a intenção de cometer atividades ilegais. Além disso, esses especialistas também contribuem para o desenvolvimento de novas funcionalidades e melhorias em sistemas de informática.

Principais atividades positivas de um hacker pode estar atrelada à criação de melhorias de segurança para o país, pois o mesmo é capaz de identificar fragilidades e vulnerabilidades em sistemas tecnológicos além de conscientizar a importância da segurança e privacidade digital. Já em relação a Inovação Tecnológica o mesmo pode atuar com ferramentas e software que podem beneficiar uma comunidade evitando assim danos como violação de privacidade e danos financeiros.

Em resumo, as atividades dos hackers podem ter uma ampla gama de resultados, desde benefícios legítimos, como aprimoramento da segurança cibernética, até consequências negativas, como transparência de privacidade e danos financeiros. A ética desempenha um papel fundamental na determinação desses resultados, e a distinção entre hackers éticos e maliciosos é crucial. É importante respeitar a legalidade e a ética ao lidar com atividades relacionadas à segurança cibernética e ao hacking.

4.6. Crackers

Os crackers podem ser caracterizados como indivíduos que, tendo conhecimento em informática, computação e outras tecnologias, empregam essas habilidades de forma ilícita para acessar sistemas, sites, servidores, bancos de dados e assim por diante. Em determinadas situações, a motivação é puramente avaliar a fragilidade dos serviços, enquanto em outras, busca-se obter vantagens financeiras ou benefícios pessoais.

Para maior conhecimento sobre as atividades de um “cracker” o mesmo pode ser atrelado às atividades como Invasões de Sistemas que certamente são

invadidas sem a concepção e consentimento do usuário, que pode tanto ser uma pessoa física ou jurídica, assim levando à apropriação de servidores, contas e redes pessoais e corporativas.

O roubo de dados também é uma das principais práticas de um cracker, que através de uma invasão de rede computacional poderá obter acesso às informações pessoais e sigilosas de grandes companhias, por exemplo. Informações estas como, nome completo, CPF, dados bancários e etc, com o intuito de obter vantagens pecuniárias, ou seja, a venda dessas informações para criminosos utilizam de “má índole” e assim se beneficiando sobre estes dados obtidos.

É importante ressaltar que as atividades dos crackers são ilegais e prejudiciais. Eles podem resultar em danos financeiros como citado, perda de privacidade, segurança gerando impactos negativos em organizações e indivíduos afetados. Além disso, os crackers estão sujeitos a processos legais e deliberações severas quando identificados e capturados.

Diante da categorização desses perfis de infratores, adquirimos uma compreensão geral de quem são, quais são seus objetivos e como geralmente operam. No entanto, a questão que se coloca é: como é possível identificá-los antes mesmo de cometerem atos ilegais que os identifiquem? Isso porque, quando nos referimos ao sujeito ativo, sabemos que os dados normalmente obtidos para sua identificação incluem o endereço da máquina que envia as informações, ou seja, o IP, juntamente com seu login e senha. Considerando a possibilidade de ocultação deliberada de informações e o uso de dados falsos, a identificação rápida do sujeito ativo na prática torna-se uma tarefa desafiadora.

O sujeito ativo que comete crime cibernético no Brasil é uma figura complexa, muitas vezes caracterizada por um conjunto diversificado de características e motivações. Em geral, podemos identificar os seguintes aspectos relacionados ao sujeito ativo dos crimes cibernéticos no país são eles: Perfil Diversificado, o sujeito ativo dos crimes cibernéticos no Brasil não possui um perfil único. Ele pode ser jovem ou mais velho, com diferentes níveis de habilidades técnicas. O cibercriminoso pode ser um hacker experiente, um membro de uma organização criminosa, um funcionário desonesto ou até mesmo um adolescente curioso,

As motivações para a prática de crimes cibernéticos no Brasil também são diversas. Algumas pessoas podem buscar lucro financeiro por meio de fraudes online, enquanto outras podem agir por razões ideológicas, como ativismo cibernético. Há ainda aqueles que cometem esses delitos por diversão ou para testar suas habilidades.

Ferramentas e técnicas avançadas, como malware, engenharia social, phishing e outras estratégias para alcançar seus objetivos. A capacidade de explorar vulnerabilidades em sistemas e redes é uma característica comum desse perfil, pois existem diferentes sistemas de softwares para utilização no mundo digital.

O cibercriminoso busca ocultar sua identidade real por trás de proxies, VPNs ou outros métodos de anonimato online. Isso torna a identificação do sujeito ativo um desafio significativo para as autoridades, uma das alternativas para investigação é rastrear através do endereço IP (é um endereço exclusivo que identifica um dispositivo na Internet ou em uma rede local.) da máquina, alcançando assim o infrator.

Os crimes cibernéticos têm um impacto significativo na sociedade brasileira, afetando a segurança digital, a privacidade dos cidadãos e a economia. O sujeito ativo, ao realizar esses atos ilegais, contribui para a disseminação de ameaças digitais que podem prejudicar empresas, instituições governamentais e cidadãos comuns.

Por fim, o sujeito ativo que comete crimes cibernéticos no Brasil é uma figura multifacetada, com motivações e características diversas. Compreender esse perfil é fundamental para desenvolver estratégias eficazes de prevenção e combate aos crimes cibernéticos, bem como para promover a segurança digital no país.

4.7. Sujeito Passivo

Quando nos referimos a um crime específico, é comum identificar claramente quem está realizando a ação criminosa (o sujeito ativo) e quem está sofrendo as consequências dessa ação (o sujeito passivo). No entanto, nos casos de crimes virtuais, essa identificação não é tão direta. Em termos gerais,

podemos afirmar que o sujeito ativo sempre será uma pessoa física ou jurídica, pública ou privada, que detém o controle sobre o bem jurídico em questão. Por outro lado, o sujeito passivo da infração penal pode ser qualquer pessoa, seja ela física ou jurídica, que esteja sofrendo as consequências do ato criminoso.

Portanto, o sujeito passivo de um crime cibernético pode ser um indivíduo comum, uma pessoa física, ou até mesmo uma entidade jurídica. Isso ocorre porque os crimes virtuais podem resultar em danos diversos, como desvio de patrimônio, deterioração do patrimônio, ou violação de informações. Ambos, indivíduos e entidades, estão sujeitos às ações dos criminosos.

No entanto, é importante destacar que muitos dos crimes cibernéticos praticados atualmente não são divulgados ou reportados. Isso acontece, em parte, devido à falta de divulgação de informações sobre esses crimes e à falta de denúncias por parte das vítimas. Por exemplo, muitas grandes empresas evitam divulgar possíveis ataques cibernéticos ou invasões para não demonstrar fraquezas em suas medidas de segurança. Da mesma forma, muitas pessoas físicas não denunciam esses crimes devido à falta de punição adequada aos infratores e à falta de mecanismos de denúncia acessíveis, apesar de já existirem tais recursos disponíveis. Esse cenário contribui para a proliferação desses crimes cibernéticos sem que sejam devidamente combatidos.

Essa figura representa aqueles que, de alguma forma, são afetados pelas ações ilegais no ambiente virtual, seja por meio de ligações, mensagens, e- mails ou aplicativos, a conscientização sobre o tema é relevante pois o número de pessoas que caem em fraudes “golpes” tem aumentado a cada dia.

Mirabete (2008, p. 114) ressalta que o sujeito passivo podem ser duas ou mais vítimas, como estabelecido no artigo 147 do Código Penal: “ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave”, esse crime é comum nas redes virtuais, podendo ter ao mesmo tempo duas ou mais vítimas.

O sujeito passivo nos crimes cibernéticos pode ser extremamente diversificado. Pode ser uma pessoa física, uma pessoa jurídica, uma instituição pública ou privada, ou até mesmo uma entidade titular de um bem jurídico protegido. Isso significa que qualquer indivíduo, organização ou entidade que utilize a tecnologia e a internet pode potencialmente se tornar um sujeito passivo.

No contexto empresarial, as organizações são frequentemente alvo de ataques cibernéticos, visando o desvio de informações sensíveis, propriedade intelectual, interrupção de operações comerciais e extorsão por meio de ransomware. Empresas podem sofrer sérias consequências financeiras e de reputação como resultado desses ataques.

As pessoas Físicas, também podem ser vítimas de crimes cibernéticos. Isso inclui roubo de identidade, invasão de contas online, assédio cibernético (cyberbullying), fraudes financeiras, entre outros. As vítimas podem experimentar traumas psicológicos e prejuízos financeiros consideráveis.

A denúncia é uma das alternativas para identificar o infrator, porém apesar da crescente incidência de crimes cibernéticos muitos casos não são denunciados. Isso pode ocorrer devido à falta de conscientização sobre os mecanismos de denúncia, à preocupação com a exposição pública ou à descrença nas chances de identificar e punir os criminosos.

Portanto , o sujeito passivo dos crimes cibernéticos no Brasil representa uma ampla gama de atores, incluindo indivíduos e organizações, que enfrentam diversas formas de dano devido a atividades ilegais na internet. O entendimento de suas preocupações e necessidades é fundamental para o desenvolvimento de estratégias de prevenção e combate aos crimes cibernéticos e para garantir a segurança digital e a justiça no país.

5. Capítulo V

5.1. Convenção de Budapeste

A Convenção de Budapeste, estabelecida em novembro de 2001, é um acordo internacional que reúne países Europeus para o compartilhamento colaborativo de informações de rede, visando a prevenção e combate aos crimes cibernéticos.

Essa referida convenção consiste em um ordenamento desenvolvido pelo Conselho da Europa em 2002, em que seu objetivo girava em torno da proteção da sociedade contra a criminalidade no ciberespaço. A princípio, a Convenção de Budapeste promovia a escolha de uma legislação comum que objetivam uma

maior cooperação entre os Estados da União Europeia, mas atualmente encontra-se aberta à assinatura por todos os países que a desejarem, tendo em vista que os crimes cibernéticos atingem todos os territórios do mundo (FERNANDES, 2013)16 .

O propósito é simplificar a colaboração global no combate ao crime cibernético. Este tratado foi elaborado sob a supervisão do Comitê Europeu para os Problemas Criminais, com o auxílio de uma comissão de especialistas, e visa identificar e definir os principais detalhes dos problemas através da internet. Notavelmente, este tratado representa o pioneirismo no contexto internacional. A Convenção tem, até o momento, recebido a assinatura de 66 países que adotaram o tratado, enquanto aproximadamente 160 países utilizam como referência para a formulação de suas leis locais.

O exemplo de aplicabilidade em caso concreto de tal Convenção recentemente, conforme jurisprudência e decisão do Superior Tribunal de Justiça do Estado de São Paulo:

> **Decisão:** O Tribunal, por maioria, conheceu da ação declaratória de constitucionalidade, vencida pelos Ministros André Mendonça e Nunes Marques. No mérito, por unanimidade, julgou parcialmente procedente o pedido formulado na inicial para declarar a constitucionalidade dos dispositivos indicados e da possibilidade de solicitação direta de dados e comunicações eletrônicas das autoridades nacionais a empresas de tecnologia, nas específicas hipóteses do art. 11 do Marco Civil da Internet e do **art. 18 da Convenção de Budapeste**, ou seja, nos casos de atividades de coleta e tratamento de dados no país, de posse ou controle dos dados por empresa com representação no Brasil e de crimes cometidos por indivíduos localizados em território nacional, com comunicação desta decisão ao Poder Legislativo e ao Poder Executivo, para que adotem as providências necessárias ao aperfeiçoamento do quadro legislativo, com a discussão e a aprovação do projeto da Lei Geral de Proteção de Dados para Fins Penais (LGPD Penal) e de novos acordos bilaterais ou multilaterais para a obtenção de dados e comunicações eletrônicas, como, por exemplo, a celebração do Acordo Executivo definido a partir do Cloud Act, tudo nos termos do voto do Relator. Ausentes, justificadamente, o Ministro Nunes Marques e o Ministro Roberto Barroso, que afirmou suspeição neste julgamento. Presidência da Ministra Rosa Weber. Plenário, 23.2.2023”

Conforme descrito pelo ministério público federal em 23 de Dezembro de 2021 “As questões tratadas na Convenção de Budapeste estão a criminalização de condutas, normas para investigação e produção de provas eletrônicas e meios de cooperação internacional”. Já no Brasil a implementação do decreto foi aderida em 12 de abril de 2023, conforme decreto DECRETO Nº 11.491, DE 12 DE ABRIL DE 2023.

Além da velocidade na troca de informações, a convenção de Budapeste é de extrema importância para o Brasil, pois oferece uma estrutura essencial para a cooperação internacional no combate ao crime cibernético. O Brasil, como uma nação que enfrenta desafios crescentes em termos de segurança cibernética, colhe diversos benefícios ao aderir a esse tratado internacional.

Em primeiro lugar, a Convenção estabelece uma base sólida para o combate ao crime em escala global. A natureza transnacional de muitos crimes cibernéticos exige cooperação entre países, e a adesão à Convenção permite ao Brasil colaborar de maneira mais eficaz com outras nações na identificação, investigação e responsabilização de delitos cibernéticos.

Além disso, o acordo fornece um conjunto de diretrizes e práticas recomendadas para a orientação. Isso é particularmente importante para o Brasil, uma vez que ajuda na padronização das leis e regulamentos relacionados à segurança cibernética brasileira. Essa padronização é fundamental, pois facilita a abordagem de questões legais de maneira mais eficaz e coesa.

A adesão também promove a melhoria das práticas de segurança em nível nacional. O Brasil pode aproveitar as diretrizes da Convenção para fortalecer suas defesas cibernéticas, protegendo melhor suas redes e sistemas de informações críticas contra ameaças. A proteção dos cidadãos e das empresas brasileiras contra crimes cibernéticos é outra conquista importante da adesão à Convenção. Isso inclui defesa contra fraudes online, roubo de dados, extorsão por meio de ransomware e outros tipos de ataques. A participação na Convenção ajuda a criar um ambiente de negócios mais seguro e a garantir a privacidade das pessoas.

Já a luta contra o cibercrime organizado, que muitas vezes opera em escala internacional, é uma das prioridades da Convenção. Além disso, a adesão reforça a imagem do Brasil no cenário internacional como um ator comprometido com a segurança cibernética e o combate ao crime. Isso demonstra o compromisso do país em enfrentar os desafios crescentes da cibersegurança e contribuir para um ambiente global mais seguro.

6. Considerações Finais

A tipicidade dos crimes cibernéticos no Brasil é um assunto de extrema importância nos dias atuais, uma vez que a evolução tecnológica trouxe consigo novas formas de cometimento de delitos. Nesse contexto, o objetivo deste trabalho foi analisar a tipicidade dos crimes cibernéticos no ordenamento jurídico brasileiro, considerando a legislação atual e sua aplicação pelos tribunais.

Para tanto, foi realizada uma revisão da metodologia bibliográfica, descritiva e doutrinária, com os principais conceitos relacionados aos crimes cibernéticos e sua tipificação no Brasil, bem como uma análise dos casos julgados pelos tribunais brasileiros, jurisprudências e a legislação vigente.

A tipificação adequada para os ilícitos penais virtuais no Brasil é imposto na Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que é a principal norma que trata dos crimes cibernéticos. Ela prevê, por exemplo, os crimes de invasão de dispositivo informático, interceptação de comunicações eletrônicas e obtenção, transferência ou divulgação não autorizada de dados pessoais.

Diante da ampla acessibilidade da internet para a transmissão de informações, ela proporcionou aos infratores que fazem uso da rede a facilidade de permanecerem, em sua maioria, protegidos pelo anonimato. Isso torna consideravelmente desafiadora a tarefa de identificá-los pessoalmente e, por conseguinte, localizar o seu endereço.

Devido ao avanço digital tecnológico, o ordenamentos Brasileiro elaborou e promulgou leis que ordena os crimes virtuais, uma delas foi a citada anteriormente a Lei lei 12.737/2012, que ficou conhecida nacionalmente como “Lei Carolina Dieckmann”, criada após o vazamento de fotos íntimas da atriz do seu computador pessoal, embora ainda não seja suficiente para punir os infratores.

Portanto, concluo que, algumas condutas ainda não estão previstas de forma adequada na legislação brasileira, o que dificulta a punição de certos tipos de crimes cibernéticos. Por isso, é importante que o Poder Legislativo revise e atualize constantemente a legislação em relação aos crimes cibernéticos, de forma a acompanhar as evoluções tecnológicas e garantir a proteção dos direitos

fundamentais das pessoas, a adaptação contínua das leis é crucial para manter o país à frente dos desafios em constante evolução da cibersegurança.

REFERÊNCIAS

JESUS, D. de; MILAGRE, J. A. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016

AZEVEDO; J. S. de.; CARDOSO, T. M. **Crimes cibernéticos: evolução e dificuldades na colheita de elementos de autoria delitiva**. 2021. 25 f. Trabalho de Conclusão de Curso (Bacharel em Direito) – Una Bom Despacho, Bom Despacho. 2021.

O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – **Código Penal, passa a vigorar com as seguintes alterações**. Fonte: Agência Senado.

PINHEIRO, Emeline Piva. **Crimes virtuais: uma análise da criminalidade informática e da resposta estatal**. Santa Catarina: UFSC, 2006. Disponível em: . Acesso em: 02 OUT. 2019.

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

LOPES, Alan Moreira. **Crimes praticados por meio eletrônico**. 1ª Ed. Curitiba: Ag Book, 2012.

CRUZ, D.; RODRIGUES, J. **Crimes cibernéticos e a falsa sensação de impunidade**. Revista Científica Eletrônica Do Curso De Direito, ed. 13, jan. 2018 (CRUZ; RODRIGUES, 2018).

BRASIL. Lei nº 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**. Diário Oficial da União, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 02/03/2023.

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**. Diário Oficial da União, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 15/02/2023.

Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Diário Oficial da União, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16/03/2023.

NASCIMENTO, S. de P. **Cibercrime: conceitos, modalidades e aspectos jurídicos penais**. Âmbito Jurídico, 3 set. 2019. Disponível em: https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitosmodalidades-e-aspectos-juridicos-penais. Acesso em: 14/03/2023.

GONÇALVES, J. R.; OLIVEIRA, L. R. G. **A ineficácia da punibilidade do cyberbullying no Brasil**. Revista Educar Mais, v. 4, n. 2, 2020.

D'URSO, Luiz Augusto. **Lei que torna crimes cometidos pela internet mais graves é sancionada**. Migalhas, 2021. Disponível em: https://www.migalhas.com.br/quentes/346274/lei-que-torna-crimes-cometidos-pelainternet-mais-graves-e-sancionada. Acesso em: 04/02/2023

ALMEIDA, N. G. N. DE. **A importância da metodologia científica através do projeto de pesquisa para a construção da monografia**. Folha de Rosto, v. 2, n. 1, p. 57-66, 30 jun. 2016. (metodologia)

FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. REVISTA DA FACULDADE DE DIREITO DA UFMG, 2013, 2013.62: 139-178.

MIRABETE, Julio Fabbrini. Manual do Direito Penal: parte geral. 24 ed. São Paulo: Atlas, 2008.

JESUS, D. E. Direito Penal – **1° vol. – Parte Gera**l. São Paulo: Saraiva, 2011.

CAPEZ, F. **Curso de Direito Penal**. São Paulo: Saraiva, 2011.

Ciências Humanas e Sociais Unit Aracaju v. 2 n.3 p. 215-236 Março 2015 | periodicos.set.edu.br

Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm>. Acesso em: 10 de Outubro de 2023.

NORONHA apud CAPEZ, Fernando. **Curso de direito penal: parte especial. 7**. ed. São Paulo: Saraiva, 2007. v. 2, p. 236. 2 NUCCI, Guilherme de Souza. Código penal comentado. 6. ed. São Paulo: Revista dos Tribunais, 2006, p. 595. 3 HUNGRIA, Nélson; FRAGOSO, Heleno Cláudio. Comentários ao código penal. 5. ed. Rio de Janeiro, Forense, 1982. v. 6, p. 38-39

OLIVEIRA, Julio Cesar Vieira de. Crime de Estupro e as alterações da Lei nº. 12.015/09. **Monografia apresentada à Universidade Vale do Itajaí** – UNIVALI, como requisito parcial à obtenção do grau em Bacharel em Direito. São José, 2010.

Migalhas.com. **Estelionato praticado por meio da internet: Uma visão acerca dos crimes digitais. Disponível em: <**https://www.migalhas.com.br/depeso/359821/estelionato-praticado-por-meio-da-internethttps://www.migalhas.com.br/depeso/359821/estelionato-praticado-por-meio-da-internet>. Acesso em 20 de Setembro de 2023.

Brasil escola. **Cyberbullying**. Disponível em: https://brasilescola.uol.com.br/sociologia/cyberbullying.htm>. Acesso em: 12 de Setembro de 2023.

Agravo de Instrumento **nº 2136050-33.2022.8.26.0000**, da Comarca de Hortolândia, em que é agravante MABE MERCOSUR PARTICIPAÇÕES LTDA.

Correio do Estado. **Estelionato é o crime virtual mais recorrente do Estado em 2023**. Disponível em: <https://correiodoestado.com.br/cidades/estelionato-e-o-crime-virtual-mais-recorrente-do-estado-em-2023/417824/>. Acesso em 07 de Novembro de 2023.