

CENTRO UNIVERSITÁRIO UNINOVAFAPÍ
BACHARELADO EM DIREITO

MARIA EMANUELLE DOS SANTOS RODRIGUES
MICHELE CARVALHO SILVA
YSIS GALIANA DA SILVA SANTOS

**A (IN)SUFICIÊNCIA LEGISLATIVA BRASILEIRA NA PUNIÇÃO DOS CRIMES
VIRTUAIS**

TERESINA
2022

MARIA EMANUELLE DOS SANTOS RODRIGUES
MICHELE CARVALHO SILVA
YSIS GALIANA DA SILVA SANTOS

**A (IN)SUFICIÊNCIA LEGISLATIVA BRASILEIRA NA PUNIÇÃO DOS CRIMES
VIRTUAIS**

Artigo de Trabalho de Conclusão de Curso apresentado à Banca Examinadora do Centro Universitário UNINOVAFAP, como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientadora: Profa. Ma. Viviane Maria de Pádua Magalhães

TERESINA
2022

FICHA CATALOGRÁFICA

R696i Rodrigues, Maria Emanuelle dos Santos.

A (in)suficiência legislativa brasileira na punição dos crimes virtuais. Maria Emanuelle dos Santos Rodrigues; Michele Carvalho Silva; Ysis Galiana da Silva Santos. – TERESINA: UNINOVAFAPI, 2022.

Artigo (Graduação em Direito) – Centro Universitário UNINOVAFAPI / Afya, Teresina, 2022.

22 p.; 23cm.

Orientador (a): Profa. Ma. Viviane Maria de Pádua Magalhães. Centro Universitário UNINOVAFAPI, 2022.

1. Legislação brasileira. 2. Crimes virtuais. 3. Estado. I. Título. II. Magalhães, Viviane Maria de Pádua.

CDD 340.581 22

Catálogo na publicação
Antonio Luis Fonseca Silva – CRB/1035
Francisco Renato Sampaio da Silva – CRB/1028

MARIA EMANUELLE DOS SANTOS RODRIGUES

MICHELE CARVALHO SILVA

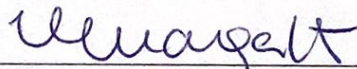
YSIS GALIANA DA SILVA SANTOS

**A (IN)SUFICIÊNCIA LEGISLATIVA BRASILEIRA NA PUNIÇÃO DOS CRIMES
VIRTUAIS**

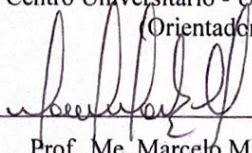
Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do Centro
Universitário UNINOVAFAPI, como requisito
parcial para obtenção do grau de Bacharel em
Direito.

Data de Aprovação: 16 /11/2022

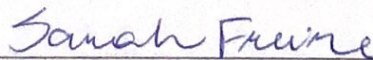
BANCA EXAMINADORA



Prof. Ma. Viviane Maria de Pádua Magalhães
Centro Universitário - UNINOVAFAPI
(Orientadora)



Prof. Me. Marcelo Martins Eulálio
Centro Universitário - UNINOVAFAPI
(1º Examinador)



Prof. Ma. Sarah Maria Veloso Freire
Centro Universitário – UNINOVAFAPI
(2º Examinador)

AGRADECIMENTOS

A Deus, em primeiro lugar, pelo dom da vida, por ter sido nosso guia, por ter nos sustentado, conduzido e nos dado força e coragem durante esta caminhada.

Aos nossos pais, pelo amor, carinho, ensinamentos, e por não medirem esforços para que pudéssemos ter a oportunidade de estudar, e por serem nossos alicerces diante de todas as dificuldades enfrentadas no decorrer destes cinco anos.

Aos nossos familiares e amigos que torceram, vibraram e nos incentivaram a conquistar nossos objetivos.

A nossa orientadora Prof. Ma. Viviane, e a todos os professores por todos os conhecimentos compartilhados ao longo desse processo.

E por fim, a todos que colaboram de alguma forma para que chegássemos até aqui. Obrigada.

RESUMO

O avanço tecnológico proporcionou grandes contribuições e vantagens para a sociedade, mas também viabilizou grandes lacunas para a prática de atos ilícitos. A evolução tecnológica transformou o dia a dia, o modo de pensar e agir da sociedade mitigando as barreiras temporais e territoriais que anteriormente limitavam a comunicação humana e as interações sociais no ambiente virtual, fazendo com que o direito se adapte para essa modificação social. O presente artigo abordará os principais crimes cometidos no meio virtual. Iniciar-se-á com a apresentação do conceito e abordagem das considerações mais importantes sobre o assunto, elencando o contexto histórico do surgimento dessa ferramenta, bem como apresentando uma abordagem e explanação acerca da legislação vigente no ordenamento jurídico atual. Deste modo, foi realizada uma revisão bibliográfica, com fundamentação em livros de doutrinadores do Direito, artigos publicados, legislação brasileira penal e constitucional. Tendo como objetivo principal analisar como o Estado se posiciona diante das necessidades legislativas para impor limites e regulamentar a criminalidade virtual.

Palavras-Chaves: Legislação brasileira. Crimes virtuais. Estado.

ABSTRACT

The technological society, but also great contributions and benefits via large gaps for the practice of illicit acts. Technological evolution has transformed everyday life, society's way of thinking and acting mitigates temporal and territorial barriers that previously limited social communication, making the law not affected by the virtual environment, making it adapt to this transformation. Social. This article will discuss the main crimes committed in the virtual environment. It will be with the presentation of the concept and the most important considerations on the subject, listing the historical context of the survey tool, as well as presenting an explanation about the legislation in force in the current legal system. In this way, a bibliographic review was carried out, based on law books, published articles, criminal and constitutional Brazilian legislation. Having as main objective to analyze the State to position itself in the face of regulations regarding the importance and limits of virtual crime.

Keywords: Brazilian legislation. Virtual crimes. State.

1 INTRODUÇÃO

Com o passar do tempo, a tecnologia tem se tornado indispensável na vida de parte da população mundial. Para algumas pessoas a internet é fundamental para o desenvolvimento cultural, profissional e educacional, além de ser uma ferramenta de lazer e entretenimento, que possibilita a otimização de várias rotinas, bem como proporciona um alto poder de integração entre as pessoas.

Por outro lado, ligado a crescente utilização da internet, pessoas de má fé aproveitam da vasta variedade e facilidade que o ambiente virtual oferece para propagar e executar atividades ilícitas, a fim de obter vantagens financeiras, ou até mesmo ferir a integridade, dignidade e honra das pessoas, fazendo com que isso na maioria das vezes alcance uma proporção que ultrapassa os limites constitucionais ao mesmo passo em que fere o direito do outro.

Nessa direção, busca-se compreender a maneira como esse fenômeno social de criminalidade se manifesta no ambiente virtual, os vestígios que esses crimes podem deixar e como o ordenamento jurídico brasileiro se posiciona diante de tais delitos.

Dado o crescimento exacerbado do uso da tecnologia na Era Digital que vivemos atualmente na qual o maior número de informações compartilhadas entre as pessoas são por meio de dispositivos virtuais e da internet, em que grande parte das pessoas, dos mais diversos lugares passaram a comunicar-se, pode-se notar a prática comum de crimes de variadas espécies, definidos ao longo do tempo, como crimes digitais, crimes de tecnologia, cibercrimes ou crimes informáticos; dessa forma, discute-se os fundamentos dogmáticos: A legislação brasileira é (in)suficiente na punição dos crimes virtuais?

Dessarte, o objetivo geral é analisar a aplicabilidade das leis na punição dos crimes cometidos na internet, e os objetivos são: descrever o contexto histórico dos crimes virtuais; verificar as consequências de tais delitos; examinar a prática dos crimes virtuais à luz do Direito Penal; e identificar as formas de comprovação dos crimes virtuais.

Será analisado a atual realidade acerca do combate e prevenção aos crimes cometidos por meio da internet, e em quais condições a legislação brasileira se encontra preparada para lidar com esse tipo de prática delituosa, apresentando as consequências causadas em decorrência da carência normativa para tais delitos, bem como as dificuldades que o Estado enfrenta tanto para investigar, quanto para punir os infratores. A sociedade precisa ter ciência da segurança legislativa estabelecida a respeito dos crimes cometidos no âmbito virtual, para isso necessita-se de uma legislação penal adequada para a proteção de dados nos meios eletrônicos.

Para esse propósito, valendo-se do método dedutivo, que consiste na observação das ações gerais que envolvem o seguinte tema afim de obter características particulares do objeto de estudo, e do procedimento bibliográfico, utilizando-se de pesquisa documental, fundamentado em consultas de materiais teóricos, como artigos, livros e leis, assim como arquivos digitais que abordam o tema.

O trabalho divide-se, então, em três tópicos, cujo o primeiro propõe-se a descrever uma origem histórica, buscando demonstrar como se deu o surgimento e funcionamento da internet, e mais adiante, dos crimes que utilizam do meio virtual como artifício ou objeto no cometimento de infrações. Para constatar que a internet é o espaço idôneo para a prática delitiva, é necessário estabelecer a distinção das espécies de crimes informáticos, apresentando, em seguida, os obstáculos enfrentados pelos operadores do direito na punição de tais infrações, sendo, portanto, um tema de grande importância para as ciências jurídicas

Avançando no entendimento sobre os crimes informáticos, o segundo tópico objetiva discutir quais são os bens jurídicos sujeitos a serem violados por essa espécie delitiva, abordando especificamente a cerca de três espécies de delitos específicos que se desenvolvem no ambiente virtual, trazendo a tipificação e como os mesmos se manifestam na prática.

Por fim, o terceiro é destinado a análise da legislação no âmbito do Código Penal vigente acerca dos crimes cometidos na internet, a fim de verificar sua eficácia diante da vasta diversidade de delitos cometidos no âmbito virtual. O trabalho é de fundamental importância, em razão do uso inadequado de tecnologias e programas de computadores. Como resultado, busca-se verificar a (in) suficiência legislativa brasileira na punição dos crimes informáticos e o impacto das novas tecnologias no estudo do Direito, especialmente nos ramos penais.

2 CRIMES VIRTUAIS

Crimes informáticos são os delitos cometidos por meios eletrônicos. Conceitua-se crimes informáticos “como fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação” (JESUS; DAMASIO, 2016, p.49).

Em outras palavras, os crimes informáticos, são crimes cometidos em dispositivos eletrônicos, que na maioria das vezes conectados à rede de internet, que invadem programas (softwares) para obter informações armazenadas, na perspectiva de coibir tais condutas surge o direito informático.

Direito informático que é o conjunto de princípios, normas e entendimentos jurídicos oriundo de atividades informáticas. Assim, é um ato típico e antijurídico através da

informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. (JESUS; MILAGRE, 2016, p.49-50)

Como forma de coibir tais condutas e proteger o bem jurídico tutelado, não temos um código de direito penal informático, mas temos dispositivos que versam sobre a matéria no nosso Código penal.

Além da previsão legal no código penal a inviolabilidade da informação também está assegurada no artigo 5º inciso X, da Constituição Federal de 1988 que diz que “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” (BRASIL, 1988). Tais garantias decorrem assim de um direito natural.

Assim a inviolabilidade de informação e de dados informáticos é decorrência natural do direito a à intimidade e privacidade, devendo, portanto, ser reconhecido como direito essencial para a convivência social (VIANNA; MACHADO, 2013, p.16).

Com isso, a denominação mais precisa para os delitos estudados é “crimes informáticos” ou “delitos informáticos”, já que se baseia no bem jurídico penalmente que é a inviolabilidade de dados armazenados em dispositivos eletrônicos (VIANNA; MACHADO, 2013, p.21).

3 ESPÉCIES DE CRIMES VIRTUAIS

No presente tópico, foram abordados crimes contra a inviolabilidade de dispositivos informáticos, crimes contra a honra e crimes contra o patrimônio- estelionato, discorrendo sobre seus conceitos e como tais delitos são praticados.

3.1 Crimes contra honra

A honra é tutelada e resguardado na Constituição Federal de 1988, com a finalidade de resguardar um bem considerado imaterial relativo a pessoa humana. Dessa forma, o indivíduo tem direito à vida, a integridade psíquica e física, não podendo ter sua honra ultrajada, uma vez que possui seu patrimônio moral amparado constitucionalmente pela legislação.

Em nossa Carta Magna de 1988, a honra tem previsão no rol dos direitos fundamentais, previsto no art. 5º, X:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

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. (BRASIL, 1988).

Diante disto, observa-se seguramente que a honra deve ser resguardada, tanto é que o legislador se utilizou do ordenamento constitucional para asseguar-la, numa predisposição de gerar aversão e oposição a qualquer ato lesivo.

Inegavelmente a honra é um dos bens mais preciosos do ser humano. Sendo uma qualidade moral e vulnerável, podendo ser ferida e devendo, na mesma proporção ser resguardada.

Para Silva (2008), a honra é um conjunto de atributos que retratam e configuram a dignidade da pessoa humana, a reputação, a boa fama e o respeito.

No âmbito penal, a honra possui proteção no capitulo V do Código Penal, que trata-se dos Crimes contra a Honra em seus artigos 138 e 145.

Enquanto bem jurídico, não há uma aceção específica a cerca de sua definição, em razão de sua subjetividade, possuindo conceito variável, determinado por diversos fatores, dentre eles: histórico, social, econômico e político, que devem ser considerados para assim concretizar seus objetivos de proteção.

Para a doutrina, há duas classificações ao tratar-se da honra, a primeira de natureza objetiva, que diz respeito a imagem que a pessoa possui diante do meio social e a segunda, de natureza subjetiva, que é o julgamento que o indivíduo faz de si mesmo, dessa maneira descreve Prado (2008, p. 213):

“A honra, do ponto de vista objetivo, seria a reputação que o indivíduo desfruta em determinado meio social, a estima que lhe é conferida; subjetivamente, a honra seria o sentimento da própria dignidade ou decoro”.

3.1.1 Calúnia

A calúnia caracteriza-se na ação de atribuir falsamente a alguém um fato definido como crime. Neste delito, o bem tutelado é a honra objetiva da pessoa, aquela que terceiros pensam a seu respeito.

Considera-se um dos crimes mais graves ao tratar-se dos crimes contra honra, e possui tipificação no código penal brasileiro no seguinte artigo:

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.

Dessa forma, para que se configure calúnia é necessário que seja imputado a alguém um fato inverídico e definido como crime. É imprescindível a presença do *animus caluniandi*, ou seja, o dolo, a vontade efetiva de ofender a vítima e depreciar sua honra no meio em que vive.

Para Nucci (2017), caluniar é tirar a confiabilidade da pessoa no meio social a qual ela pertence, havendo sobretudo a intenção de ferir e manchar a imagem de alguém, considerando o dolo, e se consumando a partir do momento em que a falsa arguição chega ao conhecimento de outras pessoas.

3.1.2 Difamação

A difamação, trata-se de um delito que fere a honra objetiva, assemelhando-se a calúnia, dependendo assim da imputação de algum fato a alguém. No entanto, nesse contexto não é necessário ser criminosa, tendo em vista que a capacidade para depreciar a reputação da vítima, ou seja, uma imagem que ela desfruta na coletividade, independe de sua veracidade.

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

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

Exceção da verdade

Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

Dessa forma, para configurar a tipicidade do crime, é necessário que o autor se refira ao acontecimento de forma descritiva e, não limitando-se apenas a ofender a vítima.

Igualando-se a calúnia, o momento de consumação do delito acontece, ao modo que a demais pessoa tome ciência das informações proferidas de maneira inverídica.

3.1.3 Injúria

O delito de injúria encontra-se elencado no art.140 do Código Penal brasileiro que prevê: “Art. 140 – Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena – detenção, de um a seis meses, ou multa”.

Ao tratar-se do crime de injúria observa-se que este se dará com a simples ofensa da dignidade e integridade da vítima, mediante atribuições negativas ou xingamentos, bem como com insultos ou ofensas que abale o conceito que a vítima tem de si próprio.

A dignidade é ferida quando atacam as qualidades morais da pessoa, enquanto a integridade atenta contra suas qualidades físicas ou intelectuais.

A doutrina a classifica como absoluta, quando a imputação atribuída a vítima é indiscutivelmente ofensiva a honra subjetiva, independente do lugar ou tempo que foi proferida. Já na injúria relativa, a palavra supostamente ofensiva pode ser considerada aceitável, a depender do lugar ou época em que foi dito.

Desse modo, observa-se que o legislador se preocupou em instituir normas e tipificar os institutos que tratam dos crimes contra a honra, buscando preservar o bem jurídico tutelado. Entretanto com crescimento tecnológico, e as inovações advindas desse fenômeno, a proteção da honra vem sendo questionada pelas novas formas de violação por meio das ferramentas tecnológicas que ostentam novas propagações de ofensas, após o advento da internet.

3.2 Crimes de invasão de privacidade e intimidade

Acerca de como funciona a realidade virtual, seus inúmeros dispositivos de armazenamento de dados e troca de informações, surge o que se denomina crimes virtuais, ou seja, infrações no campo digital perante o direito à privacidade e a intimidade que constituem direitos de personalidade: o que se aproxima da ideia de pessoal, intransferível, particular e segredo da pessoa humana.

De acordo com Lima (2006, p. 31), o conceito de crimes virtuais são:

(...) temos que crimes de computador são qualquer conduta humana (omissiva ou comissiva) típica, antijurídica e culpável, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, facilitado de sobremodo a execução ou a consumação da figura delituosa, ainda que cause um prejuízo a pessoas sem que necessariamente se beneficie o autor ou que, pelo contrário, produza um benefício ilícito a seu autor, embora não prejudique a vítima de forma direta ou indireta (LIMA, 2006, p. 31).

O direito à vida privada e a intimidade estão resguardados no art. 5, inciso X da Carta Magna e o mesmo texto atribui tipificação diferente ao dispor que: “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” (BRASIL, 1988). Entretanto, isto não quer dizer sejam direitos ilimitados, pois, quando se contrapõem a outros direitos fundamentais, sofrem limitações.

Dessa forma, a compreensão de intimidade e privacidade são atuais e até este momento se encontram em desenvolvimento a respeito da proteção dos dados pessoais nos meios virtuais em decorrência da evolução tecnológica na era da sociedade de informação

É importante salientar que muitas dúvidas surgem sobre o alcance desses direitos no âmbito digital.

A internet é um dos mecanismos mais importantes e eficientes que a humanidade já desenvolveu, mediante o processo de globalização alcançou patamar que atinge todas as camadas sociais, econômicas e políticas, assim, fazendo com que a ciência do direito não acompanhasse tal desenvolvimento. É notório que a popularização e massificação da comunicação e da tecnologia permita o compartilhamento e a divulgação de dados e imagens pessoais com facilidade na rotina das pessoas, ficando cada vez mais comum essas práticas sem a devida preservação legal dessas informações.

Crimes cometidos na internet com auxílio da tecnologia, ocorrem mediante agentes criminosos, que utilizam seus conhecimentos e habilidades para promoverem e alcançarem os objetivos a que se dispõem. Por outro lado, infelizmente a grande maioria dos usuários que utilizam as redes de comunicações virtuais, através de computadores, aparelhos celulares, redes sociais, endereços eletrônicos, ainda são leigos e despreparados para se defenderem do sofisticado sistema utilizado pelos criminosos.

3.3 Crimes contra a inviolabilidade do patrimônio – estelionato

No ordenamento jurídico não há delito denominado estelionato por meio virtual ou também conhecido por *scamming* como denomina o doutrinador Sydow (2022, p.612):

Scamming foi o apelido dado ao esquema fraudulento, ou seja, a fraude perpetrada através dos meios informáticos, no intuito de obter-se algumas vantagens ilícitas, em detrimento da vítima.

A *fortiori*, *scammer* é o estelionatário (ou fraudador pela nomenclatura do código) que age no meio virtual, que se utiliza de armadilhas e golpes constituídos especificamente para o uso da virtualidade e com o intuito de obter vantagens patrimoniais. E a escolha é feita pelo potencial alastrador, pela grande multiplicação, pelo número de vítimas atingidas e pela velocidade de retorno.

Sendo assim, este delito encontra-se tipificado no capítulo VI, art. 171 do Código Penal, que trata sobre o estelionato e outra fraude, como disposto:

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. (Brasil,1940).

Dessarte, o bem jurídico protegido no crime de estelionato é a inviolabilidade do patrimônio, pois trata-se de um crime patrimonial, no qual a prática consiste em utilizar de meios fraudulentos para obtenção de vantagem ilícita, sem utilização de violência ou grave ameaça, sua modalidade é dolosa, não sendo admitida a conduta culposa.

Entretanto, para que seja caracterizado o crime de estelionato é necessário que haja quatro elementos, sendo eles: enganar alguém ou induzi-la ao erro; ocorra obtenção de vantagem ilícita; tenha o emprego de artifício ardil ou qualquer outro meio fraudulento; que seja causado prejuízo à vítima. Para Grego (2022. ed.19) “O crime de estelionato é regido pelo binômio vantagem ilícita/prejuízo alheio. A conduta do agente, portanto, deve ser dirigida a obter vantagem ilícita, em prejuízo alheio”, em outras palavras, o agente utiliza-se de meios que levem outra pessoa ao erro, e assim obter dela vantagem ilícita, causando-lhe prejuízo.

Portanto, trata-se de um crime comum, cujo agente pode ser qualquer pessoa, sem que haja necessidade de qualificação específica, no estelionato, o sujeito passivo e a pessoa que aplica a fraude, mas pode ocorrer também concurso de pessoas, como, por exemplo, um sujeito induz ou mantém uma pessoa sobre, enquanto outro agente obtém vantagens ilícitas, nesse caso ambos serão sujeitos ativos.

Desse modo, o sujeito passivo é a vítima que é induzida ao erro e tem seu patrimônio violado, aquela que sofre o prejuízo, entretanto, pode haver dois sujeitos passivos, onde uma pessoa é enganada e outra pessoa sofre o prejuízo patrimonial.

Conforme o parágrafo quinto do artigo 171 do código penal a ação é pública condicionada, ou seja, a vítima tem que requerer que o autor do crime seja denunciado pelo Ministério Público, o artigo ainda dá um rol de em que casos a ação penal será incondicionada a representação.

§ 5º Somente se procede mediante representação, salvo se a vítima for:

I - a administração Pública, direta ou indireta;

II - criança ou adolescente;

III - pessoa com deficiência mental; ou

IV - maior de 70 (setenta) anos de idade ou incapaz (Brasil,1940).

Sendo assim, nos casos em que o estelionato for cometido contra a administração pública, criança ou adolescente, pessoas com deficiência mental, maiores de setenta anos ou incapaz, o ministério público, poderá apresentar denúncia, sem manifestação da vítima.

4 CRIMES VIRTUAIS NA LEGISLAÇÃO

No presente tópico, foram abordados os crimes contra a inviolabilidade de dispositivos informáticos, crimes contra a honra e crimes contra o patrimônio- estelionato, discorrendo sobre como esses crimes são praticados, trazendo seus conceitos e quem são os sujeitos ativos e passivos na ação.

4.1 Lei 12.965/2014 (Marco Civil da Internet)

O Marco Civil da Internet é uma Lei que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria (BRASIL,2014).

A lei 12.965/2014 foi sancionada pela ex-presidente Dilma Rousseff, no qual a mesma contém trinta e dois artigos e cinco capítulos, que tratam sobre os princípios da privacidade, da neutralidade e sobre a guarda de registros de acesso. Nesse sentido, Leite e Lemos (2014, p.02) comentam sobre esses princípios:

O respeito ao princípio da neutralidade de rede na internet veda a discriminação no tráfego de dados na internet em razão de seu conteúdo, origem e destino, serviço, terminal ou aplicação. É um importante instrumento no estímulo à inovação na internet, facultando o poder de escolha do usuário, promovendo a concorrência e a liberdade de circulação de dados e informações na rede. O segundo pilar do Marco Civil da Internet é o reforço da garantia constitucional da liberdade de expressão no ambiente online, procurando equilibrá-la com a proteção da intimidade, da honra e da imagem das pessoas. Além de tratá-la como fundamento das regras sobre internet, o texto é inovador na disciplina sobre a remoção de conteúdos da internet e sobre a responsabilidade de intermediários, um tema que ainda é objeto de controvérsias judiciais. As regras de não responsabilização de intermediários por atos de terceiros (a não ser pelo descumprimento de ordem judicial) e a preocupação com transparência em caso de retirada de conteúdo reforçam o papel da internet como espaço aberto aos debates públicos. Por fim, o Marco Civil da Internet introduz o tema da proteção de dados pessoais no sistema jurídico brasileiro. A partir da perspectiva de que as pessoas são titulares de seus dados pessoais, estabelece regras sobre o consentimento para tratamento de dados, permite somente coleta de dados relacionados com a finalidade das atividades prestadas, reafirma a necessidade de transparência nas políticas de privacidade, entre outras medidas.

O Marco Civil da Internet tem a finalidade de regular o uso da internet no Brasil, e por esse motivo, recebeu o apelido de “Constituição da Internet” de acordo com Damásio de Jesus (2016 p. 71):

O Marco Civil da Internet é considerado a “Constituição da Internet”, garantindo direitos e deveres a todos os atores da Internet brasileira (usuários, provedores de conexão e de serviços em geral). Fruto de um projeto nascido em 29 de outubro de 2009, da Secretaria de Assuntos Legislativos do Ministério da Justiça, em parceria com a Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, o Marco Civil foi uma construção colaborativa, disponível para consulta pública entre novembro de

2009 e junho de 2010, tendo recebido mais de duas mil contribuições. Após a fase de participação popular, ingressou no Congresso em 24 de agosto de 2011, por meio do Projeto de Lei n. 2.126, de iniciativa do Poder Executivo, projeto que visou estabelecer princípios, garantias, direitos e deveres para o usuário da Internet no Brasil. A legislação tem escopo de evitar, igualmente, decisões contraditórias proferidas pelo Judiciário, em casos semelhantes envolvendo tecnologia da informação, gerando insegurança jurídica.

É importante destacar que o Marco Civil da internet, foi uma importante inovação na legislação brasileira, visto que, não existia no Brasil outra lei específica que tratasse dos deveres dos provedores de acesso, aplicações e dos direitos dos usuários (JESUS, 2014, p.18). Outro ponto que deve ser mencionado, é a responsabilidade dos provedores de internet, cujo o artigo dezoito da lei 12.965/14 isenta os provedores de conexão de internet de serem responsabilizados civilmente por conteúdos gerados por seus usuários, porém no artigo dezenove da mesma lei, ressalta que:

O provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. (Brasil, 2014).

Por ser uma norma que tenta garantir a liberdade de expressão e evitar a censura, o Marco Civil da Internet responsabiliza o provedor de aplicações por danos que decorram de conteúdo gerado por terceiro, somente em caso de descumprimento de decisão judicial. Entretanto, a decisão deve conter a identificação clara e específica do conteúdo apontado como infringente para assim permitir a localização inequívoca do material.

4.2 Lei 14.155/2021 e suas alterações

Promulgada em 27 de maio de 2021 a lei 14.155/2021 altera alguns artigos do Decreto-Lei 2.848/1940, tornando mais grave os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, para fins didáticos será analisada as alterações nos artigos 154-A e 171 do Código Penal.

Desse modo, a referida lei trouxe modificações importantes para o Código Penal, alterando os crimes de dispositivos informáticos, tipificado no artigo 154-A do Código Penal, no qual será comparado as atualizações legislativas com a redação anterior.

Com isso, inicialmente destaca-se o caput do referido artigo, que constava o seguinte texto:

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: (BRASIL,1940).

Entretanto, após a lei 14.155/2021 passou a ter a seguinte redação:

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: (BRASIL,1940).

Desse modo, antes na redação anterior continha: “invadir dispositivo informático alheio”, porém, com a modificação passou a ser: “invadir dispositivo informático de uso alheio”, com isso, o legislador tipifica que a invasão do dispositivo informático, necessita que seja de uso de terceiro, não podendo ser do agente que executa a ação. Ademais, antes o agente necessitava violar indevidamente o mecanismo de segurança do dispositivo informático, todavia, com a atualização, não se faz mais necessário esta violação para a qualificação do delito, basta que haja invasão no dispositivo informático conectado ou não a internet, com o fim de obter, adulterar ou destruir dados de informações sem autorização do usuário do dispositivo. Outra alteração importante no referido artigo, foi a majoração da pena, antes a pena era de detenção de três meses a ano e multa, passando para reclusão, de um ano a quatro anos e multa.

Da mesma forma, os parágrafos segundo e terceiro sofreram alterações, no parágrafo segundo aumentava-se a pena de um sexto a um terço se a invasão resultasse em prejuízo econômico, porém, a pena passou a ter aumento de um terço a um sexto da pena se a invasão resultar em prejuízo econômico.

Por conseguinte, o parágrafo terceiro dispõe que 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, a pena será de reclusão de dois a cinco anos e multa, de modo que o mesmo dispositivo previa pena de reclusão de seis meses a dois anos e multa, se a conduta não constituísse crime mais grave.

Continuando, passando para o artigo 171 do Código penal, que trata sobre o estelionato, a lei 14.155/2021, incluiu os parágrafos 2º-A e 3º-B, trazendo a modalidade de estelionato mediante fraude eletrônica como causa de aumento de pena se o crime for cometido mediante fraude eletrônica.

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, 1940).

Ademais, no Parágrafo quarto foi incluído o estelionato contra vulnerável como causa de aumento de pena, que era caracterizado somente se o crime fosse praticado contra idoso, porém após a lei 14.155/2021, passou a ser causa de aumento de pena, o crime de estelionato cometido contra idoso ou vulnerável. Apesar da inovação do dispositivo, com a nova redação surgiu lacunas ao citar a expressão “vulnerável”, alguns doutrinadores como Sydow (2021, p.639) acreditam que o legislador a aplica de modo análogo referente a:

- a. Menores de 14 (quatorze) anos.
- b. Alguém que, por enfermidade não tem o necessário discernimento para a prática do ato.
- c. Alguém que por deficiência mental, não tem o necessário discernimento para a prática do ato.
- d. Alguém que, por qualquer outra coisa, não pode oferecer resistência.

Por fim, é importante ressaltar que o parágrafo previa aumento do dobro da pena, caso o delito fosse cometido contra idosos, no entanto, após alteração, a pena poderá sofrer aumento de um terço ao dobro da pena, considerando a relevância do resultado gravoso, em situações em que a vítima for idoso ou vulnerável.

4.3 A Convenção de Budapeste

A convenção de Budapeste, também conhecida como Convenção sobre o cibercrime, consiste em um tratado internacional firmado para definir harmonicamente os crimes praticados no âmbito virtual e suas formas de persecução.

Elaborado na Europa, surgiu da necessidade de intensificar e unificar a cooperação internacional afim de aprimorar a capacidade de investigação dos crimes virtuais, garantido que toda violação e abuso referentes as tecnologias sejam penalizados. A princípio, a convenção prega a universalização e unificação de uma única legislação, para que houvesse maior cooperação entre os Estados da União, atualmente sendo facultativo a participação daqueles que desejarem.

No Brasil, a adesão a convenção ocorreu através de um Decreto Legislativo, no entanto, ainda necessita da promulgação presidencial para a sua efetiva publicação.

Dentre o conteúdo elencado na convenção de Budapeste, estão as normas para investigação e produção de provas eletrônicas e os meios de cooperação e criminalização de condutas.

Tendo em vista seu caráter fronteiriço, observa-se uma unificação para prevenção no que diz respeito ao enfrentamento da cibercriminalidade. Oportunizando ao Brasil a possibilidade de otimização das normas sobre crimes virtuais, seguindo os padrões internacionais.

Por fim, é importante ressaltar que uma vez aderido o tratado, é necessário que o Estado adeque suas normas a legislação nacional estipulada na convenção.

4.4 Lei nº 12.737/ 2012 (Lei Carolina Dieckmann)

No contexto jurídico, o campo de discussão a respeito dos crimes virtuais ainda é bastante recente, assim como as legislações para combaterem essas práticas delituosas são escassas, haja visto que os crimes virtuais podem alcançar patamares ainda mais sofisticados, chegando ao ponto de quebrar a segurança da própria rede de computadores, assim culminando em outros crimes, tais como: estupro virtual, pedofilia, sequestro, utilização de acesso a contas bancárias, estelionato, utilização indevida de dados e imagens, entre outros. A maior parte das vítimas nem ao menos sabem que estão tendo sua privacidade violada, a memória e internet invadidos, como foi o famoso caso popularmente conhecido no final do ano de 2012 da atriz Carolina Dieckmann que guardava em seu computador fotos íntimas e ao precisar reparar alguns danos na memória de seu dispositivo, teve 36 de suas imagens íntimas divulgadas nas redes sociais. Essas práticas criminosas confrontam os direitos básicos individuais: liberdade, à vida e ao patrimônio indiscutivelmente lesados.

Por se tratar de uma personalidade pública, no caso, a atriz Carolina Dieckmann, o crime virtual anteriormente mencionado, ganhou repercussão midiática que levou a aprovação imediata e em um curto intervalo de pouco mais de um mês da Lei nº 12.737, de 30 de novembro de 2012, lei esta que recebeu o nome da própria atriz, sancionada pela então Presidente Dilma Rousseff.

Antes do surgimento da Lei nº 12.737/12 não era possível identificar adequadamente as condutas criminosas. Esses delitos eram tipificados baseados nos crimes comuns existentes no Código Penal. No Brasil ainda não existia a definição específica de um

crime de invasão de sistemas ou dispositivos digitais. Existia somente vagas determinações sobre crimes cibernéticos, existia, também a possibilidade de crimes cometidos por funcionários públicos contra a própria administração pública e o reconhecimento de estelionatos e furtos por meios eletrônicos mediante a Lei de interceptações.

Compreende-se que o delito de invasão de dispositivo informático condiz, de acordo com a Lei nº 12.737/12 “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” (art. 154-A, caput, Lei nº 12.737).

Mesmo com as tentativas da lei de coibir esses tipos de crimes, desde de 2012 o contexto dos crimes cibernéticos no Brasil alterou-se significativamente, tanto no que diz respeito a qualidade, quanto a quantidade dos delitos. Cada vez mais, os criminosos vão se especializado para enganar suas vítimas, apostando principalmente nas falhas de segurança dos sistemas informáticos. Assim, ao que parece, para os criminosos, os crimes virtuais são mais seguros de se praticar do que os crimes comuns: a própria natureza dos crimes virtuais dificulta sua investigação pelos poderes legais.

Sabe-se que na prática, os crimes previstos no Código Penal, são aplicados por analogia quando praticados no ambiente virtual, mediante tecnologia. Contudo, algumas leis específicas, como é o caso da Lei Carolina Dieckmann, foram sancionadas a fim de combater, responsabilizar e punir de acordo com a legislação vigente.

Apesar de tudo, é importante mencionar que existe dificuldade no combate a invasões dos sistemas de computadores e celulares; motivos pelos quais demandam legislações específicas para combater tantos prejuízos que afetam violentamente pessoas em todas as camadas sociais, seja de ordem moral, ou financeira, são prejuízos imensos cometidos mediante os crimes virtuais.

A Lei Carolina Dieckmann foi sancionada com o objetivo de assegurar a privacidade de informações pessoais dos cidadãos no âmbito digital e virtual. Essa Lei acrescentou ao Código Penal, lei que tipifica os crimes em território brasileiro possíveis de punição, os artigos 154-A e 154-B, alterando as redações dos artigos 266 e 298, ambos do mesmo diploma legal.

O Artigo 154-A dispõe sobre a invasão de dispositivo:

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem

autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa (BRASIL,1940).

Por sua vez, o art. 154-B dispõe sobre o tipo da ação penal para tais crimes:

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos (BRASIL,1940).

A lei colocou no Código Penal o crime de invasão de dispositivo informático, que é aquele tipificado no art. 154-A acima destacado. Diz ainda que a conduta deve ensejar violação de um dispositivo, com intuito de adulterar, obter ou destruir dados sem autorização do titular ou proprietário do dispositivo.

Se enquadra neste tipo de ato criminosos a conduta compreendida em instalar vírus (provocando vulnerabilidades e deficiência) em sistemas informáticos para o fim de obter vantagens financeiras ilícitas. Ainda, a produção, oferecimento, distribuição, venda ou difusão de programa de computador ou de outro dispositivo também são condutas que se encaixam no crime tipificado no art. 154-A, do Código Penal, incluído pela Lei Carolina Dieckmann. A pena aplicável às condutas previstas no art. 154-A, do Código Penal, é de reclusão de 1 (um) a 4 (quatro) anos e multa.

Também, segundo o parágrafo 2º; “Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.

Nos parágrafos seguintes, há outras hipóteses de aumento de pena:

§ 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 2 (dois) a 5 (cinco) anos, e multa.

§ 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL,1940)

Contudo, para comprovar crimes enquadrados na Lei Carolina Dieckmann e provar a ocorrência dos crimes digitais, é indispensável reunir todas as provas que estiverem ao alcance da vítima para demonstrar que a mesma sofreu uma conduta criminosa. Tais provas podem ser elencadas em: mensagens de celular/WhatsApp; E-mails; comprovantes de pagamento; fotos; extratos de ligações; gravações e tudo o mais que possa ajudar a identificar o tipo de crime e seus infratores. Ou seja, tudo que demonstrar que ocorreu dano decorrente de uma conduta ilegal, deve ser utilizado.

E por fim, é indispensável salientar que os crimes praticados sejam denunciados, para que as penalizações sejam aplicadas quando for constatada a consumação da conduta criminosa.

5 CONCLUSÃO

Através do presente estudo foi possível entender que o avanço tecnológico foi essencial para todas as esferas da sociedade, possibilitando o desenvolvimento social, cultural e econômico da sociedade.

Observa-se que assim como a tecnologia está em constante evolução, o Direito deve se adaptar as mudanças ocorridas na sociedade, principalmente quando trata-se da Era Digital, onde tem se desencadeado diversos tipos de crimes sem que haja leis específicas para regulamentá-los.

Contudo, atrelado a mesma evolução, abriu portas para que as pessoas más intencionadas usem destes recursos para ludibriar pessoas, e causarem diversos danos a população.

Nos crimes praticados no ambiente virtual, há uma certa dificuldade para a tipificação, sendo um obstáculo na maioria das vezes tendo em vista que a legislação penal atual aborda condutas muito específicas para a punição de tais delitos.

Dessa forma, compreende-se que já existem normas que amparam os crimes cometidos na internet, porém tais leis não possuem uma eficácia quanto a sua tipificação. Sendo assim a criação de uma legislação mais específica para tais crimes, com sanções mais rígidas, afastaria a ideia de impunidade nas quais se tem nos dias atuais, nas quais as pessoas cometem crimes e não possuem a devida punição.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal.

_____. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

_____. **Decreto - lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Rio de Janeiro, 7 de dezembro de 1940; 119º da Independência e 52º da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 10/10/2022

_____. **Lei 12.735 de 30 de novembro de 2012**. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: outubro de 2022.

_____. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Brasília, 27 de maio de 2021; 200º da Independência e 133º da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 10/10/2022

_____. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet, lei nº 12.965, de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 10/10/2022.

GRECO, Rogério. **Curso de direito penal**: volume 2: parte especial: artigos 121 a 212 do código penal / Rogério Greco. – 19. ed. – Barueri [SP]: Atlas, 2022.

JESUS, Damásio de Marco Civil da Internet :**comentários à Lei n. 12.965, de 23 de abril de 2014** / Damásio de Jesus, José Antonio Milagre. – São Paulo: Saraiva, 2014.

_____. Damásio de. **Manual de crimes informáticos** / Damásio de Jesus, José Antonio Milagre. – São Paulo: Saraiva, 2016.

LIMA, Paulo Ferreira. **Crimes de Computador e Segurança Computacional**. Campinas: Millennium, 2006.

MARCO Civil da Internet / **George Salomão Leite, Ronaldo Lemos** (coordenadores). – São Paulo: Atlas, 2014.

NUCCI, Guilherme de Souza. **Manual do Direito Penal**. 7. ed. São Paulo: Revista dos Tribunais, 2011

PRADO, L. R. **Curso de direito penal Brasileiro**: volume II, parte especial, 7 ed., 2008.

SILVA, José Afonso da. **Curso de Direito Constitucional** Positivo. 30^a ed. São Paulo: Malheiros, 2008, p. 209.

SYDOW, Spencer Toth **Curso de Direito Penal Informático** / Spencer Toth Sydow – 3.ed.rev. e atual. – Salvador: Editora JusPodivm, 2022. 864p.

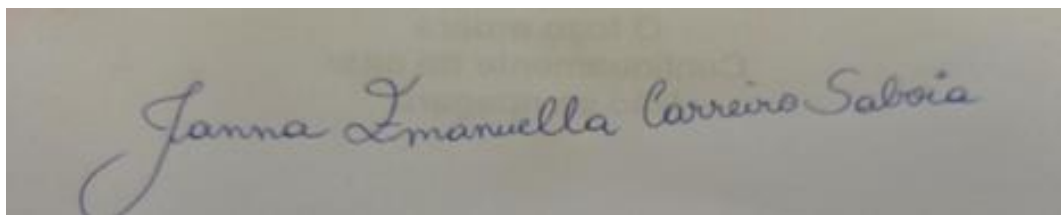
VIANNA, Tulio. **Crimes informáticos**/ Tulio Vianna; Felipe Machado- Belo Horizonte: Fórum, 2013. 112p.

DECLARAÇÃO DE REVISÃO ORTOGRÁFICA

Eu, Janna Emanuella Carreiro Saboia, graduado (a) em Letras pela Universidade Estadual do Maranhão (UEMA), declaro para o Centro Universitário – UNINOVAFAPI que revisei o Trabalho de Conclusão de Curso de Bacharelado Direito intitulado: **A (in)suficiência legislativa na punição dos crimes virtuais.** Das alunas **MARIA EMANUELLE DOS SANTOS RODRIGUES E MICHELE CARVALHO SILVA.**

Declaro ainda que o presente trabalho se encontra de acordo com as normas ortográficas e gramaticais vigentes.

Teresina, 28 de Novembro de 2022.

A photograph of a handwritten signature in blue ink on a light-colored surface. The signature reads "Janna Emanuella Carreiro Saboia" in a cursive script.

JANNA EMANUELLA CARREIRO SABOIA – 009.555.353-36