PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO I

CRIMES VIRTUAIS E A ADEQUAÇÃO DA LEGISLAÇÃO PENAL BRASILEIRA

ORIENTANDA: KAMILA MARTINS POMPILIO
ORIENTADORA: PROFª MS. ELIANE RODRIGUES NUNES

GOIÂNIA
2023

KAMILA MARTINS POMPILIO

CRIMES VIRTUAIS E A ADEQUAÇÃO DA LEGISLAÇÃO PENAL BRASILEIRA

Artigo Científico apresentado à disciplina de Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUC GOIÀS). Orientadora: Profa. Ms. Eliane Rodrigues Nunes

GOIÂNIA

2023

KAMILA MARTINS POMPILIO

CRIMES VIRTUAIS E A ADEQUAÇÃO DA LEGISLAÇÃO PENAL BRASILEIRA

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

Orientadora: Prof. Ms. Eliane Rodrigues Nunes Nota

Examinadora Convidada: Prof.: Marina Rúbia M. Lôbo de Carvalho Nota

RESUMO

O presente trabalho visa explorar a questão dos crimes virtuais e a adequação da legislação penal brasileira para lidar com essa modalidade de crime. Para sua elaboração, foram feitas consultas em diversas fontes tais como bibliografias, artigos, legislação, jurisprudência, sites e reportagens. Acerca dos crimes virtuais no Brasil, utiliza-se como base para a punição desses crimes o Código Penal, entretanto, constata-se que o ordenamento jurídico carece de legislação específica para tais delitos, tendo em vista o crescente número de infrações cometidas no meio virtual.

Palavras-chaves: Crimes virtuais. Crimes Cibernéticos. Legislação. Internet.

Abstract

The presente work aims to explore the issuo of virtual crimes and the adequacy of Brazilian criminal legislation to deal with this type of crime. For its elaboration, consultations were made in several sources such as bibliographias, articles, legislation, jurisprudence, websites and reports. Regarding virtual crimes in Brazil, the Penal Code is used as a basis for the punishment of these crimes, however, it appears that the legal system lacks specific legislation for such crimes, in view of the growing number of infractions committed in the environment.

Keywords: Cybercrimes. Cyber Crimes. Legislation. Internet.

SUMÁRIO

Introdução

É evidente que a sociedade está em constante evolução e, como resultado, o Direito também evolui. No âmbito penal, desde os primórdios da civilização, a punição tem sido buscada para aqueles que violam as regras que governam a sociedade. Com a velocidade em que a tecnologia se desenvolve atualmente, surge continuamente novas formas de crimes.

Embora a tecnologia avance rapidamente, o Direito deve se adaptar a ela. O ambiente virtual tem se tornado um meio para a prática de crimes, pois muitos acreditam que é difícil identificar os autores de atos ilícitos na *internet*. No entanto, essa não é sempre a realidade.

Observa-se, portanto, que há uma grande complexidade para o ordenamento jurídico solucionar os conflitos oriundos da ampla presença da internet no mundo, o que gerou muitas transformações não devidamente acompanhadas pela legislação brasileira. Isso faz com que, na medida do possível, os juristas enquadrem as novas condutas lesivas nos tipos penais já existentes, já que as legislações e o controle das autoridades não são eficientes quanto aparentam ser.

O propósito deste trabalho consiste em expor sobre os crimes virtuais, estabelecendo uma conexão com a legislação brasileira e delineando tanto as evidências concretas quanto os aspectos positivos e negativos, como por exemplo, a carência de legislação específica para tais crimes no país.

Importante destacar que há diversas nomenclaturas em relação aos crimes virtuais (como, por exemplo, crimes cibernéticos, cibercrimes, crimes informáticos), a qual não se tem um consenso por parte dos doutrinadores, sendo assim, consideraremos como crimes virtuais aqueles já tipificados no código penal, que são práticos em ambientes virtuais, bem como condutas especificas que somente podem ser cometidas nesses ambientes.

Em suma, almeja-se que este trabalho contribua para a área do Direito Penal, promovendo o enriquecimento e o esclarecimento acadêmico e científico acerca dos crimes virtuais, tema ainda desafiador para muitas pessoas, incluindo aquelas que atuam na área jurídica.

1. O SURGIMENTO DO CRIME VIRTUAL

1.1. HISTÓRICO

Com intuito de facilitar o cotidiano, assim surgem os computadores e demais redes de comunicação. Aquilo que antes era realizado com longa duração, passou a ser executado com mais rapidez.

O ser humano desde a antiguidade vem em busca do seu desenvolvimento, com novos projetos e ferramentas que torne o dia a dia mais fáceis, tornando suas atividades de certa forma mais prazerosa.

Com isso, o mundo passou por diversas transformações, podendo assim ser citada uma das mais importantes que foi a Revolução Industrial, a qual alterou o estilo de vida da população no geral, trazendo um avanço significativo na mudança do homem no campo, para as cidades, forçando um rápido crescimento populacional no meio urbano. Teve início na Inglaterra a partir da segunda metade do século XVIII, e foi marcada pelo grande desenvolvimento tecnológico, que garantiu o surgimento da indústria e consolidou o processo de formação do capitalismo.

A partir do avanço da tecnologia na Revolução Industrial, que fez com que a matéria-prima chegasse com mais rapidez as pessoas, através do controle dos trabalhadores a máquinas de vapor, a qual permitia com que as fabricas produzissem mais, e as novas invenções como os navios e locomotivas. Diante disso, surgiram diversas invenções, como por exemplo, a Fotografia (1839), Telefone (1876), Luz Elétrica (1879), Televisão (1924), dentre outros, no qual modificaram a forma que as pessoas viveram naquela época e que vivem atualmente.

Em meados do século XX, houve um marco no desenvolvimento e surgimento de novas tecnologias, que pode ser chamada de Era da Informação ou Era Digital, também conhecida como a Terceira Revolução Industrial. A informática passou então a fazer parte da vida diária das pessoas, como afirma Medeiros (2010, p. 2):

> Os modernos sistemas computacionais e o aprimoramento das aplicações tecnológicas em vigor vão sendo lançados no mercado

> sempre na ânsia de melhorar e facilitar a forma de nos comunicarmos, permitindo, inclusive, que diversos países, como é o caso do Brasil, pudessem ser integrados ao mundo globalizado sob diversos aspectos.

Com advento da informática, na década de 1960 surge a *internet***,** que consiste em um complexo de máquinas que operam de forma integrada, interligando todo o mundo e permitindo que se acessem informações de todo tipo de forma remota. O ambiente virtual é conhecido como *cyberespaço*, inicialmente definido como o "lugar" virtual no qual a conversação ocorre (CARVALHO, 2014).

Notavelmente, inúmeras vantagens e benefícios a *internet* proporcionou, fazendo com que as relações sociais e comerciais entre pessoas e nações estivessem conectadas em uma só rede, possibilitando até mesmo um crescimento exponencial econômico entre países. A utilização desse espaço virtual trouxe modificação no cotidiano das pessoas, tendo em vista que ela está presente em diversas atividades do dia a dia, tal como as relações profissionais, financeiras e pessoais.

Contudo, de igual forma, condutas danosas foram criadas, diante da evolução tecnológica no mundo virtual, que fez com se tornasse impossível atualmente pensar em um mundo sem *internet*.

Despertou-se então em muitos criminosos, a possibilidade de tornar desse espaço virtual um meio para a prática do crime. Houve assim, uma grande migração de bandidos para esse meio, a qual se iniciou uma nova categoria de crimes: os crimes *cibernéticos* ou crimes virtuais.

Nesse sentido Correa Segundo (2016, pg. 19) afirma:

> Não existe um consenso na literatura acerca do surgimento desses crimes. Entretanto existem muitos fatos datados a partir do século XX, nos anos 60. Casos de espionagem eletrônica em sistemas informáticos assim como de sabotagem destes sistemas foram levantados nesse período. Foi desenvolvido por programadores, ainda nessa década, um jogo chamado Core Wars que se reproduzia todas as vezes que era ativado causando uma grande sobrecarga na memória do computador do outro jogador. Em contrapartida os mesmos mentores desse jogo criaram um dispositivo que era capaz de destruir essas cópias de reprodução originadas do mesmo jogo o que consideraríamos nos dias de hoje como um antivírus.

Na década de 70, pode-se destacar o surgimento da figura do *hacker*, que começam a ser citados e relacionados aos crimes virtuais por invasão feita em sistemas e furtos de *software* em computadores conectados à rede.

Os crimes virtuais se alastraram ainda mais na década de 80. Houve uma preocupação com a fragilidade que apareceu no sistema, pois propagou-se diferentes tipos de crimes, como invasão de sistemas, pedofilias, pirataria, tendo então a necessidade de maior segurança virtual, para a identificação e punição dos responsáveis por tais delitos, que poderiam estar espalhados em diversas partes do mundo, fazendo com que houvesse certa dificuldade em realizar a captura desses criminosos. Carneiro (2012).

Há de salientar como foi no caso do *hacker* Kevin Mitnick, conhecido por ser um dos mais famosos hackers dos Estados Unidos, se não o mais famoso do mundo, a qual o governo norte americano em uma caça desesperadora, só conseguiu encontrar e puni-lo depois de muitos anos, pelos crimes que havia cometido, atualmente Kevin trabalha para o governo americano na área de segurança de informação.

No Brasil, a preocupação com o assunto só começou nas últimas décadas, tendo em vista, o grande aumento populacional que aderiu a inovação tecnológica.

> “O Brasil começou a se preocupar com esse assunto especialmente a partir das últimas décadas, com o aumento da popularização dessa inovação tecnológica, promulgando, na Constituição Federal de 1988, leis relativas à competência do Estado sobre questões de informática”. (CARNEIRO, 2012)

1.2. CONCEITO

Com advento da *internet* a tecnologia sofreu grande avanço. São inúmeras as vantagens proporcionadas por seu uso, dentre as quais se destacam: a comunicação, a informação, o entretenimento, a prestação de serviços como transferência bancária on-line, o pagamento de contas, a procura de um emprego, assistir a filmes, documentários, ouvir músicas, realizar reservas em hotéis, comprar e vender produtos e mercadorias, dentre outros. Diante da

diversidade tecnológica, pode-se dizer que é impossível um retrocesso à sociedade totalmente desvinculada de tais meios.

No entanto, esse mesmo canal que é utilizado para tais finalidades, infelizmente também é utilizado para prática de delitos, denominados crimes virtuais.

Alguns doutrinadores buscam o conceito dos crimes virtuais, como Pinheiro, Manuel Lopes Rocha (2000, p. 318) e Ivette Senise Ferreira (2005, p. 261) que diz que:

> Crimes virtuais são aqueles que têm por instrumento ou por objeto de processamento eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos.
> 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.

Para Carneiro (2012 apud PINHEIRO, 2006), “O crime é, em princípio, um crime de meio, ou seja, utiliza-se de um meio virtual”.

A definição a respeito da criminalidade informática e sua nomenclatura é ampla, não existindo um consenso comum para tais delitos, tendo em vista a gama de ilícitos possíveis de serem cometidos na *internet* ou por meio dela. Como afirma CRESPO:

> As denominações quanto aos crimes praticados em ambiente virtual são diversas, não há um consenso sobre a melhor denominação para os delitos que se relacionam com a tecnologia, crimes de computação, delitos de informática, abuso de computador, fraude informática, enfim, os conceitos ainda não abarcam todos os crimes ligados à tecnologia, e, portanto, deve se ficar atento quando se conceitua determinado crime, tendo em vista que existem muitas situações complexas no ambiente virtual. (CRESPO, (2011, p.48)

Diante disso, através de um conceito analítico finalista do crime, chega-se à conclusão de que o crime virtual é as todas as condutas típicas, antijurídicas e culpáveis contra a utilização dos sistemas de informática de uma pessoa física ou jurídica, como afirma Bramilla (2015).

1.3. CLASSIFICAÇÃO

No que tange a classificação dos crimes virtuais a doutrina assim como na conceituação não entra em um consenso, entretanto a classificação mais aceita pela doutrina é a divisão entre os crimes puros, impuros e mistos.

1.3.1. Crimes Virtuais Puros

Os crimes virtuais puros ou próprios são aqueles em que o agente ataca o sistema de informática, sendo o computador o sistema tecnológico usado como objeto para a execução do crime.

Para Damásio de Jesus:

> Crimes informáticos próprios: em que o bem jurídico ofendido é a tecnologia da informação em si. Para estes delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva penal, muitas práticas não poderiam ser enquadradas criminalmente.

Corroborando com esse conceito Marco Túlio Viana, afirma que os 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).

1.3.2. Crimes Virtuais Impuros

Os crimes impuros ou impróprios são aqueles em que o agente se utiliza do computador como meio executório para prática de um crime tipificado na legislação penal.

Segundo Damásio de Jesus:

> Crimes informáticos impróprios: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais.

Portanto o computador não é o fator primordial desse crime, e sim uma das diversas formas de materializar uma conduta delituosa.

1.3.3. Crimes virtuais mistos

Os crimes virtuais misto se consubstancia nas ações em que o agente visa o bem juridicamente protegido, a *internet* é utilizada como meio para realizar o crime. Para melhor elucidação, as palavras de Damásio de Jesus e José Antônio Milagre (2016, p. 54):

> Crimes informáticos mistos: são crimes complexos em que, além da proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro bem jurídico. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico.

Sendo assim, observa-se de acordo com a classificação que os crimes virtuais com emprego da *internet* ou computador, tem por objetivo obter vantagens sob outrem, por meio de comunicação relacionada à *internet* ou invasão de *software*.

2. TIPOS PENAIS NO MEIO VIRTUAL

Os crimes virtuais em sua grande parte são crimes já existentes no mundo real, sendo assim, fatos típicos e antijurídicos como já mencionado anteriormente, que segundo Damásio de Jesus e José Antônio Milagre (2016, p. 49) conceituam como:

> Fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito Informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal.

Diante disso, na pluralidade dos crimes cometidos na esfera virtual, será abordado alguns dos crimes mais comuns nesse meio.

2.1. FRAUDE E ESTELIONATO

Atualmente são compartilhados por todo tipo de pessoas no mundo momentos de laser diversão em tempo real, utilizando a *internet* em seus diversos canais.

Da mesma forma, é feita aquisição de produtos através de lojas virtuais, mais conhecido por *E-commerce*, que traz a facilidade na compra de um determinado produto em apenas alguns cliques, sendo nesse meio realizado transações bancárias pela *internet banking*.

Com advento das relações comerciais pela *internet*, os criminosos e organizações criminosas passaram a utilizar *softwares* sofisticados, a fim de forjar *URLS* e promover *links* falsos, sendo esse tipo de conduta popularmente conhecida como golpe, modalidade também chamada de *phishing* (TONI, FREDERICO, 2020)

Segundo Cassanti (2014, p. 39):

> *Phishing* é um exemplo bastante simples e muito utilizado na engenharia social e que consiste, na maioria dos casos, no envio de e-mails não solicitados para a vítima, estimulando-a a acessar páginas (*sites*) fraudulentas, preencher formulários com seus dados privados ou despertar curiosidade fazendo com que clique em um *link* para fazer

> *download* de um arquivo malicioso (*malware*) capaz de transmitir para o atacante as informações que lhe interessam.

Um exemplo de golpe são os sites falsos que através de determinado conteúdo ou até mesmo uma mensagem de texto ou *e-mail*, geralmente disfarçados, como se tivessem sido enviados pela própria agência bancária alertando sobre compras indevidas ou atualização de dados cadastrais, induzem as vítimas a indicar dados pessoais ou até bancários, tendo o agente criminoso a apropriação desses dados e posteriormente a transferência de valores e até mesmo a realização de compras em nome da vítima.

Tanto a fraude, quanto o estelionato estão tipificados no artigo 171, do Código Penal, in verbis:

> Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.
> Fraude eletrônica
> § 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. (BRASIL, 2021)

No ambiente virtual o objetivo do agente é induzir a pessoa ao erro, para que de forma voluntaria ela entregue o bem ou informe dados pessoais, que possibilite que o agente tenha vantagem diante dessas informações adquiridas.

2.2. CRIMES CONTRA HONRA

Tem se tornado cada vez maior a exposição da imagem e privacidade do indivíduo na esfera virtual, sendo sua honra atingida, tendo em vista a expansão das redes sociais e dos sites.

A honra é as características, particularidades, morais, físicas e intelectuais de um indivíduo, fazendo desse modo com que ele seja respeitado

diante da sociedade a qual faça parte, definindo assim a sua aceitação em determinado grupo social (CRESPO, 2011).

A Constituição Federal prevê sem seu artigo 5º, inciso X, a inviolabilidade da honra, sendo direito fundamental protegido constitucionalmente.

Salienta-se que a honra abrange os aspectos objetivos e subjetivos de acordo com a doutrina brasileira. A honra objetiva relaciona-se com a reputação ou a imagem que a pessoa tem perante terceiros. Já a honra subjetiva está relacionada a dignidade e o decoro da pessoa, o juízo que cada pessoa tem de si mesmo (CUNHA, 2014).

O Código Penal em seu capítulo V, estabelece três tipos de crime contra a honra, sendo estes a Calúnia, Difamação e Injúria, previstos nos artigos 138, 139 e 140. A legislação distingue o tipo penal e a pena, conforme observa-se:

> **Calúnia**
> Art. 138 Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> **Difamação**
> Art. 139 Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
> **Injúria**
> Art. 140 Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.

O crime de calúnia é comentado por Júlio Fabbrini Mirabete dizendo:

> Pratica o crime quem imputa, atribui a alguém, a prática de crime, ou seja, é afirmar, falsamente, que o sujeito passivo praticou determinado delito. É necessário, portanto, que a imputação verse sobre fato determinado, concreto, específico, embora não se exija que o sujeito ativo descreva suas circunstâncias, suas minúcias, seus pormenores. Trata-se de crime de ação livre que pode ser cometido por meio da palavra escrita ou oral, por gestos e até meios simbólicos. Pode ela ser explícita (inequívoca) ou implícita (equívoca) ou reflexa (atingindo também terceiro). A imputação da prática de uma contravenção não constitui calúnia, mas pode caracterizar o delito da difamação. Como a honra, objetiva e subjetiva, é um bem jurídico disponível, o consentimento anterior ou concomitante com o fato exclui o crime.

Já o crime de difamação consiste em atribuir a alguém, fato ofensivo a sua reputação, sendo esse fato verdadeiro ou falso. Este crime atinge a honra objetiva tendo em vista que ofende a reputação do indivíduo.

Na injúria o delito tutelado é a honra subjetiva do ofendido, que Júlio Fabbrini Mirabete considera que:

> A conduta típica é ofender a honra subjetiva do sujeito passivo, atingindo seus atributos morais (dignidade) ou físicos, intelectuais, sociais (decoro). Não há na injúria imputação de fatos preciosos e determinados, como na calúnia ou difamação, mas apenas de fatos genéricos desonrosos ou de qualidades negativas da vítima, como menosprezo, depreciação etc.

Nesses crimes, os meios virtuais são muito utilizados por agentes praticantes destes delitos, se tornando até mesmo comuns, diante do anonimato dos que o praticam, tendo em vista que tem se tornado cada vez mais difícil a identificação do criminoso e a retirada do conteúdo ofensivo.

2.3. PORNOGRAFIA INFANTIL

A pornografia infantil tem sido um dos crimes que mais causa repudio, não havendo qualquer forma de ser aceita pela sociedade, tendo em vista, a situação tão constrangedora a qual crianças e adolescentes são submetidos. Tendo em vista que se trata de um tipo de violência sexual. A circulação da pornografia infantil tem sido hoje uma verdadeira indústria altamente lucrativa pelos malfeitores, configurando violação aos direitos fundamentais das crianças e adolescentes. (TONI, FREDERICO, 2020).

O Estatuto da Criança e do Adolescente trata dos delitos relacionados com a pornografia infantil nos artigos 240 a 241-E, visando criminalizar a conduta de publicar ou divulgar foto ou vídeo de crianças e adolescentes, bem como combater à produção, venda e a distribuição da pornografia infantil, inclusive por meios de comunicação, como a *internet*.

Um dos meios de se obter materiais de pornografia infantil é através de sites “invisíveis” como é a *deep web*, que não será amplamente abordada nesse trabalho, mas que se trata de uma plataforma pouco conhecida pela população, pois é de difícil acesso e que permite que condutas ilícitas sejam praticadas através dela, uma vez que não aparecem nos mecanismos de buscas tradicionais, como é o *Google*.

3. ADEQUAÇÃO DA LESGISLAÇÃO PENAL BRASILEIRA PARA OS CRIMES VIRTUAIS

3.1 LEGISLAÇÃO ESTRANGEIRA EM RELAÇÃO AOS CRIMES VIRTUAIS

Em se tratando de legislação estrangeira, se tem como referência a Convenção de Budapeste, conhecida como Convenção sobre o Cibercrime. Foi estabelecida pelo Conselho da Europa na Hungria em 2001 e está em vigor desde 2004, após ser ratificada em cinco países, e agora é adotada por mais de 44 Estados-membros e mais alguns Estados não membros, como a Argentina, Canadá, Chile, Colômbia, Estados Unidos da América, República Dominicana e Peru, com objetivo de identificar e tipificar os crimes cometidos na *internet*.

A convenção de Budapeste é composta por quatro capítulos, a qual abrangem (a) termologias, (b) medidas a serem tomadas em nível nacional, (c) cooperação internacional e (d) disposições finais. Entre os principais aspectos do tratado estão as definições de crimes cibernéticos, que podem incluir a violação da confidencialidade de sistemas e dados informáticos, computadores, conteúdos e direitos autorais (SANTOS, 2022)

O memorando explicativo do Tratamento alerta para as crescentes preocupações com o uso malicioso dos meios de comunicação *online*, bem como a facilidade com que as informações são armazenadas em sistemas informáticos, aumentando a disponibilidade dos fluxos de informações. Esses fatores, juntamente com os recentes avanços nas novas tecnologias e mudanças na sociedade, têm contribuído para o aumento da incidência de crimes cibernéticos. Por outro lado, durante as atividades comemorativas de seu 21º aniversário em 2021, a Convenção de Budapeste destacou o potencial para incentivar estruturas de cooperação público-privadas e harmonização entre legislações e outras estruturas legais e administrativas dedicadas ao combate aos crimes cibernéticos.

É importante salientar que, embora a Convenção de Budapeste tenha sido originalmente elaborada com um enfoque punitivo, sua relevância contemporânea decorre do contínuo trabalho de atualização e diálogo com outras discussões, tais como a defesa dos direitos humanos na era digital. Nos

últimos anos, o tratado tem sido consolidado como uma base legal fundamental para a cooperação internacional, além de servir como guia para a elaboração de legislações nacionais.

Com isso, a Convenção de Budapeste possibilita a punição dos “criminosos virtuais”, apesar de cada país ter sua própria legislação e soberania. Mesmo em casos em que um crime tenha impacto em múltiplos países, as partes envolvidas podem cooperar entre si para conduzir investigações apropriadas e, se necessário, prender o infrator. (NETO, 2009).

3.2 LEGISLAÇÃO NACIONAL EM RELAÇÃO AOS CRIMES VIRTUAIS

No brasil, existem algumas iniciativas que indicam a intenção do legislador em adaptar o sistema jurídico ao novo contexto tecnológico. No entanto, a legislação em vigor ainda é insuficiente e muitos projetos relevantes ainda estão em tramitação há anos no Congresso Nacional. Apensar disso, não é correto afirmar que não há regulamentação alguma no país em relação à criminalidade informática, uma vez que muitas condutas criminosas podem ser enquadradas nos tipos penais já previstos na legislação brasileira. Caso não haja uma legislação específica, o infrator deve ser julgado dentro do próprio Código Penal, respeitando-se as devidas diferenças.

3.2.1 Lei 11.829/2008 – Pedofilia pela Internet

Como já mencionado no capítulo anterior, a finalidade da Lei 11.829 de 25 de novembro de 2008, é resguardar a integridade da criança e do adolescente. Diante disso, a legislação aprimora o combate à produção, venda e distribuição de pornografia infantil, bem como a criminalização a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na *internet*.

A legislação altera a redação da Lei 8.069/1990 que é o Estatuto da Criança e do Adolescente, em seus artigos 240 e 241 e acrescenta os artigos 241-A, 241-B, 241-C, 241-D e 241-E.

Por fim, é importante destacar que, para ter acesso a alguns dos materiais mencionados na Lei, não é necessário recorrer a nenhuma técnica de

invasão ou possuir conhecimentos avançados em programação, bastando ter armazenados em algum dispositivo virtual pessoal. A Lei reforçou ainda mais o combate a essas práticas, criminalizando comportamentos que antes não eram claramente definidos como ilícitos. (VALERA, 2019)

3.2.2 Lei 12.737/2012 – Lei dos Crimes Cibernéticos

A lei 12.737/2012 foi sancionada em 03 de dezembro de 2012, e entrou em vigor em 2013, pela Presente da República Dilma Roussef, e dispõe acerca da tipificação criminal de delitos informáticos e alterou o Código Penal.

Conhecida como “Lei Carolina Dieckmmann”, esse apelido foi dado em referência ao fato de a atriz ter sido vítima de *hackers* que invadiram seu computador e que diante da recusa da chantagem de 10 mil reais, teve suas fotos de cunho íntimo divulgadas nas redes sociais e *internet*.

A criação desta lei está intimamente ligada à Teoria Tridimensional do Direito, desenvolvida por Miguel Reale. Essa teoria foi concebida com o objetivo de adaptar o direito à sociedade, assim como a lei em questão.

A teoria mencionada era abordada e compreendida sob uma perspectiva com três elementos distintos: fato, valor e norma. Segundo Reale (2000):

> O Direito não é apenas a norma ou a letra da lei, pois é muito mais do que a mera vontade do Estado ou do povo, é o reflexo de um ambiente cultural de determinado lugar e época, em que os três aspectos – fático, axiológico e normativo – se entrelaçam e se influenciam mutuamente numa relação dialética na estrutura histórica.

A Lei em questão passou a abranger casos como esse. Sendo assim, para que a conduta seja enquadrada nessa categoria, é preciso que haja invasão de dispositivos eletrônicos de caráter pessoal, com a finalidade de obter, adulterar ou destruir dados ou informações.

Para o combate dos crimes virtuais, a referida Lei criou tipos incriminadores, com a inclusão dos artigos 154-A, 154-B e a alteração da redação dos artigos 266 e 298, in verbis:

> **Invasão de dispositivo informático**
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou

> informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput.**
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."
> **Ação penal**
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.
> **"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública**
> Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública."
> **Falsificação de documento particular**
> 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."
> (BRASIL, 2012)

Considerando o alto grau de desenvolvimento da legislação brasileira, esta Lei recebeu muitas críticas, uma vez que especialistas apontam que as penalidades são demasiadamente brandas.

Cardoso, afirma:

> O advento da Lei 12.737/2012, criou novos tipos incriminadores, contudo, o texto normativo não produziu grandes reformas no ordenamento jurídico, tampouco solucionou o problema que o Direito brasileiro enfrenta sobre o tema, todavia, este dispositivo legal trouxe significativos avanços ao tipificar condutas gravosas à sociedade, além disso, a referida lei foi a primeira a funcionar como instrumento normativo destinado especificamente à tutela do bem jurídico no mundo virtual.

No entanto, devido à grande incidência desses delitos, discute-se que os transgressores sejam submetidos a penalidades mais severas, com sanções mais rigorosas a fim de dissuadi-los de perpetrar tais atos ilícitos.

3.2.3 Lei 12.735/2012 – Lei Azeredo

A Lei 12.735/2012 foi sancionada em 30 de novembro de 2012, conhecida como Lei Azeredo, por ser elaborada pelo deputado federal Eduardo Azeredo, teve origem no projeto de lei nº 1999 (PL 84/99) e tipifica condutas realizadas mediante uso de sistemas eletrônicos, digitais ou similares, que sejam praticadas contra sistemas de informatizados e similares; e dá outras providencias. (BRASIL, 2012).

3.2.4 Lei 12.965/2014 - Marco Civil da Internet

O Marco Civil da Internet é fundamental para regulamentação do uso da internet no país.

Segundo Cardoso (2020, p. 10):

> Regula a utilização da *web* no Brasil por meio de princípios, garantias, direitos e deveres, para os usuários da rede, e traça diretrizes para a atuação do Estado.

A Lei 12.965/2014 foi sancionada em 23/04/2014, pela presidente Dilma Rousseff. Seus principais pilares são a liberdade de expressão, a proteção da privacidade e dos dados pessoais e a neutralidade da rede. Essa Lei, por ser ampla e genérica, tem impacto em diversas áreas do Direito brasileiro, e sua maior repercussão no campo criminal é relacionada à obtenção de registros de acesso junto aos provedores de *internet*.

Cardoso afirma:

> O objetivo principal do marco civil, é prever práticas criminosas no ambiente online, prezar pela neutralidade da rede, pela liberdade de

> expressão, e pela privacidade dos seus usuários, evitando que suas informações pessoais sejam vendidas ou ofertadas a empresas sem sua prévia autorização, além de assegurar o sigilo em suas comunicações. (2020, p. 10)

Apesar do esforço legislativo para regular as relações sociais na internet, há críticas à legislação devido às suas lacunas, especialmente porque as normas não cobrem todo o espectro de atividades criminosas na internet. Algumas lacunas são supridas por outras legislações, como a regulamentação de compras *online*, entre outras circunstâncias que podem ser exploradas por criminosos para cometerem delitos (SIQUEIRA, 2017, p. 126).

3.2.5. Lei 13.709/2018 – Lei Geral de Proteção de Dados

Foi introduzida recentemente uma importante inovação jurídica, a Lei Geral de Proteção de Dados (LGPD), aprovado pelo ex-presidente Michel Temer e promulgada em 19 de setembro de 2020. O objetivo dessa lei é aumentar a segurança jurídica dos cidadãos, fornecendo proteção dentro e fora do país, e garantindo a proteção dos dados pessoais de todas as pessoas no território nacional. Dados pessoais são definidos como qualquer informação que possa identificar um indivíduo. A LGPD é uma medida crucial para proteger a privacidade dos cidadãos e garantir a segurança de suas informações pessoais.

Embora a nova lei não traga disposições específicas no âmbito penal e processual penal, o Artigo 42 estabelece a responsabilidade dos administradores de empresas em casos de incidentes, respondendo tanto por suas ações quanto por omissões. Ainda que essa previsão esteja relacionada à esfera cível, é possível que seja aplicada também ao âmbito criminal e administrativo, dada a crescente atenção aos crimes empresariais. Além disso, a responsabilidade se estende aos gestores e operadores de dados, que são responsáveis pela proteção das informações sob sua guarda. (TONI, FEDRICO, 2020).

CONCLUSÃO

O presente estudo teve como propósito analisar o surgimento da *internet*, as características e conceitos do crime virtual, bem como as principais condutas ilícitas praticadas no ambiente virtual, abordando ainda, as legislações que vigoram a fim de punir os infratores de tais delitos.

Ao longo do trabalho, pode-se constatar a extrema relevância do estudo sobre os crimes na atualidade, visto que, a internet trouxe significativos benefícios à sociedade, por sua praticidade e conectividade, entretanto, os malefícios trazidos pelo mesmo meio foram expressivos, diante do aumento drástico dos crimes cibernéticos à medida que a *internet* se expande e se torna cada vez mais popular. Os danos causados por essa modalidade delitiva são inestimáveis, provocando inúmeros impactos psicológicos, econômicos e financeiros. O combate aos crimes virtuais requer legislações específicas, tendo em vista que esse ambiente se apresenta desafiador.

Pode-se constatar que a legislação brasileira não acompanhou adequadamente a rápida e intensa evolução dos crimes virtuais, tornando-se necessária a elaboração de uma legislação mais abrangente, específica e eficaz sobre o assunto.

Vale ressaltar que existem leis que tratam do referido tema como bem mencionadas no presente estudo, tais como a lei 12.737/2012 (Lei Carolina Dieckmann), Lei 12.735/2012 (Lei Azeredo), Lei 12.965/2014 (Marco Civil da Internet), assim como outras, entretanto, não são suficientes para tipificar adequadamente os infratores.

Diante disso, além do déficit da legislação, há um desafio de identificar e rastrear os perpetradores desses crimes, vez que eles podem estar em qualquer lugar do mundo e utilizam técnicas sofisticadas para mascarar suas identidades.

Por fim, salienta-se que é necessário que haja um esforço contínuo para aprimorar as leis e políticas relacionadas aos crimes virtuais, além de investimentos em tecnologias de segurança cibernética.

REFERÊNCIAS

BRAMILLA, Guilherme de Souza. Crimes virtuais. Toledo Prudente Centro Universitário, 2015.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 28 mar. 2023.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera a Lei no 9.296, de 24 de julho de 1996, que regula as interceptações telefônicas, a Lei no 9.504, de 30 de setembro de 1997, que estabelece normas para as eleições, e o Código de Processo Penal, a fim de adequar a legislação à investigação criminal pela internet e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em: 04 abr. 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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 04 abr. 2023.

BUTURI, Leonardo Viese; PANZA, Luiz Osório Moraes. Direito Penal: Internet X Estupro Virtual e Pedofilia Virtual. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/18639/1/ARTIGO%20CIENTIFICO%20LEONARDO%20VIESE%20BUTURI%20-%209MC%20-%202017101307.pdf>. Acesso em: 30 de mar. de 2023.

CARDOSO, Lucas de Holanda M. O Direito na Era Digital: O Cibercrime no Ordenamento Jurídico Brasileiro. 2020. Disponível em: < https://cepein.femanet.com.br/BDigital/arqPics/1611400792P734.pdf>. Acesso em: 02 de abr. de 2023

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Âmbito Jurídico. 2012. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/>. Acesso em: 13 dez. 2022.

CARVALHO, Paulo Roberto de Lima. Crimes cibernéticos: uma nova roupagem para a criminalidade. Jus.com.br. 2014. Disponível em: < https://jus.com.br/artigos/31282/crimes-ciberneticos-uma-nova-roupagem-para-a-criminalidade>. Acesso em: 14 de dez. 2022

CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. 201. Disponível em: <https://crimes-virtuais-vitimas-reais-1nbsped_compress.pdf>. Acesso em: 01 de abril de 2023

CORREA SEGUNDO, Luiz Carlos Correa. Crimes Cibernéticos. Monografia apresentada pela Faculdade do Estado do Maranhão. São Luiz, 2016.

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

CUNHA, Rogério Sanches. Manual de Direito Penal: Parte Geral. Salvador: Juspodivm, 2014.

FERREIRA, Ivette Senise. Direito & Internet: Aspectos Jurídicos Relevantes. 2 ed. São Paulo: QuartierLatin. 2005.

JESUS, Damásio Evangelista de; MILAGRE, José Antônio. Manual de Crimes Informáticos. 1° ed. São Paulo: Saraiva, 2016.

MACHADO, Bruna de Oliveira; MATTOS, Karoline Reis; SIQUEIRA, Marcela; et al. Crimes Virtuais e a Legislação Brasileira. 2017. (Re)pensando Direito. Disponível em: <https://core.ac.uk/download/pdf/229767447.pdf>. Acesso em: 30 de mar. de 2023.

MEDEIROS, Claudia Lucio de. Deficiências da legislação penal brasileira frente aos crimes cibernéticos**.** Universidade Estadual do Ceará, 2010.

MIRABETE, Julio Fabbrini. Código Penal Interpretado. 3. Ed. São Paulo: Atlas, 2003.

NETO, Pedro Américo de Souza. Crimes de Informática. [S.l]: Universidade do Vale do Itajaí, 2009.

PINHEIRO, Patricia Peck. Proteção de dados pessoais – Comentários à Lei N.13.709/2018 (LDPD). São Paulo: Saraiva Educação, 2018.

REALE, Miguel. Teoria Tridimensional do Direito, p. 85. 5ª ed., Editora Saraiva, São Paulo, 2003.

ROCHA, Manuel Lopes. Crimes da Informática. Remy Gama Filho. Editora: CopyMarket.com, 2000.

SANTOS, Bruna Martins dos. Convenção de Budapeste Sobre o Cibercrime na América Latina: Uma Breve Análise Sobre a Adesão e Implementação na Argentina, Brasil, Chile, Colômbia e México. 2020. Disponível em: <https://www.derechosdigitales.org/wp-content/uploads/PT-Ciberdelincuencia-2022.pdf>. Acesso em: 02 de abr. de 2023.

SOUZA, Eric Henrique de. Crimes digitais e evolução da legislação. Jusbrasil, 2017. Disponível em: < https://ericmsouza.jusbrasil.com.br/artigos/420184154/crimes-digitais-e-evolucao-da-legislacao>. Acesso em: 13 de dez. de 2022.

TONI, Mariana Helou Giraldi; FREDERICO, Sérgio Augusto. Crimes Digitais: Responsabilização e Alternativas Para Tipificação Penal. 2020. Disponível em:

<https://cepein.femanet.com.br/BDigital/arqPics/1911401170P952.pdf>. Acesso em: 30 de mar. de 2023.

VALERA, Paulo Vinícius de Carvalho. Crimes Virtuais e Legislação Brasileira. 2019. Disponível em: <https://servicos.unitoledo.br/repositorio/bitstream/7574/2268/3/CRIMES%20VIRTUAIS%20E%20A%20LEGISLA%C3%87%C3%83O%20BRASILEIRA%20-%20Paulo%20Vin%C3%ADcius%20de%20Carvalho%20Valera.pdf>. Acesso em: 02 de abr. de 2023.

VIANNA, Túlio; MACHADO, Felipe. Crimes Informáticos Conforme a Lei 12.737/2012. 1ª ed. Belo Horizonte: Fórum, 2013.