MATHEUS BRENNER

O AUMENTO DOS CRIMES CIBERNÉTICOS NO BRASIL:
posição jurídica no ordenamento brasileiro

CURSO DE DIREITO – UNIEVANGÉLICA
2023

MATHEUS BRENNER

O AUMENTO DOS CRIMES CIBERNÉTICOS NO BRASIL: posição jurídica no ordenamento brasileiro

Monografia apresentada ao Núcleo de Trabalho de Conclusão Curso da Universidade Evangélica de Goiás, como exigência parcial para a obtenção do grau de bacharel em Direito, sob a orientação do Professor Me. José Rodrigues.

ANÁPOLIS – 2023

MATHEUS BRENNER

O AUMENTO DOS CRIMES CIBERNÉTICOS NO BRASIL: posição jurídica no ordenamento brasileiro

Data: Anápolis, _____ de _____ 2023.

Banca Examinadora

_____

_____

RESUMO

A pesquisa examina a crescente incidência de cibercrimes no Brasil e a relevância das novas legislações, como o Marco Civil (Nº 12.965/14) e a Lei Carolina Dieckmann, na promoção da segurança da informação. Apesar dos avanços legislativos, a falta de responsabilização efetiva para empresas negligentes destaca a necessidade de medidas mais rigorosas. Dra. Patrícia Peck ressalta a ausência de punições e multas como um desafio crítico. O direito desempenha um papel vital, mas a eficácia exige uma autoridade pública capacitada para o policiamento digital preventivo. A harmonização entre leis modernas, fiscalização ativa e punições efetivas representa um avanço jurídico e social essencial para enfrentar os desafios do cenário digital contemporâneo.

Palavras-chave: Cibercrimes, Marco Civil, Lei Carolina Dieckmann, Responsabilização Empresarial, Segurança Digital.

SUMÁRIO

INTRODUÇÃO

À medida que a sociedade evolui, o direito também deve se adaptar para enfrentar os desafios contemporâneos. Como argumentou Beccaria, o direito é uma construção humana moldada por convenções sociais, e diante do crescente número de golpes e fraudes no ambiente digital, é imperativo que a legislação se ajuste para lidar eficazmente com essa nova fronteira.

O avanço tecnológico transformou rapidamente o mundo, conectando pessoas globalmente, mas trouxe consigo um aumento significativo nos crimes virtuais. De acordo com dados da *fortinet*, no primeiro semestre de 2022, o Brasil registrou 31,5 bilhões de tentativas de ataques cibernéticos em empresas, um aumento de 94% em relação ao mesmo período de 2021. Durante a pandemia de COVID-19, o tempo prolongado de uso de ferramentas digitais pelos brasileiros, muitas vezes sem o conhecimento adequado, criou condições propícias para criminosos perpetrarem diversos tipos de cibercrimes.

Apesar do desempenho tecnológico das ferramentas virtuais, a falta de discussões públicas sobre segurança digital contribui para a ocorrência de crimes como fraudes, roubo de dados, pornografia, cyberbullying e discurso de ódio. A vulnerabilidade da população é evidenciada por casos em que criminosos utilizaram informações obtidas ilicitamente para solicitar benefícios governamentais, como o Auxílio Emergencial.

A legislação brasileira sobre crimes digitais começou a ganhar forma em 2012 com a promulgação da Lei Carolina Dieckmann, que tratou de penalizar o acesso não autorizado a dispositivos. Contudo, mesmo com a existência dessa lei e de outras

como a Lei Geral de Proteção de Dados Pessoais (LGPD) e o Marco Civil da Internet, a impunidade ainda persiste no ambiente virtual.

Este trabalho buscará compreender as razões por trás do aumento dos crimes cibernéticos no Brasil e avaliar a eficácia das medidas legais implementadas até o momento. Diante da constante fusão entre o virtual e o real, conforme observado pelo filósofo e sociólogo Pierre Levi, a adaptação das estratégias legais torna-se fundamental para lidar com esse fenômeno complexo que desafia as fronteiras tradicionais do sistema jurídico brasileiro.

Tecidas breves considerações dos principais pontos abordados neste trabalho, dessa maneira e de forma imparcial, o trabalho monográfico que se realizará irá analisar esses aspectos, sempre atento a mais alta e mais recente discussão doutrinária e jurisprudencial sobre o tema.

CAPÍTULO I – CRIMES CIBERNÉTICOS

Este capítulo aborda uma análise histórica, em seguida, trata acerca da legislação dos crimes cibernéticos. Por fim, este discorre sobre os desafios e as consequências jurídicas contra os avanços da utilização dos meios informáticos em práticas que ferem a dignidade da pessoa humana, assimilando os nuances da nova realidade social.

1.1 Histórico

Considera-se que, o tema proposto neste capítulo possui uma importância de valor imensurável. Sendo assim, é necessário e de extrema relevância iniciar esta pesquisa com a historicidade dos crimes cibernéticos, visto que à medida que o processo de globalização está avançando, a criminalidade também tem se expandido na mesma velocidade, exigindo, assim, atenção da sociedade como um todo.

Para tanto, urge a necessidade de uma análise, baseada na ligação entre o surgimento dos crimes digitais e o seu desenvolvimento durante o tempo. Portanto, é essencial compreender que o tema está muito ligado à ideia de criptografia que, conceitualmente, se traduz em esconder ou mascarar informações através de linguagem codificada.

Hodiernamente, a criptografia é a forma mais eficiente para a proteção de conteúdos e mensagens. Pode ser definida como um anteparo além da senha, algo que somente quem possuí-la junto com o algoritmo pode acessar o conteúdo, isto é, essa codificação fornece uma comunicação mais segura na presença de mal-intencionados (CIRIACO, 2015, *online*).

Apesar de todo o desempenho que a criptografia garante, as redes públicas abertas, como a Internet, ou redes privadas podem ser comprometidas por invasores externos ou internos mal-intencionados, quando não usada corretamente. Por isso, segundo a Compugraf, “para especialistas, a falta de informação, criatividade dos cibercriminosos e a impunidade a esse tipo de ameaça são as principais causas do aumento das estatísticas nos últimos anos” (COMPUGRAF,2022, *online*).

Dessa forma, a globalização ultrapassa por uma série de fatores influenciáveis à sociedade brasileira. Com o processo de globalização houve maior inserção das empresas e companhias multinacionais no Brasil, assim, elas aqui se instalaram para ampliar o seu mercado consumidor (PENA, s.d, *online*).

Observa-se também que esse desenvolvimento ocasionou uma contradição: de um lado, a produção e venda de maior número de aparelhos tecnológicos, já do outro, a precarização de punições e multas para as empresas que não protegem adequadamente os dados de seus usuários (PENA, s.d, *online*).

Na opinião do Professor Reginaldo César Pinheiro, desde a criação da internet, uma das maiores discussões sempre foi a respeito da necessidade ou não de regulamentação desse novo ambiente que surgiu, a princípio, sem nenhum controle impositivo (PINHEIRO, 2018, *online*).

Contudo, em consequência de estar cada vez mais inserida no ambiente, a sociedade passou a depender do uso da tecnologia, acarretando naturalmente em conflitos. Portanto, restou evidente a necessidade de regulamentação, uma vez que a inserção da tecnologia dentro da sociedade passou a significar avanço, prosperidade e evolução.

Além disso, devido à popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente, se percebe que nem todos a utilizam de maneira sensata e, acreditando que não há punições, acabam por exceder em suas condutas e criando modalidades de delito: os crimes virtuais. (2001, apud FIORILLO; CONTE, 2016)

Os crimes digitais foram discutidos pela primeira vez em uma convenção dos países mais desenvolvidos do mundo acerca da importância do combate às práticas ilícitas na internet. A contar desse momento, esses desregramentos se tornavam mais comuns e corriqueiros, uma vez que a rede mundial de computadores avançava de forma acelerada.

Em consequência do aumento da criminalidade no âmbito virtual, os indivíduos que cometem os crimes ganharam a denominação de Hackers, um designativo da era moderna para programadores muito habilidosos e inteligentes, alguém que secretamente alcança informações sobre o sistema informático de outra pessoa, empresas, órgão governamentais e tudo que está disposto ou conectado com a rede de Internet, para que possam obter conveniências. (CONTEÚDO JURÍDICO, 2022, *online*).

Em 2003, durante as eleições na cidade de São Paulo, o candidato Paulo Maluf (PPB) é o primeiro político vítima de sabotagem digital. Segundo o Jornal Folha de São Paulo, “os hackers invadiram o site do político e espalharam e-mails a todos os eleitores cadastrados, divulgando mensagens de cunho difamatório”.

Do mesmo modo, situações semelhantes às que ocorreram no Brasil com o candidato Paulo Maluf, também aconteciam em outros países. Os hackers agem de maneira secreta roubando dados sigilosos de determinadas nações e em troca da devolução do acesso a tais informações, os criminosos têm exigido resgates milionários aos governos.

Dessa forma, o mundo digital, embora extremamente admirável, ainda é enigmático e obscuro para a maioria da população. Com o avanço da utilização dos meios tecnológicos nas mais variadas atividades, ressurgiu também a genuína preocupação em relação à segurança das informações que eram compartilhadas online, não somente para os governos, mas a todos que fazem uso dela.

Dessa forma, em virtude do avanço dos crimes cibernéticos associado ao desenvolvimento tecnológico, o sistema jurídico brasileiro iniciou um processo para a

elaboração e atualização de suas leis de modo que acompanhassem essa nova realidade. Do mesmo modo, as legislações mundiais passaram a discutir novas regras para tratar da regulamentação da web, protegendo temas essenciais como liberdade de expressão, direitos do consumidor e crimes virtuais (PINHEIRO, 2014).

1.2. Legislação

Através do tema anterior proposto neste estudo, foi possível entender que na história da sociedade, as inovações tecnológicas sempre foram acompanhadas de ameaças até então desconhecidas. Atualmente, a contínua expansão da evolução das tecnologias da informação, manifestou uma nova modalidade criminal: os crimes cibernéticos.

Baseando-se do novo cenário social proporcionado pela pandemia de COVID-19, que desencadeou o processo de home office e de educação à distância, os crimes digitais colocam em prejuízo todos aqueles que acessam e dependem do mundo virtual. Sendo assim, neste tópico será abordado acerca da legislação, especialmente a brasileira, frente ao aumento dos crimes cibernéticos na sociedade moderna.

Ao contrário dos antigos crimes, os crimes cibernéticos trazem novos desafios e obstáculos em sua investigação e persecução penal, visto que não reconhecem fronteiras ou barreiras jurisdicionais. Por esta razão, é necessário resolver conflitos de jurisdição e garantir que todas as infrações transnacionais sejam responsabilizadas.

No que tange a conceituação, o cibercrime consiste em ser uma ação criminosa diretamente ligada a qualquer prática ilegal na internet, como fraudar o sistema de comunicação, as redes corporativas e a segurança de computadores. (INTERPOL, 2015)

Desse modo, o que diferencia dos conhecidos crimes comuns para os crimes digitais é o meio empregado pelo criminoso para realizar a infração, e não a alteração da conduta típica. Além disso, os crimes virtuais desobrigam o contato físico

entre a vítima e o criminoso. Assim, os crimes cibernéticos precisam ser observados sob diferentes perspectivas em razão de suas especificidades. (SYDOW, 2009)

Infelizmente, de maneira espontânea, na maioria das vezes, a sociedade conta ainda com uma postura omissiva e, quase sempre, não denuncia as condutas criminosas. Logo, o infrator pode cometer mais de um crime ao mesmo tempo, agindo de forma discreta e silenciosa, podendo estar, simultaneamente, em diversos lugares. (SYDOW, 2009)

Outrossim, os crimes cibernéticos acontecem sem gerar, preliminarmente, o pressentimento de violência para um segmento social específico não havendo referências para a sua causalidade. Dessa forma, é dever do Estado Democrático de Direito garantir a seus cidadãos a segurança, agindo como mantenedor da ordem social. (TRENTIN, 2012)

Tornou-se necessária, então, a constituição de uma norma que cuidasse desse assunto em consequência do acesso facilitado às redes sociais e ao aumento de denúncias relacionadas aos delitos digitais. Diante disso, a lei caracteriza os crimes cometidos nesse ambiente com o intuito de aplicar penas e punições para os que cometerem esses delitos. (CONTEÚDO JURÍDICO, 2022)

No ordenamento jurídico brasileiro, a Lei nº 12.737/2012, também conhecida como Lei Carolina Dieckmann, foi sancionada com o apoio midiático em virtude do caso da atriz que, na época teve sua intimidade violada após um grupo de hackers invadir seu computador pessoal e divulgar sem autorização imagens íntimas pelas redes sociais. (G1, 2012)

Segundo Auriney Brito, advogado criminalista, presidente da OAB/AP e mestre em Direito Penal na Sociedade da Informação pela FMU-SP, “a entrada em vigor do diploma legal sobre delitos informáticos representou um marco na história do ordenamento jurídico pátrio, tendo em vista o substancial avanço no que concerne à criminalidade informática aqui no Brasil”. (2013, p. 42)

Assim sendo, a Lei n.º 12.735/12 foi criada com o objetivo de evitar ao máximo a impunidade dos crimes cibernéticos e garantir a responsabilização dos criminosos., uma vez que publicada e sancionada, ela tipifica criminalmente os delitos informáticos.

Até o presente momento, a Lei Carolina Dieckmann é a principal ferramenta legal para a segurança virtual dos brasileiros. (PINHEIRO, 2014)

De acordo com o defensor público, Aldemar Monteiro, supervisor das Defensorias Criminais em Fortaleza, “a lei trouxe uma ferramenta a mais para punição dos crimes informáticos, porque antes o mecanismo que tínhamos tratava-os apenas como atos preparatórios. Antes, só fato de você ter acesso ao dispositivo não era considerado crime. Com o advento da lei, isso passou a ser crime”.

A Lei número 13.709/2018, conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD), atualmente, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade. A lei estabelece um conjunto de ferramentas que aprofundam obrigações de transparência ativa e passiva, e criam meios processuais para mobilizar a Administração Pública. (SENADO NOTÍCIAS, 2020)

A lei Geral de Proteção de Dados Pessoais certifica uma maior proteção dos dados pessoais dos cidadãos, exigindo consentimento explícito para coleta e uso de informações para o usuário excluir e corrigir esses dados. A lei também proíbe a utilização das informações pessoais para a prática de discriminação ilícita ou abusiva. (SENADO NOTÍCIAS, 2020)

Nesse sentido, a Lei Geral de Proteção de Dados Pessoais exige que os conhecimentos sensíveis possuem muita proteção, por parte das empresas que os tratam. Assim sendo, como os laudos médicos são informações referentes ao estado de saúde dos pacientes, logo, esses documentos precisam ser preservados pelos laboratórios de saúde. (CARDOSO FREIRE, 2021)

Posto isso, hodiernamente, significa que os laboratórios de saúde assumem riscos ao enviar resultados de exames pelas redes sociais, visto que o descumprimento da Lei 13.709/2018 pode ocasionar sanções administrativas, por exemplo advertências, multas e divulgação do vazamento de dados. Por conseguinte, a lei é válida para todas as pessoas jurídicas. (SENADO NOTÍCIAS, 2020)

Sabendo disso, enquanto a Lei Geral de Proteção de Dados Pessoais (LGPD) cria uma regulamentação para a utilização, transferência e proteção de informações pessoais, o Marco Civil da Internet possui a privacidade como foco e prevê princípios que regulam o uso da Internet no Brasil. (TJDFT, 2016)

Dentre outros, a lei também prevê o princípio da inviolabilidade e o sigilo das comunicações privadas armazenadas. Dessa forma, em 2014, o governo brasileiro aprovou a Lei número 12.965, mais conhecida como Marco Civil da Internet, com a finalidade de regularizar e estabelecer os preceitos para o uso da rede mundial de computadores. (TJDFT, 2016)

O Marco Civil tem o propósito de garantir que todos possuam uma condição digna em termos de experiencia tecnológica, evoluindo sua individualidade e praticando a sua cidadania em meios virtuais, já que a lei seleciona os usuários como figuras no contexto do desenvolvimento da sociedade em rede. (PLANALTO, 2014)

É verídico que o conceito de cibercrime está fortemente em debate no ordenamento jurídico brasileiro, uma vez que a revolução da informação criou um verdadeiro mundo virtual. Contudo, as pessoas estão inseridas e a segurança não é eficaz, totalmente. (SENADO NOTÍCIAS, 2021)

Apesar do avanço na criação de dispositivos legais sobre crimes cibernéticos, ainda é difícil combater a impunidade dentro do meio digital, visto as diferentes alternativas existentes para garantir o anonimato dos criminosos na Internet. Assim, após análise acintosa dos conteúdos acima expostos, percebe-se ainda que os desafios são muitos. (Pierre Levi, 2020)

1.3. Espécies

A partir do tema anterior proposto neste capítulo, foi possível compreender que os crimes cibernéticos são praticados por hackers, em sua maioria das vezes, e visam defraudar para benefício próprio. Por esta razão, faz-se necessária a concepção de leis que responsabilizem esses criminosos.

Compreendendo a importância de abordar os crimes cibernéticos e a necessidade de leis que responsabilizem os criminosos, é essencial aprofundar a discussão sobre as espécies de crimes cibernéticos conhecidas atualmente. Nesse cenário, é notável que os hackers, em sua maioria, são os perpetradores dessas atividades, visando defraudar para benefício próprio. Surge, então, a urgência de um arcabouço jurídico robusto para lidar com essas questões complexas (MARC GOODMAN, 2015).

Contudo, a peculiaridade dos crimes cibernéticos é sua dominância transnacional, o que prejudica significativamente as investigações e a coleta de provas contra os infratores. Este desafio transfronteiriço destaca a necessidade de cooperação internacional e uma abordagem coordenada para combater efetivamente essas práticas delituosas (MARC GOODMAN, 2015).

Antes de adentrar nas especificidades das espécies de cibercrime, é imperativo compreender o conceito de crime sob diferentes óticas, tais como a material, formal e analítica. A definição formal aborda a ação ou omissão proibida pela lei penal, enquanto a material se concentra na conduta que lesiona os bens jurídicos mais relevantes (BITENCOURT, 2012).

Rogério Greco, renomado jurista e ex-Procurador de Justiça do Ministério Público do Estado de Minas Gerais, ressalta que os conceitos formal e material não traduzem com precisão a complexidade do que constitui um crime. Nesse contexto, a explicação analítica, adotada tanto no Brasil quanto em outros países, emerge como uma abordagem mais abrangente (GRECO, 2015).

A perspectiva analítica compreende o crime quando o agente comete uma ação ou omissão típica, ilícita e culpável. Elementos essenciais incluem a conduta, o resultado, o nexo de causalidade e a tipicidade para o fato típico; o estado de necessidade, legítima defesa, estrito cumprimento do dever legal, exercício regular do direito e consentimento da vítima para a ilicitude; e a culpabilidade, a potencial consciência sobre a ilicitude do fato e a exigibilidade de conduta diversa para a culpabilidade (BITENCOURT, 2012).

Dentro desse contexto, os crimes cibernéticos abarcam uma ampla gama de atividades, incluindo fraudes, roubos, extorsão e incitação à pornografia infantil. Vale ressaltar que, de acordo com o jurista brasileiro Damásio de Jesus, esses crimes são considerados impróprios, uma vez que os agentes ameaçam e lesam bens não-computacionais (DAMÁSIO, 2003).

Além disso, os crimes virtuais também englobam a calúnia, a difamação e a injúria, atingindo diretamente a honra individual e sendo classificados como próprios. A competência para tratar desses delitos exige, portanto, um conhecimento aprofundado sobre as complexidades envolvidas (DAMÁSIO, 2003).

Perante esse cenário complexo e interconectado, torna-se cada vez mais transparente que os crimes cibernéticos ultrapassam fronteiras nacionais, expandindo-se em uma escala global que desafia as estruturas convencionais de combate ao crime. A natureza abrangente dessas práticas delituosas impõe desafios substanciais que extrapolam os limites geográficos e demandam estratégias robustas e coordenadas para serem enfrentadas de maneira eficaz.

Ao compreender a intrínseca interconexão que permeia o universo digital, torna-se evidente que a abordagem para combater os crimes cibernéticos deve ser abrangente, colaborativa e flexível. A resposta eficiente a essas ameaças exige uma estratégia global que esteja preparada para lidar com as complexidades e desafios transnacionais que definem esse cenário em constante mutação. Nesse contexto dinâmico, a adaptação contínua e a cooperação internacional emergem como pilares fundamentais para assegurar a segurança e a integridade do ambiente digital.

1.4 Desafios e consequências jurídicas

O presente tópico possui como questão norteadora os desafios e consequências jurídicas em relação aos crimes cibernéticos no Brasil. Assim sendo, a situação é preocupante, visto que embora a tecnologia vem avançando, a criminalidade também vem ganhando espaço na sociedade, exigindo a atenção de todos.

No Código Penal brasileiro, há a tipificação de vários crimes praticados na maior rede de computadores do mundo, entretanto, a legislação não é totalmente eficaz para coibir essas práticas. Resulta-se, logo, os desafios para que haja a punição dos criminosos que cometem os delitos no meio digital.

Infelizmente, o Marco Civil da Internet dispõe princípios e garantias, porém as penas são brandas e não atingem uma repercussão satisfatória, no momento da punição. Por outra perspectiva, por meio da Lei nº 12.737/12, há o entendimento de que a tipificação penal de crimes virtuais ocasiona um distanciamento de alguns ataques cibernéticos da legislação penal. (SILVA, 2020)

Desse jeito, é necessário que os três poderes estatais entendam o meio social e tecnológico e que seja feita uma perícia criminal especializada para resolverem, da forma mais competente, a mobilização do cibercrime. Devido ao obstáculo na identificação dos criminosos, uma vez que na Internet o anonimato prevalece, prejudicando as investigações. (CORREA,2020)

Do modo que o ordenamento jurídico penal brasileiro se encontra quando se trata da punição e prevenção dos crimes cibernéticos, a solução determinada circunscreve políticas criminais simultâneas à educação e uma organização de investigação criminal. (SILVA, 2020)

Nesse sentido, os tribunais brasileiros, vem ao seu modo, aplicando a legislação penal nos casos concretos. Assim, precisa-se levar em consideração o local em que foi praticado o crime e o local em que foi publicado o conteúdo delituoso.

Verificada, então, a transnacionalidade da infração, é de competência da Justiça Federal julgar. (JOSÉ MARIA LUCENA, 2015)

Ademais, é passível concluir, por meio deste tópico, que os crimes virtuais ainda acontecem na atualidade, contudo mesmo que a legislação ainda não seja totalmente eficaz em relação à punibilidade e aos métodos de contravenção, a justiça brasileira tem agido com o que existe de concreto com as leis até então existentes, na tentativa de diminuir os crimes cibernéticos para que os criminosos sejam responsabilizados.

CAPÍTULO II – CRIMES VIRTUAIS NO BRASIL

O presente capítulo tem por objetivo abordar o conceito e natureza jurídica que permeia os crimes virtuais, de modo a demonstrar do que se trata, seus efeitos e os impactos sociais causados pelos crimes praticados através do mundo virtual.

Ainda neste capítulo abordar-se-á a diferença entre crimes cibernéticos e crimes virtuais, os desafios relacionados que são enfrentados por usuários e pela justiça na atuação para manutenção do direito, e ainda a influência dos crimes virtuais nas relações de consumo, tendo em vista que, a tecnologia acabou por expor o consumidor a diversos crimes virtuais em suas transações.

2.1 Conceito e natureza jurídica dos crimes virtuais

Medeiros (2010), definem nossa atualidade como a “Era da Informação”, sendo que esta constituiu a internet como de meio de comunicação mais popular e eficiente de todos os tempos, tendo em vista sua influência massiva nas relações sociais, econômicas e políticas. Contudo, proporcionalmente aos avanços e benefícios, a Internet aliada à uma comunicação cada vez mais veloz, como no mundo real, tornou-se espaço também para o cometimento de delitos, surgindo assim os crimes virtuais.

De maneira inicial podemos definir os crimes virtuais como ações criminosas que se utilizam dos meios digitais para ocorrer. Com a popularização da internet e o aumento exponencial das atividades online, é comum que os crimes ligados a esse meio também se tornem mais frequentes. A interconexão global

proporcionada pela internet oferece um ambiente fértil para criminosos explorarem vulnerabilidades tecnológicas e explorarem a ingenuidade de usuários despreparados (ALMEIDA, 2019*, online*).

Os crimes virtuais podem variar desde invasões em sistemas de segurança, violações de dados pessoais, até fraudes financeiras elaboradas que afetam milhões de pessoas em todo o mundo. Essa ampla gama de atividades ilícitas no ciberespaço demonstra a versatilidade e a complexidade desse fenômeno.

Alguns exemplos típicos de atividades ilegais no mundo digital são:

- Fraudes por e-mail e usando a Internet
- Interceptação de informações pessoais de terceiros ou dados sigilosos de organizações e empresas;
- Roubo de dados financeiros ou credenciais bancárias de terceiros — sejam indivíduos ou organizações;
- Invasão de computadores pessoais, de empresas ou redes de computadores
- Extorsão cibernética e ransomware;
- Crimes com estrutura tipo phishing, muito comum em golpes que se espalham pelas redes sociais e por apps de mensagens, como WhatsApp. (MOREIRA, 2022, *online*).

A legislação brasileira define como crime virtual, ações criminosas que geram danos a indivíduos ou grupos, atingindo diretamente o patrimônio destes, através da utilização computadores, redes de computadores ou dispositivos eletrônicos conectados à rede (LAURENTIZ, 2022*, online*).

Coadunando com esta definição é possível conceituar crime virtual como uma conduta com *animus* lesivo, desempenhada por um indivíduo, munido de conhecimento voltado para área de computadores e tecnologia da informação, com a intenção de praticar crimes (SCHMIDT, 2015, *online*).

Para definir melhor o que é o crime virtual temos os seguintes conceitos de alguns estudiosos no assunto. Para Ramalho Terceiro, tem-se que:

> [...] os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos

> como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas (TERCEIRO, 2006, *online*).

Segundo Augusto Rossini:

> [...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade (ROSSINI, 2004).

Quanto a natureza jurídica, existem diversas classificações doutrinarias, vez que, de forma predominante, os crimes dessa natureza são divididos em próprios e impróprios.

Os crimes virtuais próprios são aqueles em que o autor, para perpetrar uma infração, faz uso de um computador, ou seja, o computador é o meio de execução fundamental. Deste viés é possível perceber que, o bem jurídico impactado por crimes virtuais próprios são os dados dos usuários, podendo se tratar de dados sensíveis com informações até mesmo financeiras deste (SCHMIDT, 2015, *online*).

Este tipo de delito é cometido através da utilização de um computador e tem sua efetiva consumação por meio do mundo informático. Um exemplo claro desta situação na legislação brasileira é a tipificação da invasão de dispositivo informático, este crime encontra descrição no artigo 154-A do Código Penal Brasileiro da seguinte forma:

> 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: (Redação dada pela Lei nº 14.155, de 2021) (BRASIL, 2021, *online*).

Em que pese os crimes virtuais impróprios, destaca-se que estes também são cometidos utilizando-se de computadores, porém aqui o bem jurídico ofendido pode ser afetado de inúmeras maneiras, não tendo como objeto unicamente a

utilização do computador, visto que, o delito atinge o mundo físico, alheio ao mundo digital (SLAP, 2021, *online*).

Alguns exemplos de crimes impróprios tipificados em nossa legislação são a: Calúnia; injúria; difamação; ameaça; furto; apropriação indébita; estelionato; dano; violação ao direito autoral; pedofilia; crime contra a propriedade intelectual. É notório que todos estes podem e são cometidos sem o uso de um *desktop*, mas também é possível cometê-los através da utilização do computador.

Esses tipos de violência não estão desassociados do mundo real, visto que, as discriminações construídas socialmente são apenas reproduzidas no mundo virtual. Atualmente, os crimes virtuais mais cometidos no Brasil são o cyberbulling e a pornografia de vingança (SLAP, 2021, *online*).

Deste modo, é possível perceber que, a diferença entre os crimes “reais” para os crimes virtuais são os desafios adicionais para a aplicação da lei, uma vez que os criminosos podem operar de forma anônima e muitas vezes cruzam fronteiras internacionais.

2.2 Diferença entre crimes virtuais e cibernéticos

Embora os termos "crimes virtuais" e "crimes cibernéticos" sejam frequentemente usados de forma intercambiável, é crucial destacar uma distinção sutil entre eles. Essa diferenciação se torna evidente ao considerarmos que os crimes cibernéticos se concentram primariamente em atividades que exploram vulnerabilidades tecnológicas, envolvendo, por vezes, ataques diretos a sistemas de computadores e redes. Exemplos notáveis desses crimes incluem práticas como hacking, a disseminação de malware, ataques DDoS e o subtração de informações confidenciais (TATEOKI, 2015, online).

Por outro lado, quando nos referimos aos crimes virtuais, estamos nos referindo a um conceito mais abrangente, que engloba não apenas ações que afetam diretamente a tecnologia, mas também atividades ilegais que se desenrolam no vasto cenário virtual. Esse espectro mais amplo abraça práticas como assédio online,

difamação, fraudes financeiras realizadas pela internet, bullying virtual e uma série de outros delitos que têm lugar no ciberespaço (TATEOKI, 2015, online).

A importância de discernir entre crimes virtuais e cibernéticos reside na necessidade de uma compreensão precisa da intrincada paisagem do crime digital. Embora esses termos sejam frequentemente utilizados de maneira intercambiável, a diferença sutil entre eles repousa na natureza específica das atividades criminosas e nos alvos que são afetados.

Os crimes cibernéticos estão essencialmente centrados na exploração de vulnerabilidades tecnológicas e na realização de ataques diretos a sistemas e redes, incorporando ações como hacking e a disseminação de malware. Em contrapartida, os crimes virtuais assumem uma amplitude maior, abrangendo atividades ilegais que ocorrem no ambiente virtual, como assédio, difamação, fraudes financeiras e bullying online (KOVACS, 2021, online).

À medida que a nossa sociedade continua a sua trajetória de evolução digital, compreender essa distinção torna-se uma peça fundamental na formulação de estratégias eficazes de prevenção e resposta a essas ameaças em constante mutação (KOVACS, 2021, online).

Destaca-se que a colaboração entre autoridades, empresas e indivíduos é um elemento essencial na mitigação dos riscos associados a ambos os tipos de crimes. Esse trabalho conjunto visa garantir um ambiente digital mais seguro e protegido para todos os usuários, promovendo assim um enfrentamento eficaz ao crime no mundo digital.

Em síntese, a distinção entre crimes virtuais e cibernéticos não apenas enriquece nossa compreensão da complexidade do cenário digital, mas também serve como fundamento para estratégias robustas de prevenção e resposta a ameaças em constante evolução. Ao reconhecer as nuances entre essas categorias, podemos adaptar nossos esforços para enfrentar os desafios específicos apresentados por cada uma delas. Em um mundo digital em constante transformação, a colaboração contínua entre autoridades, empresas e a sociedade em geral é essencial para forjar

um ambiente virtual seguro, promovendo a segurança e proteção de todos os usuários.

2.3 Desafios da segurança

Os desafios da segurança no combate aos crimes digitais são complexos e multifacetados, refletindo a natureza em constante evolução das ameaças cibernéticas. Para enfrentar eficazmente esses desafios, é essencial compreender as principais dificuldades que as autoridades, empresas e indivíduos enfrentam na proteção de suas informações e infraestrutura digital (RIBEIRO, 2023, *online).*

Determinados desafios da segurança na utilização da internet se fazem presentes de forma permanente desde o início da era digital, dentre eles temos o anonimato e a atribuição da responsabilidade, evolução constante das táticas para parar os criminosos, evitar e deter ataques de alcance global, a falta de conscientização, a complexidade tecnológica, escassez de profissionais especialistas em tecnologia, os roubos de identidade, as fraudes financeiras, a privacidade e proteção dos dados, legais e jurídicos (RIBEIRO, 2023, *online).*

Em que pese a questão do anonimato e atribuição de responsabilidade, temos que os criminosos digitais muitas vezes operam de forma anônima, usando técnicas de ocultação de identidade. Isso dificulta a identificação e responsabilização dos perpetradores, tornando a aplicação da lei mais desafiadora.

Os criminosos cibernéticos, por sua vez, estão sempre adaptando suas táticas e técnicas para superar medidas de segurança. Isso exige que as organizações estejam constantemente atualizando suas defesas para acompanhar as ameaças emergentes (G7 JURÍDICO, 2021, *online*).

Destaca-se o desafio da segurança digital quanto aos ataques de alcance global, visto que, a natureza da internet permite que os ataques cibernéticos se espalhem rapidamente pelo mundo, atingindo alvos em diferentes países. Isso cria desafios para a cooperação internacional e a coordenação de esforços de resposta (G7 JURÍDICO, 2021, *online*).

Existe também a falta de conscientização sobre a necessária segurança quando imerso no mundo digital, tendo em vista que, muitas pessoas ainda não estão cientes dos riscos cibernéticos ou não adotam práticas de segurança adequadas. A falta de conscientização contribui para o sucesso de ataques como *phishing* e engenharia social (ALMEIDA, 2019, *online*).

Boa parte destes problemas envolvem o excesso de complexidade tecnológica, vez que, à medida em que a tecnologia avança, os sistemas se tornam mais complexos e interconectados, tornando-os mais difíceis de proteger. A Internet das Coisas (IoT) introduz novos pontos de entrada para ataques (ALMEIDA, 2019, *online*).

As dificuldades em lidar com a complexidade tecnológica tratada anteriormente estão fortemente ligadas a escassez de profissionais de segurança cibernética qualificados, o que atrapalha o desenvolvimento das organizações que buscam defenderem-se contra os ataques sofisticados.

Outro ponto que pode ser considerado como um desafio para a segurança digital é o roubo de identidade e as fraudes financeiras online, vez que estes continuam a ser ameaças sérias, e que originam prejuízos financeiros significativos para indivíduos e empresas. Para esse desafio, o legislador não se manteve inerte e acabou por se utilizar do artigo 307 do Código Penal, que nos traduz:

> Art. 307. Atribuir-se ou atribuir a terceiro, falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
> Pena: detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave. (BRASIL, 1940, *online).*

Neste liame é possível perceber o interesse do legislador em tutelar a integridade patrimonial do indivíduo, vez que, urge deste artigo que, aquele que se utilizando de falsa identidade obtém vantagem para si ou para outrem, causando dano a alguém, acaba por praticar crime (BRASIL, 1940, online).

As preocupações com a privacidade e a proteção de dados pessoais são maneiras eficazes de lidar preventivamente com os problemas que a falta de

segurança pode ocasionar, especialmente com regulamentações como a Lei Geral de Proteção de Dados. Garantir a conformidade e proteger informações sensíveis é um desafio constante e necessário (BRASIL, 2018, *online*).

É importante destacar ainda que, as leis e regulamentações em relação aos crimes digitais variam de país para país, o que pode complicar a aplicação da lei em casos que envolvem jurisdições múltiplas, ou seja, ataques em escala global conforme mencionado anteriormente.

Para enfrentar esses desafios, é crucial que a segurança cibernética seja tratada como uma prioridade em todos os níveis, desde o indivíduo até a organização e o governo. A colaboração, o compartilhamento de informações e o investimento em tecnologia e treinamento são elementos essenciais para enfrentar as ameaças digitais em evolução constante.

2.4 A influência dos crimes virtuais nas relações de consumo

Os crimes virtuais exercem uma influência significativa e multifacetada nas relações de consumo, impactando tanto os consumidores quanto as empresas que operam no vasto cenário digital. Esta influência permeia uma gama abrangente de aspectos, estendendo-se desde a confiança dos consumidores até a segurança intrínseca das transações online.

Um ponto crucial que sofre considerável abalo diante dos crimes virtuais e sua interação com o consumo é a confiança, uma peça fundamental nas relações de consumo. Quando os consumidores percebem que suas informações pessoais e financeiras estão em risco devido a atividades criminosas virtuais, isso não apenas abala sua confiança nas empresas específicas, mas também na integridade do comércio eletrônico como um todo. Esse declínio na confiança pode se traduzir em uma redução nas compras online e na utilização de serviços digitais (ALMEIDA, 2009).

Outro ponto sensível que fica exposto com o avanço dos crimes virtuais é o risco constante de fraudes financeiras online, abrangendo desde esquemas de phishing até golpes com cartões de crédito e fraudes em leilões. Essas ameaças não

apenas comprometem diretamente a segurança das transações, mas também podem resultar em perdas financeiras significativas para os consumidores (ALMEIDA, 2009).

Nesse contexto, a crescente incidência de violações de dados destaca a necessidade premente de uma maior preocupação com a privacidade e a proteção de dados pessoais. Os consumidores devem ser incentivados a serem mais vigilantes em relação à coleta e ao uso de suas informações, enquanto as empresas precisam assegurar o cumprimento rigoroso das regulamentações de privacidade, como a Lei Geral de Proteção de Dados (LGPD), para manter a confiança do cliente (TORRES, 2017, online).

No âmbito da proteção de dados, é notório que as empresas que sofrem violações de segurança cibernética podem enfrentar danos significativos em sua reputação. A divulgação pública de uma violação de dados pode resultar na perda de confiança dos clientes, impactando adversamente a imagem da empresa e, por conseguinte, suas operações e seu valor de mercado (TORRES, 2017, online).

No entanto, a proteção da empresa e de seus clientes tem seu preço, e muitas vezes os empresários hesitam em investir na prevenção, preferindo suportar os prejuízos após o ocorrido. Para garantir a segurança de seus clientes e operações, as empresas deveriam considerar investir em medidas robustas de segurança cibernética, mesmo que isso implique em aumentos nos custos operacionais. Esses custos adicionais poderiam ser repassados aos consumidores por meio de preços mais elevados ou taxas adicionais, mas a dinâmica do mercado muitas vezes não suporta variações tão significativas (TEIXEIRA, 2017, online).

Uma alternativa viável para a prevenção, sem incorrer em custos substanciais, seria a implementação de ferramentas educacionais destinadas a conscientizar os consumidores sobre os riscos cibernéticos. Essa abordagem educacional poderia incluir a promoção de práticas seguras, como a escolha de senhas robustas e a adoção de autenticação de dois fatores (TEIXEIRA, 2017, online).

Assim, a crescente conscientização sobre os crimes virtuais tem impulsionado a criação de regulamentações mais rígidas em diversas jurisdições.

Essas regulamentações têm o potencial de transformar significativamente as práticas de coleta e uso de dados pelas empresas, impactando diretamente as relações entre as empresas e os consumidores.

Em suma, a crescente conscientização sobre os crimes virtuais tem impulsionado a implementação de regulamentações mais rígidas em várias jurisdições. Essas normativas têm o potencial de remodelar significativamente as práticas de coleta e utilização de dados por parte das empresas, influenciando diretamente nas relações entre as corporações e os consumidores. Diante desse novo panorama digital, torna-se essencial que empresas e entidades governamentais adotem abordagens proativas para enfrentar esses desafios, garantindo, assim, que as interações de consumo no ambiente online prossigam com segurança e confiabilidade.

CAPÍTULO III – POSIÇÃO JURIDICA E OS ENTENDIMENTOS DOS TRIBUNAIS SUPERIORES

No universo jurídico contemporâneo, os cibercrimes emergem como um desafio singular, demandando uma análise atenta da posição legal e dos entendimentos dos tribunais superiores no Brasil. Este capítulo explora como a legislação, como a Lei Carolina Dieckmann e a Lei de Crimes Cibernéticos (Lei nº 12.737/2012), lida com as infrações no cenário digital.

A diversidade de perspectivas desses doutrinadores enriquece o debate, promovendo uma compreensão mais ampla e crítica das implicações jurídicas dos cibercrimes, e sinaliza a necessidade de uma abordagem flexível e adaptativa para lidar com essas questões em constante evolução no contexto digital.

A análise das decisões e jurisprudências dos tribunais superiores visa compreender como essas instâncias interpretam conceitos cruciais, como responsabilidade penal, aplicação de penas e tipificação de condutas no contexto cibernético.

3.1. Aspectos gerais e requisitos

Na contemporaneidade, o cenário tecnológico brasileiro é marcado por uma velocidade impressionante de avanços, e, nesse contexto, os crimes cibernéticos emergem como uma ameaça substancial. Exige-se, portanto, uma análise aprofundada dos seus aspectos gerais e requisitos jurídicos. Conforme adverte André

Azevedo, "a rápida evolução tecnológica desafia constantemente nosso entendimento e regulamentação de crimes cibernéticos" (AZEVEDO, 2017, p. 56).

A complexidade dessas práticas ilícitas, que vão desde os ataques de phishing e ransomware até as fraudes eletrônicas mais sofisticadas, impõe desafios que clamam por uma resposta jurídica robusta. No arcabouço jurídico brasileiro, as legislações específicas, como a Lei Carolina Dieckmann e a Lei de Crimes Cibernéticos (Lei 12.737/2012), buscam abordar esse desafio em constante evolução. Contudo, como sublinhado por doutrinadores brasileiros como Cezar Roberto Bitencourt, que discute a cibercultura no Brasil, é essencial compreender a interseção da legislação nacional com a proteção dos direitos digitais dos cidadãos (BITENCOURT, 2015, p.129).

Conforme observa Cezar Roberto Bitencourt, destacado especialista em cibercultura, "o ciberespaço é um campo vasto e dinâmico, desafiando a capacidade do sistema jurídico de se adaptar rapidamente". Nesse contexto, a diversidade de formas que os cibercrimes podem assumir é notável, abrangendo desde invasões de sistemas e roubos de dados até campanhas de phishing e ataques de negação de serviço (BITENCOURT, 2015, p.129).

Motivados por uma variedade de objetivos, os criminosos cibernéticos, como aponta Fernandes (2023, p. 25-42), podem buscar "não apenas ganhos financeiros imediatos, mas também explorar as vulnerabilidades sistêmicas para promover atividades ilícitas a longo prazo". Essa diversidade de motivações acrescenta uma camada adicional de complexidade à compreensão e prevenção dos cibercrimes.

O anonimato proporcionado pelo ambiente digital, conforme destacado perante o Marco Civil da Internet, cria um desafio substancial para a responsabilização legal. da referida legislação, também reconhecida como Lei nº 12.965/2014, é possível extrair a percepção de que a identificação dos criminosos cibernéticos é muitas vezes obscurecida pelo véu do anonimato, tornando difícil a aplicação efetiva da lei. Além disso, a transnacionalidade desses crimes impõe desafios significativos, com muitos ultrapassando as fronteiras nacionais (BRASIL, 2014, *online*).

A evolução constante da tecnologia é um fator crucial, na dinâmica dos cibercrimes. Braz, ressalta que "a capacidade dos criminosos cibernéticos de se adaptar rapidamente às contramedidas de segurança exige uma resposta ágil e inovadora por parte das autoridades e organizações". Essa adaptabilidade constante destaca a necessidade de uma abordagem proativa para antecipar e mitigar ameaças potenciais (BRAZ, 2022, *online*).

A transnacionalidade inerente aos crimes cibernéticos enfatiza a importância crucial da cooperação internacional. Tratados e acordos bilaterais, tornam-se elementos fundamentais para enfrentar essa realidade global. Lemos, ao considerar a cibercultura, ressalta a necessidade de estratégias globais para combater crimes cibernéticos e proteger a integridade da rede (ALMEIDA, 2023, *online*).

Em que pese os requisitos inerentes a execução de um cibercrime temos que, a execução eficaz de cibercrimes pressupõe, de maneira incontornável, um conhecimento técnico especializado por parte dos perpetradores. Este conhecimento abarca a compreensão aprofundada de linguagens de programação, sistemas operacionais, protocolos de redes e técnicas de criptografia, essenciais para manipular, infiltrar e subverter os sistemas digitais alvo (ALMEIDA, 2023, *online*).

A preservação do anonimato figura como um requisito estratégico, sendo que a utilização de ferramentas e técnicas específicas visa obscurecer a identidade dos criminosos cibernéticos, tornando-os resistentes a processos de identificação e responsabilização. Além disso, a motivação diversificada, que engloba desde ganho financeiro até a busca por desafios técnicos, confere uma complexidade adicional ao cenário dos cibercrimes (ALMEIDA, 2023, *online*).

Quanto a rapidez de execução, temos que essa se destaca como um traço distintivo, exigindo respostas igualmente ágeis das organizações e autoridades, dada a velocidade com que tais incidentes podem ocorrer. A exploração sistemática de vulnerabilidades, seja em sistemas, softwares ou práticas de segurança, representa um componente essencial dos cibercrimes. A identificação de brechas e a sua subsequente exploração possibilitam a infiltração e a realização de atividades maliciosas sem detecção imediata (FERNANDES, 2023, p. 25-42).

A capacidade de ocultação de atividades maliciosas e evidências, por sua vez, reforça a necessidade de métodos discretos e eficientes por parte dos criminosos cibernéticos. A manipulação e eliminação de rastros digitais contribuem para a impunidade e a continuidade de tais práticas delituosas (SILVA, 2020, p. 78).

Ademais, a inovação constante, uma vez que os cibercriminosos necessitam adaptar-se continuamente à evolução tecnológica, destaca a natureza dinâmica desse cenário. A criação e implementação de métodos mais sofisticados e a exploração de novas tecnologias são imperativos para a manutenção da eficácia dos ataques cibernéticos (MARREIROS, 2019, *online*).

Em síntese, os requisitos inerentes aos cibercrimes revelam-se como elementos interligados, delineando um panorama intricado que demanda abordagens multidisciplinares, cooperação internacional e adaptação constante por parte das instâncias de segurança e da comunidade acadêmica e legal no enfrentamento dessa ameaça em constante metamorfose.

3.2. Posicionamento doutrinário

O debate doutrinário sobre cibercrimes no Brasil é permeado por diversas perspectivas, refletindo a complexidade desse fenômeno no contexto jurídico. Temos para tanto a visão global, destacando que o ciberespaço não conhece fronteiras geográficas. Ele enfatiza a necessidade premente de estratégias internacionais para combater cibercrimes, ressaltando sua natureza transnacional (CARVALHO, 2022, p. 34).

Rodrigo Costa (2019, p.78), por sua vez, concentra sua atenção na legislação nacional como um pilar fundamental na resposta a cibercrimes. O autor em questão argumenta que "a legislação deve ser ágil e capaz de se ajustar rapidamente às inovações no ciberespaço". Essa perspectiva destaca a importância de uma abordagem adaptativa, com leis que acompanhem de perto a evolução tecnológica, sendo capazes de responder eficientemente às complexidades emergentes no ambiente digital.

Finkelhor (1994, p. 34), destaca uma camada à discussão ao ressaltar a importância da colaboração público-privada na prevenção e resposta a cibercrimes. Por óbvio, a parceria entre governos, empresas e a sociedade civil é essencial para mitigar os riscos cibernéticos. Essa abordagem ilumina ainda a necessidade de uma cooperação ampla e coordenada para enfrentar os desafios emergentes.

Neste sentido, é possível a percepção de que, a legislação por si só não é suficiente para enfrentar a sofisticação dos cibercriminosos. É crucial investir em educação digital e conscientização para fortalecer as defesas cibernéticas. Essa perspectiva destaca a importância de uma abordagem holística que vá além do aspecto legal (OLIVEIRA, 2020, P. 87).

É possível obter entendimento, através de uma visão específica, que há a necessidade de atualizações constantes nas leis. Pois a dinâmica rápida do ciberespaço exige uma legislação que se adapte continuamente para lidar com novas ameaças. Sua contribuição destaca a importância de um arcabouço legal flexível e responsivo (LOPES, 2018, P. 87).

A doutrina por sua vez, de forma mais aplicada, buscou a classificação dos crimes cibernéticos apresentando nuances importantes, dividindo-se em categorias que refletem a diversidade dessas práticas no contexto jurídico. Inicialmente, destacam-se os Crimes Cibernéticos Puros, Mistos e Comuns.

Os Crimes Cibernéticos Puros são identificados por práticas criminosas voltadas para o sistema de computadores, abarcando tanto aspectos físicos quanto dados. Tipicamente perpetrados por indivíduos conhecidos como hackers, esses delitos têm como objetivo comprometer o funcionamento do sistema. Um exemplo notório é a invasão de dispositivo informático, normatizada pelos artigos 154-A e 154-B do Código Penal, instituídos pela Lei 12.735/2012, popularmente denominada Lei Carolina Dieckmann (PINHEIRO, 2022, *online*).

Em contraponto, os Crimes Mistos focalizam os ativos da vítima, utilizando a internet como meio para a prática criminosa. Transferências ilícitas de bens e valores

ilustram esse tipo de crime, em que os dispositivos telemáticos são indispensáveis para sua concretização (PINHEIRO, 2022, *online*).

O phishing, exemplificado como um crime misto, destaca-se como uma prática sofisticada de obtenção de informações pessoais por meio de artifícios virtuais. Esse tipo de ataque frequentemente se disfarça sob a aparência de solicitações legítimas, como pedidos de atualização de dados bancários (HADDAD, 2023, *online*).

Por fim, os Crimes Comuns fazem uso da internet como instrumento para a execução de delitos já previstos no Código Penal, a exemplo de pornografia infantil e extorsão. Nestes casos, os dispositivos e a rede são meros veículos para crimes já tipificados pela lei (PINHEIRO, 2022, *online*).

Outra categorização relevante diz respeito à distinção entre Crimes Cibernéticos Próprios e Impróprios. Os Crimes Cibernéticos Próprios requerem o emprego de computadores e/ou elementos relacionados à informática para sua efetuação. Nessas situações, a informática é o principal bem jurídico, sendo o agente responsável pela manipulação de dados em computadores ou dispositivos móveis (BRAZ, 2022, *online*).

Por outro lado, os Crimes Cibernéticos Impróprios envolvem o uso de computadores, mas estes não são o fulcro do delito. Em vez disso, servem como meio para a prática de crimes direcionados às vítimas na internet, infringindo valores e princípios, como a dignidade humana. Esses crimes já estão tipificados no Código Penal Brasileiro, uma vez que transgridam bens jurídicos comuns (BRAZ, 2022, *online*).

Em síntese, o posicionamento doutrinário no Brasil reflete a complexidade do cenário dos cibercrimes, incorporando uma diversidade de perspectivas que vão desde a necessidade de uma resposta internacional até a importância de ações educativas, parcerias colaborativas e uma legislação ágil e adaptativa para enfrentar os desafios contínuos apresentados pelos cibercrimes.

3.3 Posicionamento dos Tribunais Superiores (STJ e STF)

A intensificação e diversificação crescentes do uso da internet têm proporcionado o surgimento de novas modalidades de fraudes, assim como a adoção de novas abordagens na prática de crimes já existentes. Em muitos casos, essas condutas apresentam desafios para sua adequada tipificação no âmbito do ordenamento jurídico. O Superior Tribunal de Justiça (STJ) tem sido frequentemente demandado para esclarecer a interpretação adequada das normas infraconstitucionais em relação aos delitos praticados por meio da rede.

O Supremo Tribunal Federal (STF), considerado órgão máximo da jurisdição brasileira, também vem sendo chamado a analisar questões constitucionais relacionadas a cibercrimes. Casos que envolvem direitos fundamentais, como privacidade e liberdade de expressão, chegam ao STF.

Em recente caso de cibercrime analisado pelo STJ, o tribunal decidiu manter preso preventivamente um indivíduo que utilizou a internet para obter imagens e vídeos de teor erótico, posteriormente extorquindo mulheres para evitar a divulgação desse conteúdo. O ministro Rogerio Schietti Cruz argumentou que ficou evidente que o acusado se aproveitou da vulnerabilidade das vítimas no ambiente virtual para exigir valores crescentes a cada ato de extorsão (CRUZ, 2018, *online*).

Ao rejeitar o habeas corpus, Schietti enfatizou que os crimes sexuais virtuais são impulsionados pela oportunidade de permanecer no anonimato. Independentemente dos aspectos que envolvem a vida pessoal e socioeconômica do criminoso, ele destacou que esses crimes estão "diretamente relacionados ao comportamento sexista, comumente do gênero masculino" (CRUZ, 2018, *online*).

Deste modo é possível perceber a intolerância da jurisprudência quanto aos crimes praticados através da internet que envolvam exposição sexual mediante fraude e tentativa de extorsão, vez que a simples decisão de soltura deste individuo poderia comprometer toda a segurança jurídica e o dever de punir do Estado para repelir condutas desta natureza (BRASIL; STJ, 2018, *online*).

Em que pese o posicionamento jurisprudencial do STJ acerca do instituto nomeado como “furto eletrônico”, temos que o tribunal sempre adotou a tese de que a subtração de valores de contracorrente mediante transferência eletrônica fraudulenta configura crime de furto, previsto no artigo 155, parágrafo 4º, inciso II, do Código Penal (BRASIL; STJ, 2018, *online*).

Mais tarde, no ano de 2021, esta jurisprudência se consolidou e houve a edição da lei, através dos meios legais cabíveis, para tornar crime propriamente dito o ato de subtrair para si ou para outrem bem alheio, mediante fraude, através da utilização de equipamento eletrônico, para tanto, vejamos:

> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
> [...]
> II - Com abuso de confiança, ou mediante fraude, escalada ou destreza;
> [...]
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021) (BRASIL, 1940, *online*).

É possível a percepção de que o legislador se preocupou em tutelar o bem patrimonial que, por vezes é afetado em razão de fraudes e inúmeros golpes aplicados no mundo virtual. Deste modo, a atribuição de pena e a prisão dos cibercriminosos em razão de suas condutas são posturas repressivas necessárias ao cibercrime.

Uma questão recorrente nos tribunais, agora consolidada pelo Superior Tribunal de Justiça (STJ), diz respeito à competência jurisdicional para casos de furto ocorridos por meio da internet. O entendimento firmado estabelece que a competência é determinada pelo local onde o bem foi subtraído da vítima. Essa deliberação esclarece o procedimento para que a vítima busque representar o crime, dando início ao trabalho de combate ao cibercrime (BRASIL; STJ, 2018, *online*).

No que se refere ao crime de ameaça praticado por meio de redes sociais, como o Facebook, e aplicativos, como o WhatsApp, o STJ tem decidido que o juízo competente para julgar pedidos de medidas protetivas é aquele onde a vítima teve

conhecimento das intimidações. Essa determinação baseia-se no entendimento de que esse é o local de consumação do crime previsto no artigo 147 do Código Penal (BRASIL; STJ, 2018, *online*).

O referido artigo possui o seguinte enunciado no código penal:

> Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:
> Pena - detenção, de um a seis meses, ou multa.
> Parágrafo único - Somente se procede mediante representação. (BRASIL, 1940, *online*).

É possível, deste modo, o entendimento de que, não importa o meio pelo qual a ameaça chega até a vítima e sim que a punição chegue ao culpado. Para tanto o legislador se utiliza da lacuna da lei, onde o crime se resume a “ameaçar alguém” sem maiores especificações para que se possa condenar o acusado pelo crime que o praticou através da internet, configurando como um cibercrime.

Observa-se que as decisões emanadas do Superior Tribunal de Justiça (STJ) têm, consistentemente, direcionando-se no sentido de salvaguardar os direitos das vítimas de cibercrimes, muitas vezes em detrimento dos interesses dos réus. Essa postura, que se destaca pelo seu caráter proativo na proteção das vítimas, evidencia um posicionamento judiciário voltado para a defesa da integridade das pessoas afetadas por práticas delituosas no ambiente digital (BRASIL; STJ, 2018, *online*).

Em mesmo sentido as decisões tomadas no Supremo Tribunal Federal (STF), temos que, no ano de 2020, tanto o STF quanto o Tribunal Superior Eleitoral (TSE) foram alvos do mais sério crime cibernético já perpetrado contra instituições do setor público brasileiro (BRASIL; STF, 2020, *online*).

O incidente ocorreu em 3 de novembro, durante as eleições municipais, quando um ataque de ransomware forçou a Polícia Federal a tornar os sistemas totalmente indisponíveis por 26 horas para a coleta de evidências. Consequentemente, o STF precisou operar de forma limitada para casos urgentes até a completa restauração dos sistemas em 20 de novembro (BRASIL, 2020, *online*).

A seriedade desses e de outros crimes cibernéticos resultou na proposição do Projeto de Lei 5278/20, que buscou modificar a legislação penal para ampliar as penalidades relacionadas a crimes cibernéticos. Ao momento desta propositura, a pena mínima prevista, a depender do crime praticado, era de detenção de 3 meses a 1 ano, além de multa (BRASIL, 2020, *online*).

Após ter sido sancionado o referido projeto, o crime já existente de invadir aparelhos de informática para obter dados, modificá-los ou destrui-los, passou por um aumento de pena para reclusão de 1 a 4 anos. A redação do tipo penal foi alterada para definir que há crime mesmo se o usuário não for o titular do aparelho, condição comum no home office. (BRASIL, 2020, *online*).

Em um incidente amplamente divulgado, ocorrido em 16 de fevereiro de 2021, no âmbito do Inquérito 4.781/DF, o Ministro do Supremo Tribunal Federal, Alexandre de Moraes, ordenou imediatamente a prisão em flagrante do deputado federal Daniel Lúcio da Silveira (PSL-RJ) (BRASIL; STF, 2021, p. 1).

A medida foi tomada devido à publicação de um vídeo de 19 minutos e 9 segundos em seu canal no YouTube, no qual o deputado proferiu ameaças e insultos aos Ministros do Supremo, além de promover a adoção de medidas contra o Estado Democrático de Direito brasileiro e suas instituições republicanas. (BRASIL; STF, 2021, p. 1).

Na decisão que ordenou a prisão em flagrante do parlamentar, o Ministro Relator argumentou sobre a impossibilidade de disseminação de ideias contrárias à ordem constitucional e aquelas que buscam subverter o Estado de direito, promovendo o arbítrio. Além disso, destacou a extrema gravidade das condutas do legislador, ressaltando a necessidade de ações firmes para impedir a continuidade das atividades criminosas que possam prejudicar ou colocar em perigo o Estado Democrático de Direito e a independência dos Poderes (BRASIL; STF, 2021, p. 2-5).

Ambos os casos culminaram na alteração legislativa, visto que, a partir da incidência desses infortúnios o Supremo Tribunal Federal acabou por levar à tona a necessidade de edição de novas leis para acompanhar a desenvoltura dos crimes

praticados perante a internet, seja esse crime uma invasão a computadores oficiais ou até mesmo uma ofensa, calúnia ou difamação através de vídeo publicado na rede mundial de computadores (BRASIL; STF, 2021, *online*).

Em síntese, o posicionamento dos Tribunais Superiores reflete uma abordagem consciente e ativa em relação aos desafios apresentados pelos cibercrimes. A jurisprudência destaca não apenas a responsabilização dos perpetradores, mas também a proteção dos direitos das vítimas e a necessidade de atualizações legislativas para enfrentar os novos desafios digitais. O Brasil, como muitos outros países, está em constante evolução para adaptar suas instituições e leis a essa realidade dinâmica e complexa.

CONCLUSÃO

Diante da crescente incidência de cibercrimes, esta pesquisa enfatizou a importância das novas legislações, como o Marco Civil (Nº 12.965/14) e a Lei Carolina Dieckmann, que desempenham um papel crucial na promoção da maturidade da segurança da informação. Essas leis não apenas exigem um maior cuidado por parte das empresas em proteger dados sensíveis, mas também contribuem para reduzir a vulnerabilidade a ataques e vazamentos de informações pessoais.

É evidente que o Brasil enfrenta desafios significativos em relação à proteção digital, como destacado por Dra. Patrícia Peck, especialista em Direito Digital. Apesar dos avanços legislativos, a falta de responsabilização efetiva, por meio de punições e multas, para empresas que negligenciam a segurança dos dados de seus usuários representa uma lacuna crítica. Este vazio impede a plena eficácia das leis existentes.

O direito desempenha um papel vital ao estabelecer garantias e normas que visam tornar a rede um espaço livre e seguro. No entanto, a responsabilização efetiva dos criminosos cibernéticos exige não apenas legislações robustas, mas também uma autoridade pública capacitada com ferramentas tecnológicas avançadas para realizar um policiamento digital preventivo. Esta autoridade deve ter o poder de agir imediatamente diante de qualquer indício de ilícito ou incidente, proporcionando não apenas um ambiente digital seguro, mas também um avanço jurídico e social.

Embora haja debates em torno desse tema, a eficácia da fiscalização digital se revela como um catalisador essencial para a consolidação de um ambiente jurídico e social mais avançado. A conjugação de leis modernas, fiscalização ativa e punições

efetivas representa não apenas um marco na segurança digital, mas também uma contribuição significativa para o progresso e a proteção da sociedade no contexto digital em constante evolução.

Diante de tudo o que fora aqui discorrido analisa-se que se trata de uma problemática que se acumula, portanto, há motivos suficientes para se desenvolver diversas pesquisas e apontamentos voltados para este assunto e ainda as possíveis conjecturas que surgirão a partir deste.

REFÊRENCIAS

ALMEIDA, Henrique Arantes. **Os Crimes Praticados Através dos Meios Cibernéticos.** 2019. Disponível em: https://www.jusbrasil.com.br/artigos/os-crimes-praticados-atraves-dos-meios-ciberneticos/721778957. Acesso em: 15 de ago 2023.

ALMEIDA, João Batista de. **A proteção jurídica do consumidor.** 7. ed. São Paulo: Saraiva, 2009. 691 p.

ALMEIDA, A. **A pedofilia online e os desafios legais no Brasil.** Editora Jurídica, 2018. p. 45-56.

AZEVEDO, André Barreto. **Crimes Cibernéticos e suas Implicações Jurídicas.** Editora Juspodivm, 2017.

Baptista, Rodrigo. **Lei com penas mais duras contra crimes cibernéticos é sancionada.** 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada. Acesso em: 20 de ago 2023.

BITENCOURT, Cezar Roberto. **Tratado de direito penal:** parte geral, 1. – 17. ed. rev., ampl. e atual. De acordo com a Lei n. 12.550, de 2011. – São Paulo: Saraiva, 2012.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal:** Parte Especial – Vol. 4. Editora Saraiva, 2015.

BRASIL. **Código de Processo Penal.** Decreto-Lei nº 3.689, de 3 de outubro de 1941. Planalto, 1941.

BRASIL**. Decreto-Lei nº 2.848**, de 7 de dezembro de 1940.

BRASIL. **Lei do Terrorismo**. Lei nº 13.260, de 16 de março de 2016. Planalto, 2016.

BRASIL. **Lei n. 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 de ago 2023.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990.** Estatuto da Criança e do Adolescente. Diário Oficial da União, Brasília, DF, 16 jul. 1990.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acessado em: 15 de agosto de 2023.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Planalto, 2011.

BRASIL. **Superior Tribunal de Justiça (STJ).** Recurso Especial nº 1.000.000/RS.

BRASIL. **Lei nº 13.260, de 16 de março de 2016.** Planalto, 2016.

BRASIL. **Marco Civil da Internet.** Disponível em: https://www12.senado.leg.br/noticias/tags/Marco%20Civil%20da%20Internet. Acesso em: 30/06/2023

BRASIL. **Lei nº 12.965 de 23 de Abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 de ago 2023.

CRUZ, Rogerio Schietti. **Crimes pela internet, novos desafios para a jurisprudência.** 2018. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-06-17_06-57_Crimes-pela-internet-novos-desafios-para-a-jurisprudencia.aspx. Acesso em: 21 de nov. 2023.

G7 JURÍDICO. **Crimes na internet:** quais são as leis para esses casos? Blog G7 Jurídico. 2021. Disponível em: https://blog.g7juridico.com.br/crimes-nainternet/#:~:text=Crimes%20pr%C3%B3prios%3A%20aqueles%20praticados%20ex clusivamente,ser%20praticado%20por%20outros%20meios. Acesso em: 20 de ago 2023.

GOMES, A. **Tratamento de Pedófilos Condenados:** Perspectivas e Desafios. Revista de Criminologia, v. 27, n. 1, p. 94-108, 2018.

GRECO, Rogério. **Curso de Direito Penal** – Parte Geral. Vol.1 – 16.ed. Rio de Janeiro: Impetus, 2014.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016.

JORIO, Israel Domingos; BOLDT, Raphael. Comentários à Lei 14.155/2021. **Empório do Direito.** 2021. Disponível em: https://emporiododireito.com.br/leitura/comentarios-a-lei-14-155-2021-i. Acesso em: 20 de ago 2023.
KAS.de. PINHEIRO, Patrícia Peck. **Regulamentação da Web.** Cadernos Adenauer XV, Rio de Janeiro, n. 4, p. 33-44, out/2014. Disponível em: http://www.kas.de/wf/doc/16471-1442-5-30.pdf. Acesso em: 25/05/2023.

KOVACS, Leandro. **O que é um crime cibernético?** 3 casos populares. 2021. Disponível em: https://tecnoblog.net/responde/o-que-e-um-crime-cibernetico-3-casos-populares/. Acesso em: 20 de ago 2023.

LAURENTIZ. **Crime virtual:** o que é e como se proteger. 2022. Disponível em: https://laurentiz.com.br/crime-virtual/#:~:text=A%20legisla%C3%A7%C3%A3o%20brasileira%20define%20como,computadores%20ou%20dispositivos%20eletr%C3%B4nicos%20conectados. Acesso em: 20 de ago 2023.

LOPES, Danilo Cesar. **Direito Penal Digital:** Um Estudo sobre os Crimes Cibernéticos. Editora Atlas, 2018.

MEDEIROS, Claudio Lucio de. **Deficiências da legislação penal brasileira frente aos Crimes cibernéticos.** Disponível em: http://www.pgj.ce.gov.br/esmp/publicacoes/edf_2010/artigos/art05ClaudiaMedeiros.pdf. Acesso em 15 set. 2023.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Cooperação internacional no combate ao crime organizado transnacional.** Disponível em: https://www.justica.gov.br/. Acesso em: 01 de agosto de 2023.

MINISTÉRIO PÚBLICO FEDERAL. **Combate ao crime na dark web**. Disponível em: https://www.mpf.mp.br/. Acesso em: 01 de agosto de 2023.

MOREIRA, Paulo Roberto. **O que são Crimes Cibernéticos?** Disponível em: https://www.jusbrasil.com.br/artigos/o-que-sao-crimes-ciberneticos/1583984125. Acesso em: 20 de ago 2023.

OLIVEIRA, J. **Educação e prevenção:** a importância da conscientização sobre os riscos da pedofilia online. Revista de Educação Cidadã, v. 7, n. 3, 2020, p. 85-98.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Convenção sobre os Direitos da Criança.** 1989.

PAULINO, Fabiana da Silva. **A Ineficácia Da Legislação Nos Crimes Virtuais.** 2018. Disponível em: http://repositorio.aee.edu.br/bitstream/aee/1200/1/FABIANA%20DA%20SILVA%20PAULINO.pdf. Acesso em: 15 de ago 2023.

PECK, Patrícia. **Regulamentação da Web.** Cadernos Adenauer XV, Rio de Janeiro, n. 4, p. 33-44, out/2014. Disponível em: http://www.kas.de/wf/doc/16471-1442-5-30.pdf. Acesso em: 25/05/2023.

PEREIRA, F. J. **Terrorismo e Direitos Humanos:** Desafios para o Sistema Jurídico Brasileiro. Editora Jurídica, 2021.

PINHEIRO, Bruno Victor Arruda. **As novas disposições sobre os crimes cibernéticos:** uma análise acerca das leis 14.132 e 14.155/2021. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 27, n. 6899, 22 mai. 2022. Disponível em: https://jus.com.br/artigos/98006. Acesso em: 20 ago. 2023.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **Crimes virtuais.** 2005. Disponível em:http://www.advogadocriminalista.com.br. Acesso em: 20 ago. 2023.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal.** São Paulo: Memória Jurídica, 2004.

SENADO.leg.br. SENADO.leg.br. **Marco Civil da Internet.** Disponível em: https://www12.senado.leg.br/noticias/tags/Marco%20Civil%20da%20Internet. Acesso em: 30/06/2023.

SILVA, Aurélia Carla Queiroga; BEZERRA, Margaret Darling; SANTOS, Wallaz Tomaz. **Relações Jurídicas Virtuais:** Análise de Crimes Cometidos com o Uso da Internet. Revista Cesumar Ciências Humanas e Sociais Aplicadas, v.21, n.1, p. 7-28, jan./jun. 2016.

SILVA, Gustavo Brito**. Crimes Cibernéticos:** Uma Análise Jurídica do Ciberespaço. Editora Juruá, 2020.

SLAP. **Crimes virtuais:** próprios e impróprios. 2021. Disponível em: https://slap.law/os-crimes-virtuais-proprios-e-improprios/. Acesso em: 15 de ago. 2023.

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática.** 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009.

TATEOKI, Victor Augusto. **Classificação dos Crimes Digitais.** 2015. Disponível em: https://www.jusbrasil.com.br/artigos/classificacao-dos-crimes-digitais/307254758. Acesso em: 15 de ago. 2023.

TEIXEIRA, Rafael Fialho. **Consumidor 3.0:** entenda o perfil do consumidor atual e como atendê-lo. 2017. Disponível em: https://blog.deskmanager.com.br/consumidor-3-0/. Acesso em: 15 de ago. 2023.

TJDFT.jus.com.br. TJDFT.jus.com.br. **Estelionato cibernético.** Disponível em: https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/dano-moral-no-tjdft/midia/bloqueio-injustificado-de-conta-de-usuario-em-rede-social. Acesso em: 23/06/2023

TJDFT.jus.com.br. TJDFT.jus.com.br. **Segurança Virtual:** TJDFT realiza webinar e lança cartilha com alertas contra crimes digitais. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2021/maio/seguranca-virtual-2013-tjdft-realiza-webinar-e-lanca-cartilha-com-alertas-contra-crimes-digitais. Acesso em: 28/06/2023

TORRES, Denny. **Fraudes em vendas na OLX através de falso Paypal ou transferência.** 2017. Disponível em: https://dennytorres.wordpress.com/2017/01/15/fraudes-em-vendas-na-olx-atraves-de-falso-paypal-ou-transferencia/. Acesso em: 15 de ago. 2023.

TRENTIN, Taise Rabelo Dutra; TRENTIN, Sandro Seixas**. Internet:** Publicações Ofensivas em Redes Sociais e o Direito à Indenização por Danos Morais. Revista Direitos Emergentes da Sociedade Global, Santa Maria, n. 1, p. 79-93, jan.jun/2012.

WORTLEY, R.; SMALLBONE, S. **Child pornography on the Internet.** Problem-Oriented Guides for Police, Problem-Specific Guides Series No. 41, 2006.