PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA JURÍDICA

OS IMPACTOS PSICOLÓGICOS, SOCIAIS E PENAIS NAS VÍTIMAS DE CRIMES CIBERNÉTICOS

ORIENTANDO: GUILHERME ARAÚJO SILVA

ORIENTADOR: PROF DRº GIL CÉSAR COSTA DE PAULA

GOIÂNIA

2025

GUILHERME ARAÚJO SILVA

OS IMPACTOS PSICOLÓGICOS, SOCIAIS E PENAIS NAS VÍTIMAS DE CRIMES CIBERNÉTICOS

Monografia Jurídica apresentado à Disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUC-GOIÁS).

Profa. Orientador Doutor Gil Cesár Costa de Paula.

GOIÂNIA

2025

GUILHERME ARAÚJO SILVA

OS IMPACTOS PSICOLÓGICOS, SOCIAIS E PENAIS NAS VÍTIMAS DE CRIMES CIBERNÉTICOS

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientador: Prof. Doutor Gil César Costa De Paula Nota

_____

Examinador (a) Convidado (a): Prof. (a): Mestre Paula Ramos Nora de Santis Nota

OS IMPACTOS PSICOLÓGICOS, SOCIAIS E PENAIS NAS VÍTIMAS DE CRIMES CIBERNÉTICOS

[1] Guilherme Araújo Silva

Os golpes cibernéticos geraram impactos sociais e psicológicos significativos nas vítimas, evidenciando a urgência de discutir a responsabilidade no âmbito do direito penal. O estudo analisou as consequências dessas fraudes, abordando o aumento da desconfiança, o isolamento social e os problemas de saúde mental, como a ansiedade e a depressão. A pesquisa enfatizou que as consequências foram além do dano financeiro, afetando a vida pessoal e as relações interpessoais dos indivíduos. Os resultados apontaram que a falta de apoio psicológico para as vítimas agravou a situação, tornando-as mais vulneráveis a novos ataques. Com isso, o tema levantou a necessidade de políticas públicas eficientes que incluíssem a conscientização sobre segurança cibernética e o suporte às vítimas. A conclusão reforçou que a responsabilização dos agressores foi fundamental para a dissuasão desses crimes, além de ter sido uma necessidade para a recuperação das vítimas e a restauração de sua confiança no ambiente digital. Essa responsabilidade precisou ser incluída nas legislações e práticas judiciárias, visando não apenas a punição dos infratores, mas também a proteção e o amparo aos afetados.

Palavras-chave: golpes cibernéticos; impactos sociais; saúde mental; responsabilidade penal; políticas públicas.

THE PSYCHOLOGICAL, SOCIAL AND CRIMINAL IMPACTS ON VICTIMS OF CYBERCRIMES

Cyber scams **caused** significant social and psychological impacts on victims, highlighting the urgency of discussing responsibility within the scope of criminal law. The study **analyzed** the consequences of these frauds, addressing increased distrust, social isolation, and mental health issues such as anxiety and depression. The research **emphasized** that the consequences **went** beyond financial loss, **affecting** victims' personal lives and interpersonal relationships. The results **pointed out** that the lack of psychological support for victims **worsened** the situation, making them more vulnerable to new attacks. Thus, the topic **raised** the need for effective public policies that **included** awareness of cybersecurity and support for victims. The conclusion **reinforced** that holding perpetrators accountable **was** essential to deterring such crimes and also **served** as a necessity for victims' recovery and the restoration of their trust in the digital environment. This responsibility **needed to be incorporated** into legislation and judicial practices, aiming not only at punishing offenders but also at protecting and supporting those affected.

Keywords: cyber scams, social impacts, mental health, criminal responsibility, public policies.

[1] Acadêmica de Direito Guilherme Araújo Silva, Pontíficia Universidade Católica de Goiás.

SUMÁRIO

INTRODUÇÃO

Os golpes cibernéticos têm se tornado uma realidade alarmante na sociedade contemporânea, trazendo consequências significativas para as vítimas, à medida que o mundo digital se expande, o número de fraudes e crimes cibernéticos cresce, resultando em impactos psicológicos e sociais profundos, este texto busca explorar como essas experiências afetam a vida das pessoas e qual o papel do Direito Penal na responsabilização dos criminosos, ao mesmo tempo em que promove a proteção das vítimas.

O principal objetivo deste estudo é analisar os efeitos que os golpes cibernéticos causam nas vítimas, enfatizando as dimensões psicológicas e sociais resultantes, buscando-se compreender como esses incidentes podem desencadear quadros de ansiedade, depressão, estigmatização e desconfiança, além de impactar a confiança interpessoal e o convívio social dos indivíduos afetados, a reflexão sobre esses aspectos é fundamental para o desenvolvimento de políticas públicas que atendam às necessidades dessas vítimas, oferecendo suporte e assistência adequados.

A metodologia utilizada na presente abordagem é de natureza dedutiva, partindo-se de premissas gerais sobre os efeitos dos crimes cibernéticos para, posteriormente, analisar os casos particulares e suas repercussões sociais e jurídicas, a pesquisa foi baseada em revisão bibliográfica, analisando artigos acadêmicos, relatórios institucionais e contribuições doutrinárias de autores como *Luciano Timm*, que discute a proteção jurídica dos consumidores em ambientes digitais, *Patrícia Peck Pinheiro*, referência em Direito Digital no Brasil, e *Silvio Meira*, especialista em segurança cibernética e transformação digital.

Entre os principais desafios enfrentados na análise do tema estão a subnotificação dos casos já que muitas vítimas não registram ocorrência por vergonha ou falta de conhecimento e a dificuldade de quantificar os danos psicológicos, que muitas vezes são invisibilizados pelo sistema de justiça, além disso, a legislação ainda se mostra, em certos aspectos, defasada frente à velocidade com que os crimes digitais evoluem, criando lacunas jurídicas e dificuldades na responsabilização efetiva dos autores.

A discussão sobre os impactos dos golpes cibernéticos é de suma importância, pois aborda questões de segurança e proteção dos cidadãos na era digital, cada vez mais, as vítimas são expostas a um ambiente nefasto, onde a desconfiança e o medo permeiam suas interações sociais, portanto, a conscientização sobre o problema fortalece a demanda por ações proativas por parte do Estado e da sociedade, visando à criação de um ambiente mais seguro e solidário.

Os impactos sociais das fraudes online são visíveis na erosão da confiança nas relações interpessoais e na deterioração do tecido social, quando um indivíduo se torna vítima de um golpe cibernético, é comum que ele passe a questionar sua capacidade de julgar as intenções das pessoas ao seu redor, isso pode resultar no isolamento social e na dificuldade em formar novas relações, afetando não apenas a vítima, mas também o seu círculo de convivência.

Os efeitos psicológicos dos golpes cibernéticos são igualmente preocupantes, a sensação de violação da privacidade, acompanhada da perda de bens e da insegurança constante, pode desencadear problemas de saúde mental, como estresse e depressão, muitas vítimas se sentem culpadas ou envergonhadas, o que pode levar à autocrítica negativa e sentimentos de inadequação, reorganizar e abordar essas questões é crucial para a recuperação e reintegração das vítimas na sociedade.

Nesse contexto, a responsabilidade do Direito Penal se torna essencial, o enquadramento legal dos crimes cibernéticos e a implementação de punições mais severas para os infratores são fundamentais para promover um ambiente de segurança digital, a responsabilização dos agentes que realizam esses crimes não apenas protege as vítimas, mas também envia uma mensagem de que a sociedade não tolera atos de fraude e violência online.

Além da punição dos infratores, é crucial que o sistema penal também considere medidas de apoio às vítimas, isso inclui a criação de mecanismos que possibilitem um atendimento psicológico adequado, bem como programas de reabilitação social que ajudem as pessoas a superarem os impactos decorrentes dos ataques que sofreram, o alinhamento entre a legislação e as necessidades sociais pode proporcionar um suporte emocional e psicológico que é, frequentemente, negligenciado.

Os impactos psicológicos e sociais dos golpes cibernéticos nas vítimas demandam uma atenção especial tanto da sociedade quanto do sistema jurídico, a

compreensão dos efeitos devastadores desses crimes é fundamental para a construção de políticas públicas eficazes que protejam os cidadãos e promovam a responsabilidade no âmbito do Direito Penal, proteger as vítimas e responsabilizar os autores dos crimes não é apenas uma questão de justiça, mas um imperativo ético e social para a construção de um futuro digital mais seguro.

1.HISTÓRICO SOBRE GOLPES CIBERNÉTICOS

Os golpes cibernéticos surgiram com o advento da Internet, tornando-se um fenômeno recorrente e crescente à medida que mais pessoas passaram a utilizar a rede mundial de computadores, desde os primórdios da era digital, criminosos têm explorado vulnerabilidades tecnológicas e a ingenuidade dos usuários para cometer fraudes e obter vantagens indevidas.

Rosa conceitua o que vem a ser um crime cibernético:

> É a conduta atente contra o Estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento rudimentar, o crime de Informática é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão. (ROSA, 2002, p. 53 – 54).

No início da década de 1990, com a popularização da Internet, os primeiros casos de fraudes online começaram a aparecer, os golpes digitais, que envolviam o envio de e-mails fraudulentos que simulavam empresas legítimas, tornaram-se uma das técnicas mais utilizadas por golpistas para roubar informações pessoais, essas mensagens enganadoras convidavam os destinatários a clicar em links maliciosos, levando a sites falsos projetados para coletar dados sensíveis.

Rosa explica ainda que:

> O crime de informática pressupõe dois elementos indissolúveis, contra os dados que estejam preparados as operações do computador e através do computador, utilizando-se de softwares e hardwares, para perpetrá-los, a expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamentos automático e a sua transmissão, ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele a privacidade, a honra, ao patrimônio público ou privado, a administração pública. (ROSA, 2002, p. 53 – 54).

Com o avanço da tecnologia, os golpes foram se refinando, nos anos 2000, os criminosos começaram a empregar malware, que são softwares maliciosos utilizados para infectar dispositivos, roubar informações e até mesmo controlar sistemas remotamente, essa nova abordagem ampliou o escopo dos golpes, permitindo ataques mais sofisticados e devastadores.

Para Silva, comenta a seguir:

> A internet é um campo extremamente abastecido de informações valiosíssimas e de imensurável valor, o que se torna altamente atraente a ataques e por ser um ambiente de fácil acesso, de inúmeras possibilidades e com muitos usuários que diariamente, utilizam a internet, não só para passar o tempo, mas sim, para o trabalho, atividades acadêmicas. (SILVA, 2021, p. 06).

Outro marco na história dos golpes cibernéticos foi o surgimento das redes sociais na década de 2010, as plataformas como Facebook e Twitter se tornaram alvos atraentes para golpistas, que utilizavam perfis falsos e anúncios enganadores para enganar usuários, os golpes de romance, onde pessoas se passam por pretendentes amorosos para explorar emocionalmente e financeiramente suas vítimas, ganharam destaque nesse período.

Adicionalmente, o aumento do comércio eletrônico trouxe novas oportunidades para fraudes, os golpes relacionados à compra e venda de produtos, como sites falsos que prometem mercadorias a preços irrealistas, tornaram-se comuns, esses esquemas lesavam consumidores que confiavam na reputação de plataformas digitais, sem saber que eram vítimas de fraudes elaboradas.

As consequências econômicas desses golpes não são negligenciáveis. Estima-se que os golpes cibernéticos custam bilhões de dólares em prejuízos anuais para indivíduos, empresas e governos ao redor do mundo, essa realidade impulsionou o desenvolvimento de tecnologias de segurança cibernética e maior conscientização sobre a importância de proteger informações pessoais e financeiras.

O lento processo de conscientização da população sobre a realidade dos golpes cibernéticos é um reflexo da falta de educação digital em muitos países, os usuários não têm conhecimento suficiente para identificar sinais de fraudes, o que os torna mais vulneráveis a ataques, sendo as iniciativas educacionais têm sido implementadas, buscando informar e capacitar os cidadãos a reconhecerem os diversos tipos de golpes.

A globalização e a natureza transnacional da Internet também dificultam o combate a essas fraudes, os criminosos operam a partir de diferentes países, tornando a responsabilização e a legislação uma tarefa desafiadora para as autoridades, a lacuna legal em muitos países permite que golpistas escapem de punição, o que estimula a continuidade dessas atividades ilícitas.

Nos últimos anos, os golpes cibernéticos evoluíram para incluir técnicas de engenharia social mais complexas, onde golpistas manipulam comportamentos humanos para obter resultados favoráveis, essa abordagem leva em conta a psicologia das vítimas, explorando medos, desejos e vulnerabilidades emocionais para conseguir enganar.

Ademais, o surgimento de novas tecnologias, como a inteligência artificial, tem gerado tanto oportunidades quanto desafios na luta contra os golpes cibernéticos, por um lado, ferramentas de IA podem ser utilizadas para detectar fraudes de maneira mais eficaz, por outro lado, golpistas também estão começando a usar IA para criar fraudes mais realistas e, portanto, mais difíceis de detectar.

De acordo com Silva, sobre o assunto:

> Com o aumento dos novos golpes, surge a necessidade de aplicação da legislação do ordenamento jurídico brasileiro que possa repreender de qualquer forma os crimes praticados no meio virtual, bem como intensificar as investigações e trazer punições mais duras que sejam capazes de intimidar os infratores e puni-los. (SILVA, 2021, p. 04).

As legislações em torno dos golpes cibernéticos têm avançado, mas ainda enfrentam muitos desafios, embora países em todo o mundo tenham começado a implementar leis mais rigorosas, a rápida evolução da tecnologia dificulta a manutenção de um marco legal atualizado e eficaz, isso tem gerado debates sobre a melhor forma de abordar a questão do crime cibernético no direito penal.

A resposta de instituições financeiras e empresas de tecnologia ao aumento de golpes cibernéticos tem sido significativa, as medidas como autenticação em duas etapas, alertas de segurança em tempo real e programas de compensação para vítimas são algumas das estratégias adotadas para reduzir o impacto das fraudes e proteger os usuários.

Além disso, a colaboração internacional entre governos, empresas e organizações não governamentais tem se mostrado essencial no combate a esses

crimes, as iniciativas conjuntas são essenciais para promover a troca de informações e melhorar as estratégias de detecção e prevenção de fraudes.

A história dos golpes cibernéticos é marcada por uma evolução constante em métodos e técnicas de engano, demonstrando a necessidade de adaptação contínua por parte das autoridades, empresas e usuários, enquanto a Internet continuar a ser um espaço de inovação e interconexão, os golpes cibernéticos provavelmente continuarão a representar uma ameaça significativa, a proteção contra essas fraudes não recai apenas sobre as instituições, mas também sobre os usuários, que precisam estar cientes dos riscos associados à navegação online.

A conscientização e a educação digital são fundamentais para capacitar os indivíduos a reconhecerem e evitar comportamentos que possam torná-los presas fáceis para golpistas, as campanhas de informação sobre segurança na Internet, junto a treinamentos específicos que ensinem sobre a identificação de fraudes, são passos essenciais para fortalecer a defesa contra esses tipos de crime.

O futuro dos golpes cibernéticos está interligado ao avanço da tecnologia e à preparação da sociedade para lidar com esses desafios, a colaboração entre variados setores, a inovação em segurança digital e a conscientização pública são pilares cruciais na construção de um ambiente digital mais seguro.

À medida que a sociedade avança no uso da tecnologia, a luta contra os golpes cibernéticos deve continuar a evoluir, para garantir que os benefícios da era digital possam ser experimentados por todos, sem o medo constante de serem vítimas de fraudes.

1.1 DEFINIÇÃO E TIPOS DE GOLPES CIBERNÉTICOS

Os golpes cibernéticos são ações fraudulentas realizadas por criminosos utilizando a tecnologia da informação e a Internet como meio principal de execução, o objetivo desses golpes é enganar as vítimas, levando-as a fornecer informações pessoais e financeiras, a realizar pagamentos indevidos ou a comprometer seus dispositivos de segurança, a natureza anônima e global da Internet propicia um ambiente fértil para esses crimes, tornando a detecção e a responsabilização extremamente desafiadoras.

Barbosa, explica que:

> O crime cibernético é uma prática que tem como alvo, ou faz uso do meio digital, como os computadores, celulares, e outros, para se concretizar, afeta qualquer pessoa, da criança ao idoso, qualquer ato para obter vantagens ilícitas, como, por exemplo, vantagens financeiras, praticado pelo meio digital, é um crime cibernético. (BARBOSA, 2022, p. 13).

Esses golpes podem assumir diversas formas e técnicas, muitas das quais evoluem a cada dia à medida que os criminosos se tornam mais sofisticados em suas abordagens, os golpistas exploram vulnerabilidades, tanto tecnológicas quanto comportamentais, para fazer com que as vítimas confiantemente revelem seus dados ou realizem ações que podem resultar em prejuízos financeiros e emocionais.

Pharmingé classifica com um tipo de ataque cibernético onde os criminosos redirecionam o tráfego de um site legítimo para um site falso, com o objetivo de roubar informações pessoais, como nomes de usuário, senhas e dados financeiros, esse ataque é uma combinação dos termos “phishing” e “farming”.

Conforme explicado por Silva:

> Por intermédio do Pharming, um site legítimo pode ser manipulado para direcionar usuários a outros sites, e que podem instalar softwares maliciosos nos computadores dos visitantes, sendo capaz ainda, de coletar dados pessoais tais como senhas ou informações financeiras. (SILVA, 2021, p. 09).

Um dos tipos mais conhecidos de golpe cibernético é o phishing, que envolve o envio de e-mails ou mensagens que aparentam ser de fontes confiáveis, como bancos ou empresas conhecidas, esses e-mails frequentemente contêm links que levam a páginas da web falsas, projetadas para coletar informações sensíveis, como senhas e números de cartão de crédito, o phishing é uma técnica que se aproveita da familiaridade dos usuários com as marcas conceituadas para induzi-los ao erro.

De acordo com Silva:

> O “Blind Phishing” acontece por disparos de e-mails em massa, onde os criminosos contam com a ingenuidade e desconhecimento de parte dos destinatários acerca desse tipo de golpe na internet, que geralmente, por exemplo, o e-mail ter algum link ou anexo tendencioso para que o receptor baixe um vírus em seu dispositivo”. (SILVA, 2021, p. 08).

Outro tipo comum de golpe é o "vishing", ou phishing por voz, nesse caso, os golpistas realizam chamadas telefônicas, muitas vezes se passando por representantes de empresas, instituições financeiras ou até mesmo órgãos

governamentais, o objetivo é persuadir a vítima a fornecer informações pessoais ou financeiras, utilizando táticas de pressão e manipulação.

Os golpes de "smishing", ou phishing por SMS, seguem uma linha semelhante ao phishing tradicional, mas utilizam mensagens de texto para enganar as vítimas, os golpistas enviam SMS que parecem legítimos, muitas vezes alegando que o destinatário ganhou um prêmio ou precisará confirmar informações de conta, o toque humano da comunicação via SMS torna esses golpes ainda mais impactantes e, em muitos casos, mais difíceis de detectar.

Silva explica sobre o Smishing ou Phishing: “Phishing realizado pelo envio de disparos de SMS para celulares, são geralmente são mensagens com informações de que a vítima está endividada ou ganhou um sorteio inesperado, fazendo com que a vítima tome decisões imediatas”. (SILVA, 2021, p. 08).

Os "ransomwares" são outra forma de golpe cibernético que tem ganhado notoriedade, nestes casos, o malware é instalado nos dispositivos da vítima, criptografando seus dados e exigindo um resgate para liberá-los, esse tipo de golpe é particularmente devastador, pois pode resultar na perda permanente de informações importantes e em prejuízos financeiros significativos.

Os golpes de "romance" emergiram com o aumento das plataformas de namoro online, os golpistas criam perfis falsos, muitas vezes utilizando fotos de pessoas atraentes e histórias emocionais para conquistar a confiança de suas vítimas, uma vez estabelecido um vínculo emocional, eles frequentemente manipulam a vítima para enviar dinheiro, alegando ter problemas financeiros ou emergências.

Os "golpes de advance-fee" são outro tipo comum, onde a vítima é convencida a pagar uma taxa adiantada para receber uma quantia posteriormente, esses golpes frequentemente envolvem promessas de heranças, prêmios ou investimentos, a lógica do golpe é simplesmente que a vítima nunca recebe a quantia prometida, enquanto os golpistas lucram com as taxas adiantadas.

Os "attaques de man-in-the-middle" representam uma técnica mais técnica, onde um golpista intercepta e manipula a comunicação entre duas partes, isso pode ocorrer em redes Wi-Fi públicas, onde as informações transmitidas podem ser

capturadas em tempo real, os golpistas podem usar esses dados para roubar informações sensíveis, como credenciais de login e dados bancários.

Os sites falsos também constituem uma forma de golpe cibernético, os golpistas criam páginas da web que se assemelham a sites legítimos, mas que são projetadas para coletar informações dos usuários, isso inclui lojas online fraudulentas que se assemelham a empresas conhecidas, levando os consumidores a fazerem compras que nunca serão entregues.

Os golpes de "cryptojacking" são outra manifestação moderna que se tornou comum na última década, esse tipo de golpe envolve a hijacking do poder de computação de um dispositivo para minerar criptomoedas sem o consentimento do proprietário, os usuários podem perceber que suas máquinas estão mais lentas ou aquecidas excessivamente, mas não têm ideia de que estão sendo usadas para atividades ilegais.

Os "golpes de sequestro de conta" acontecem quando um criminoso obtém acesso aos dados de login de uma conta online e, em seguida, assume o controle da conta da vítima, isso pode resultar em prejuízos financeiros, roubo de identidade e muitos outros problemas adicionais, este tipo de golpe destaca a importância de manter senhas seguras e usar autenticação em dois fatores.

Além disso, também existem ataques direcionados, conhecidos como "targeted phishing" ou "spear phishing", onde os golpistas direcionam suas táticas a indivíduos ou grupos específicos, esses ataques são mais elaborados e frequentemente se aproveitam de informações pessoais que os golpistas obtêm das redes sociais ou de outras fontes, como resultado, os e-mails ou mensagens criadas parecem quase reais, aumentando a probabilidade de que a vítima caia na armadilha.

Os golpes de "Bait and Switch" ocorrem quando os golpistas atraem as vítimas com uma oferta enganosa, como produtos a preços baixos, apenas para mudar os termos da negociação ou não entregar o produto após o pagamento, esse tipo de golpe explora a frustração dos consumidores em busca de boas ofertas, manipulando a psicologia do desejo por economizar.

O uso de aplicativos maliciosos também se tornou um método frequente para perpetrar fraudes, os golpistas podem criar aplicativos que parecem legítimos,

mas que têm como objetivo roubar dados pessoais dos usuários ou instalar malware em seus dispositivos, esses aplicativos podem ser oferecidos em lojas de aplicativos não oficializadas ou até mesmo em marketplaces conhecidos, tornando-se mais difíceis de detectar.

Os golpes cibernéticos são uma preocupação crescente no mundo digital, apresentando uma variedade de formas e técnicas que evoluem constantemente, desde phishing até ransomware e ataques direcionados, os métodos utilizados pelos golpistas são tão diversos quanto as tecnologias que exploram.

A compreensão destes diferentes tipos de golpes ajuda usuários e organizações a se protegerem e a tomarem precauções adequadas diante do ambiente cada vez mais complexo da criminalidade cibernética, nesse cenário, promover a educação em segurança digital e o engajamento ativo na proteção de informações pessoais se tornam ações essenciais para mitigar os riscos associados a esses crimes.

1.1.1 MECANISMO DE ATRAÇÃO DAS VÍTIMAS

Os golpistas cibernéticos utilizam uma variedade de mecanismos sofisticados para atrair e enganar suas vítimas, esses métodos são frequentemente baseados em psicologia, manipulando emoções e comportamentos humanos para facilitar a execução do golpe, e compreender esses mecanismos é crucial para desenvolver estratégias de prevenção e proteção contra fraudes online.

Em reportagem a BBC, os especialistas Johnstone e Psaroulis afirmam que:

> Os golpistas usam técnicas psicológica sofisticadas, eles exploram nossas vulnerabilidades humanas mais profundas e ignoram o pensamento racional para explorar nossas respostas emocionais, essa “guerra psicológica” coage as vítimas a tomarem decisões impulsivas, as vezes os golpistas espalham seus métodos entre muitas vítimas em potencial para ver quem é vulnerável. Outras vezes, os criminosos se concentram em uma pessoa específica. (JOHNSTONE E PSAROULIS, 2024, p. 01).

Os especialistas Johnstone e Psaroulis explicam sobre golpes em ligações aleatórias:

> Os golpistas começam com pequenas solicitações para estabelecer um sentimento de compromisso. Depois de concordar com estes pequenos pedidos, é provável que atenda a demandas maiores, motivados por um desejo de agir de forma consciente. A chamada não virá de um número da

> agenda da vítima, mas o golpista pode fingir ser alguém que você contratou para trabalhar em sua casa, ou talvez um de seus filhos, usando o telefone de um suposto amigo. (JOHNSTONE E PSAROULIS, 2024, p. 01).

Um dos principais mecanismos é a criação de um senso de urgência, os golpistas frequentemente informam suas vítimas que elas devem agir rapidamente, seja para resgatar um prêmio, evitar uma penalidade ou garantir uma oferta limitada, essa pressão é projetada para inibir a reflexão crítica e levar as vítimas a agir de forma impulsiva, aumentando assim as chances de sucesso do golpe.

Os especialistas Johnstone e Psaroulis explicam sobre a criação do senso de urgência:

> Os golpistas fabricam cenários que exigem ação imediata, como alegar que uma conta bancária está em risco, ou que a uma oferta está prestes a expirar. Esta tática visa a impedir que as vítimas avaliem a situação de forma lógica, ou busquem algum aconselhamento, pressionando-as a tomar decisões precipitadas. (JOHNSTONE E PSAROULIS, 2024, p. 01).

Para os especialistas da BBC:

> Os Golpistas se aproveitam das emoções para provocar reações que ofuscam o julgamento. Eles podem ainda, ameaçar com problemas na Justiça com a finalidade de colocar medo, prometer altos retornos de investimentos, para explorar a ganância ou compartilhar histórias angustiantes, mas falsas, para obter simpatia e bens financeiros. (JOHNSTONE E PSAROULIS, 2024, p. 01).

Outro mecanismo eficaz é o uso das fraudes de confiança, os golpistas se passam por instituições conhecidas, como bancos ou empresas de renome, aumentando a probabilidade de que as vítimas confiem neles.

Ao estabelecer uma falsa legitimidade, como logotipos e endereços de e-mail semelhantes, os criminosos podem enganar facilmente indivíduos que não estão cientes da possibilidade de fraude.

Os especialistas da BBC alertam que

> Por meio de conversas prolongadas, os golpistas criam um compromisso psicológico om seu esquema. Ninguém vai muito longe, simplesmente pelo fato de exigir a senha, mas é natural ser amigável com pessoas que são amigáveis com a vítima. Depois de ficar na linha por longos períodos, a vítima também fica cognitivamente cansada, isso não torna a vítima mais aberta a sugestões, mas também a isola de amigos ou familiares que poderiam reconhecer e combater o golpe. (JOHNSTONE E PSAROULIS, 2024, p. 01).

As emoções desempenham um papel central na atração de vítimas, os golpistas muitas vezes exploram sentimentos como medo, ganância, compaixão ou desejo de pertencimento, por exemplo, golpes de romance aproveitam o desejo de

conexão emocional, enquanto robôs de "phishing" criam medo ao afirmar que a conta da vítima foi comprometida, levando-a a fornecer informações pessoais sob pressão emocional.

Os golpes relacionados a investimentos são outro exemplo de como a atração pela possibilidade de lucro pode ser explorada, os golpistas frequentemente divulgam informações sobre investimentos de alto retorno e baixo risco, manipulando a avareza das pessoas, muitas vítimas são atraídas pela promessa de riqueza rápida, levando-as a investir dinheiro em esquemas fraudulentos que nunca oferecem o retorno prometido.

As redes sociais também se tornaram um campo fértil para a atração de vítimas, os golpistas utilizam esses canais para criar perfis falsos, interagindo com usuários e estabelecendo uma relação de confiança antes de apresentar um golpe, a vulnerabilidade causada pela exposição nas redes sociais torna as pessoas ainda mais suscetíveis ao engano, pois elas tendem a confiar mais em indivíduos que parecem ser amigos ou conhecidos.

Além disso, o compartilhamento de notícias sobre supostas ofertas imperdíveis ou concursos ganhos por outras pessoas cria uma falsa sensação de segurança, muitos usuários acreditam que, se outras pessoas tiveram experiências positivas com uma marca ou oferta, eles também podem confiar no que está sendo proposto, levando-os a desconsiderar potenciais sinais de alerta.

Os golpistas também podem manipular a aparência de seus sites ou comunicações para que sejam visualmente atraentes e convincentes, usando design profissional e layouts semelhantes aos de empresas reconhecidas, eles criam um ambiente que se parece legítimo, isso reforça a confiança do usuário, tornando-o mais propenso a compartilhar informações e realizar transações.

Um outro mecanismo importante é a segmentação de público, os golpistas muitas vezes adaptam suas abordagens de acordo com o perfil de suas vítimas, utilizando dados demográficos e comportamentais para personalizar suas tentativas de golpe, essa personalização aumenta a eficácia do ataque, pois as mensagens são direcionadas a grupos que têm maior probabilidade de serem atraídos pela proposta.

Os ataques em massa também possuem um apelo particular, como os e-mails de phishing enviados para centenas ou milhares de pessoas simultaneamente a ideia de que alguém pode estar "especialmente escolhido" para receber uma oferta exclusiva pode ser tentadora para muitos, esse tipo de mensagem coletiva faz com que as pessoas se sintam parte de algo maior, levando alguns a agir sem pensar.

A técnica da reciprocidade também é um mecanismo utilizado, os golpistas podem oferecer algo "gratuito" ou de valor antes de pedirem algo em troca, por exemplo, eles podem enviar uma amostra grátis de um produto ou oferecer um serviço ao usuário, criando a obrigação de corresponder à generosidade, o que muitas vezes leva a vítima a fornecer informações que não teria dado de outra forma.

A desinformação e a manipulação de dados também são estratégias acionadas para atrair vítimas, os golpistas frequentemente disseminam informações falsas, como relatórios de segurança ou alegações de novos recursos de segurança, para fomentar um clima de insegurança, isso pode levar as pessoas a reagirem impulsivamente, fornecendo dados ou clicando em links maliciosos.

A normalização do comportamento fraudulento na cultura digital também pode contribuir para a atração de vítimas, à medida que os golpes se tornam mais comuns, os usuários podem começar a subestimar a gravidade do problema, fazendo com que ignorem sinais de alerta.

A familiaridade com fraudes online pode levar a um sentimento de descrença na prevenção, expondo ainda mais as vítimas, esses ataques são mais elaborados e frequentemente se aproveitam de informações pessoais que os golpistas obtêm das redes sociais ou de outras fontes, como resultado, os e-mails ou mensagens criadas parecem quase reais, aumentando a probabilidade de que a vítima caia na armadilha.

Os golpes de "Bait and Switch" ocorrem quando os golpistas atraem as vítimas com uma oferta enganosa, como produtos a preços baixos, apenas para mudar os termos da negociação ou não entregar o produto após o pagamento, esse tipo de golpe explora a frustração dos consumidores em busca de boas ofertas, manipulando a psicologia do desejo por economizar.

Por último, o uso de aplicativos maliciosos também se tornou um método frequente para perpetrar fraudes, os golpistas podem criar aplicativos que parecem legítimos, mas que têm como objetivo roubar dados pessoais dos usuários ou instalar malware em seus dispositivos, esses aplicativos podem ser oferecidos em lojas de aplicativos não oficializadas ou até mesmo em marketplaces conhecidos, tornando-se mais difíceis de detectar.

Os golpes cibernéticos são uma preocupação crescente no mundo digital, apresentando uma variedade de formas e técnicas que evoluem constantemente, desde phishing até ransomware e ataques direcionados, os métodos utilizados pelos golpistas são tão diversos quanto as tecnologias que exploram.

De acordo com Barbosa:

> A compreensão dos temas abordados é de extrema relevância para a legislação brasileiro, pois a globalização e a inserção da tecnologia coexistem no ambiente profissional e pessoal das pessoas. A internet é sinônimo do avanço da comunicação e hoje, vem se expandindo por todo o mundo, tornando-se cada dia mais acessível (BARBOSA, 2022. P. 22).

A compreensão destes diferentes tipos de golpes ajuda usuários e organizações a se protegerem e a tomarem precauções adequadas diante do ambiente cada vez mais complexo da criminalidade cibernética, nesse cenário, promover a educação em segurança digital e o engajamento ativo na proteção de informações pessoais se tornam ações essenciais para mitigar os riscos associados a esses crimes.

2.OS IMPACTOS PSICOLÓGICOS NAS VÍTIMAS

Os impactos psicológicos nas vítimas de diversas experiências adversas, incluindo violência, acidentes, desastres naturais e abusos, são profundos e podem perdurar por muitos anos, esses efeitos não se limitam a danos imediatos; frequentemente, eles se manifestam em formas que afetam a vida cotidiana da pessoa, sua saúde mental e sua capacidade de funcionar normalmente dentro da sociedade, e entender essas consequências é fundamental para oferecer o suporte necessário, facilitando a recuperação e reintegração das vítimas em seus contextos sociais e familiares.

Conforme explica Alves:

> É essencial destacar que as respostas ao trauma podem variar de pessoa para pessoa. Assim como a gravidade do trauma emocional pode ser influenciada por fatores como o nível de resiliência da pessoa, o suporte social e as circunstâncias especificas em que o trauma ocorreu. (ALVES, 2024, p. 01).

Um dos efeitos mais comuns nas vítimas é o desenvolvimento de transtornos de estresse pós-traumático (TEPT), que pode ocorrer após experiências traumáticas, as vítimas de TEPT frequentemente revivem a experiência trauma por meio de recordações intrusivas, pesadelos e flashbacks, tornando suas vidas cotidianas insuportáveis, esses sintomas podem ser acompanhados de ansiedade severa e evitamento de lugares ou situações que lembrem o evento traumático, resultando em dificuldades em levar uma vida normal.

De acordo com Deus e Munhos:

> O Transtorno do estresse pós-traumático (TEPT), ou perturbação de estresse pós-traumático (PSPT), é o distúrbio de ansiedade que se manifesta por meio de uma variedade de sintomas físicos, psicológicos e emocionais. Esta condição ocorre em pessoas que foram vítimas ou testemunhas de eventos violentos ou experiencias traumáticas. Entre os sintomas mais comuns, estão o distanciamento emocional, os pesadelos e flashbacks involuntários de memórias traumáticas. (DEUS; MUNHOS. 2024, p. 01).

Além do TEPT, as vítimas podem experimentar depressão severa como consequência da experiência traumática, esse estado emocional geralmente é caracterizado por sentimentos persistentes de tristeza, desesperança e até mesmo a perda de interesse em atividades que anteriormente eram prazerosas, a depressão pode levar ao isolamento social, dificultando ainda mais a recuperação emocional, já que o suporte social é essencial para a cura.

Barnhill explica ainda que:

> O transtorno de estresse pós-traumático (TEPT), é o transtorno incapacitante que se desenvolve após a exposição a um evento traumático. É caracterizada por pensamentos intrusivos, pesadelos e flashbaks, esquiva de lembranças do trauma, cognições negativas e mau humor, hipervigilância e distúrbios do sono. O diagnóstico é baseado em critérios clínicos. O tratamento inclui psicoterapia e as vezes, terapias farmacológicas adjuvantes. (BARNHILL, 2023, p. 01).

Outra consequência psicossocial significativa é a ansiedade, muitas vítimas relatam sofrer de ansiedade generalizada ou de ataques de pânico que podem ser debilitantes, a constante sensação de perigo iminente, mesmo em ambientes que deveriam ser seguros, torna-se uma rotina para os sobreviventes, essa ansiedade

crônica pode manifestar-se em forma de comportamentos compulsivos de verificação ou evitamento, complicando ainda mais suas interações sociais.

Para Sá, comenta sobre esse assunto:

> Do ponto de vista jurídico, a violência nas redes sociais pode ser caracterizada como um crime, pois muitas vezes envolve difamação, calúnia, ameaças e até mesmo incitação à violência física. Essas atitudes podem causar danos morais e psicológicos as vítimas, além de afetar sua reputação e imagem perante a sociedade. (SÁ, 2023, p. 2 – 3).

As relações interpessoais também são profundamente afetadas pela experiência traumática, as vítimas frequentemente lutam para confiar nos outros, o que pode levar à deterioração de relacionamentos familiares e amizades, a insegurança e o medo podem levar as vítimas a se retirarem de suas redes de apoio, criando um ciclo vicioso que perpetua o sofrimento psicológico e social.

Além disso, as vítimas podem desenvolver uma percepção distorcida de si mesmas e dos outros, isso pode se manifestar na forma de baixa autoestima, sentimento de culpa ou vergonha, e uma visão negativa do mundo, o trauma pode fazer com que as vítimas sintam que são responsáveis pelo que aconteceu, mesmo quando não têm controle sobre a situação, agravando ainda mais seu sofrimento emocional.

Os impactos psicológicos também podem levar a comportamentos autodestrutivos, a algumas vítimas recorrem ao uso de substâncias como uma forma de lidar com a dor emocional, levando a dependências que complicam ainda mais sua recuperação, o alcoolismo, o uso de drogas ilícitas e comportamentos de autoagressão são alguns dos métodos que as vítimas podem usar para escapar da dor psicológica.

Adicionalmente, as vítimas podem experimentar dificuldades no ambiente de trabalho, resultantes tanto de sintomas da saúde mental quanto da necessidade de se afastar para tratamento, isso pode levar à perda de emprego, o que não apenas impacta financeiramente, mas também reforça a sensação de perda de controle e impotência, perpetuando sentimentos de inadequação e fracasso.

É importante considerar que os impactos psicológicos podem variar significativamente de acordo com fatores individuais como resiliência, histórico de traumas anteriores, suporte social e as características da experiência traumática em

si, por exemplo, indivíduos que já passaram por experiências traumáticas podem ter uma resposta mais intensa a novos traumas, enquanto outros podem encontrar força em suas experiências anteriores para ajudar em sua recuperação.

Os efeitos catastróficos de um trauma podem se estender à saúde física, a relação entre saúde mental e física é bem documentada, e muitas vítimas observam que seu psicológico impacta diretamente sua saúde física, manifestando-se em sintomas físicos que não têm uma causa médica clara, como dores crônicas, fadiga e distúrbios gastrointestinais.

O tratamento e a terapia são cruciais na abordagem dos impactos psicológicos nas vítimas, e existem várias modalidades de tratamento, incluindo terapia cognitivo-comportamental, terapia de exposição e terapia de grupo, que visam ajudar as vítimas a confrontarem e processar suas experiências, o apoio psicoterapêutico pode proporcionar um espaço seguro para que as vítimas compartilhem suas experiências e desenvolvam estratégias de coping eficazes.

É essencial que profissionais de saúde mental estejam cientes dos diferentes traumas e suas consequências para que possam oferecer o cuidado mais adequado, o treinamento focado em traumas e sensibilidade cultural pode ajudar os terapeutas a entenderem melhor as nuances das experiências traumáticas e a trabalhar mais eficazmente com as vítimas.

É importante criar uma rede de apoio comunitária que possa ajudar as vítimas em sua recuperação, a conscientização comunitária sobre os impactos dos traumas pode ajudar a reduzir o estigma, vale destacar que a liberdade de expressão, um direito essencial assegurado pela Constituição, não é ilimitada e impõe restrições quando exercida de maneira abusiva e prejudicial, o Código Penal Brasileiro estabelece penalidades para quem comete crimes virtuais, incluindo a Lei Carolina Dieckmann, que tipifica como crime a invasão de dispositivos eletrônicos e a divulgação indevida de dados pessoais.

Os crimes cibernéticos têm recebido crescente atenção por parte do Poder Judiciário brasileiro, especialmente diante do avanço da tecnologia e da ampliação do uso da internet nas relações sociais, comerciais e pessoais, as decisões judiciais vêm

se consolidando no sentido de reconhecer a gravidade dessas infrações e a necessidade de uma atuação eficaz do Estado para a repressão dessas condutas.

O Superior Tribunal de Justiça (STJ) tem contribuído de forma significativa para o delineamento da jurisprudência acerca dos crimes digitais, em diversos julgados, o Tribunal tem afirmado que os delitos cometidos por meio da internet não apenas se equiparam, em termos penais, aos crimes tradicionais, como também apresentam características específicas que exigem medidas investigativas modernas e adequadas.

Conforme o entendimento do Superior Tribunal de Justiça:

> É plenamente válida a utilização de provas obtidas por meio de interceptações telemáticas autorizadas judicialmente, inclusive em crimes cibernéticos, especialmente quando a atuação do agente é realizada em redes sociais e aplicativos de mensagens, cuja natureza pública ou semipública justifica a persecução penal.
> (STJ – HC 598.051/SP, Rel. Min. Ribeiro Dantas, Quinta Turma, julgado em 27/10/2020, DJe 03/11/2020)

Além disso, os julgados destacam a necessidade de **interpretação evolutiva e tecnológica do Direito Penal**, adaptando os institutos tradicionais à nova realidade virtual, a aplicação da lei tem contribuído para a responsabilização de infratores, mas também para o **debate sobre limites, provas digitais, e garantias processuais**, temas que ainda demandam aperfeiçoamento legislativo e técnico.

A jurisprudência relacionada à Lei Carolina Dieckmann evidencia a relevância do combate à criminalidade digital e a necessidade de constante **modernização das práticas judiciárias**, assegurando a efetiva proteção dos direitos fundamentais dos cidadãos na era da informação.

2.2 PROCESSO DE RECUPERAÇÃO E SUPORTE PSICOLÓGICO

Os golpes cibernéticos têm se tornado cada vez mais comuns na era digital, levando a situações de estresse emocional e psicológico para as vítimas, esse tipo de crime não apenas causa perdas financeiras, mas também pode resultar em sérios danos à saúde mental dos indivíduos afetados.

Para Sá, comenta sobre esse assunto:

> A violência nas redes sociais é o fenômeno que tem se tornado cada vez mais presente em nossa sociedade contemporânea. As redes sociais que foram criadas com o objetivo de promover a comunicação e a interação entre as

> pessoas, acabaram se tornando palco para o surgimento de comportamentos agressivos e prejudiciais. (SÁ, 2023, p. 02).

O primeiro passo para que as vítimas de golpes cibernéticos possam buscar recuperação é o reconhecimento do crime, esse reconhecimento é vital, pois muitas vítimas podem sentir uma mistura de vergonha e culpa, o que dificulta a busca por suporte psicológico e jurídico.

Sá explica que:

> A violência nas redes sociais pode assumir diferentes formas, desde ofensas verbais até ameaças físicas. A facilidade de disseminação de informações e a possibilidade de interação em tempo real contribuem para a rápida propagação de conteúdos violentos. (SÁ, 2023, p. 04).

O suporte psicológico é fundamental nesse processo de recuperação, visto que as consequências emocionais, como ansiedade, depressão e transtornos de estresse pós-traumático, podem persistir mesmo após a resolução da questão financeira, um profissional qualificado pode ajudar a vítima a compreender e processar suas emoções.

Sá pondera que:

> Os profissionais da área de psicologia também têm um papel importante no tratamento das vítimas de violência nas redes sociais. Através de abordagens terapêuticas específicas, como a terapia cognitivo comportamental, é possível auxiliar as pessoas a lidarem com as consequências emocionais negativas causadas pela exposição a violência virtual. (SÁ, 2023, p. 05).

Um acompanhamento psicológico deve ser uma prioridade, e terem um psicólogo capacitado para lidar com traumas relacionados a fraudes pode ser extremamente benéfico, o tratamento pode incluir terapia cognitivo-comportamental, que ajuda a reforçar a percepção das vítimas sobre o ocorrido.

Conforme Sá, sobre o assunto:

> É necessário que haja um acompanhamento mais de perto, principalmente, nessas faixas etárias que, é onde há mais vulnerabilidade emocional, tendo em vista que é onde o psicólogo está em principal fase de desenvolvimento e fatores como estes, principalmente a exposição constante a violência online, podem trazer diversos problemas, não só as crianças, mas de modo geral, tais como: Depressão, ansiedade, isolamento e distanciamento dos amigos e família, autoestima abalada, notas na escola/faculdade e sensação de culpa pelos ataques sofridos, caso tenha havido. (SÁ, 2023, p. 07).

Além do suporte psicológico, é crucial abordar as questões legais envolvidas, a vítima deve procurar orientação jurídica para entender seus direitos e as ações que podem ser tomadas em relação ao golpe, a legislação atual fornece ferramentas para a proteção do consumidor e para a responsabilização dos agressores.

Sá explica que:

> É importante também, que se saiba que a internet não é terra sem lei, e atualmente, já existem formas de proteger de ataques virtuais sofridos de forma totalmente legal, e amparada pela lei, tendo em vista que assim como há leis que garantem a liberdade de expressão de todos os indivíduos, também há leis que garantem o direito ao bem-estar social de modo geral. (SÁ, 2023, p. 08).

O registro de uma ocorrência policial é um passo importante para a documentação do golpe e para a abertura de investigações, esse registro pode ser usado para fins legais e pode ajudar na recuperação de perdas financeiras.

As vítimas devem ser orientadas sobre a possibilidade de buscar indenização por perdas financeiras, isso pode incluir entrar em contato com instituições financeiras, plataformas online ou até mesmo processos civis contra os responsáveis pelo golpe.

Organizações e instituições que oferecem suporte a vítimas de crimes podem ser um recurso valioso, e por muitas vezes, essas entidades oferecem não apenas suporte jurídico, mas também psicológico, ajudando as vítimas a navegarem pelas complexidades do processo de recuperação.

Participar de grupos de apoio pode proporcionar um espaço seguro para as vítimas compartilharem suas experiências, esses grupos podem ajudar a normalizar a experiência emocional da vítima e oferecer um sistema de suporte comunitário.

É vital que as vítimas tenham acesso a informações sobre a importância da saúde mental, o estigma em torno de buscar ajuda psicossocial deve ser combatido, e campanhas educacionais podem ser úteis para promover a conscientização sobre as consequências emocionais das fraudes.

As vítimas devem também ser incentivadas a registrar todos os dados relacionados ao golpe (e-mails, mensagens, transações), o que não só ajuda nas

investigações, mas também na autoanálise e identificação de possíveis vulnerabilidades pessoais para prevenir futuros golpes.

Os programas educacionais sobre segurança cibernética são essenciais para prevenir que mais indivíduos se tornem vítimas de golpes, essa educação deve ser uma preocupação contínua, começando em escolas e se estendendo a adultos através de workshops e webinars.

Dado que muitos crimes cibernéticos ocorrem em uma esfera global, a cooperação internacional entre órgãos de segurança e judiciários é fundamental, o compartilhamento de informações e recursos pode auxiliar na resolução de casos e na identificação de criminosos.

As consequências psicológicas de golpes cibernéticos devem ser uma área de pesquisa contínua, e compreender melhor como essas experiências afetam os indivíduos pode levar ao desenvolvimento de políticas públicas mais eficazes para ajudar as vítimas.

A recuperação emocional e a assistência jurídica para pessoas que sofreram golpes cibernéticos são aspectos cruciais no processo de superação, e implementar uma abordagem integrada que considere tanto o suporte psicológico quanto a busca por justiça pode ajudar as vítimas a retomarem suas vidas de forma saudável e consciente.

2.2.2 OS IMPACTOS FINANCEIROS DAS VÍTIMAS QUE SOFREM GOLPES CIBÉRNETICOS

Os golpes cibernéticos têm se tornado cada vez mais frequentes e sofisticados, representando um risco significativo para a segurança financeira de indivíduos e empresas, as vítimas desses crimes enfrentam uma série de consequências financeiras que vão além da perda imediata de dinheiro, este fenômeno não apenas resulta em prejuízos diretos, mas também pode desencadear um efeito dominó que afeta outros aspectos da vida financeira das pessoas.

Para Oliveira:

> O crime cibernético é um ato ilícito, praticado por meio de dispositivos móveis, como os computadores, celulares e tablets. A consequência ocasionada pelo crime de meio, praticado na internet podem afetar pessoas e empresas no

> âmbito nacional e internacional, tais atos causam danos a reputação das vítimas e prejuízos financeiros. (OLIVEIRA, 202, p. 04).

É importante destacar que muitos golpes cibernéticos envolvem a obtenção de informações pessoais sensíveis, como dados bancários e senhas, quando essas informações são comprometidas, as vítimas podem ver suas contas esvaziadas quase que instantaneamente, a sensação de impotência é exacerbada pela dificuldade em recuperar os fundos perdidos, já que os processos de estorno costumam ser longos e intrincados.

Colaço explica que:

> No Brasil, Golpes financeiros praticados por meio de dispositivos eletrônicos foram tipificados como crimes nos art. 154 e 155 do Código Penal a partir de 2012. Nove anos depois, a Lei 14.155 de 2021 tornou mais grave a violação de dispositivos informáticos, furto e estelionato cometidos de forma eletrônica ou pela internet, com penas de multa e de reclusão de até oito anos. (COLAÇO, 2024, p. 01).

Além das perdas financeiras diretas, as vítimas de golpes cibernéticos frequentemente enfrentam custos adicionais, por exemplo, muitos optam por contratar serviços de monitoramento de crédito para proteger suas informações pessoais após um ataque, essas despesas são uma necessidade emergente, mas podem afetar o orçamento mensal da vítima, criando uma pressão financeira adicional.

Para Nogueira:

> O impacto financeiro das fraudes digitais é significativo tanto para consumidores quanto para empresas. As perdas podem ser enormes e, em muitos casos, os consumidores sofrem diretamente quando negligenciam as boas práticas de segurança. (NOGUEIRA, 2023, p. 01).

Nogueira explica ainda que:

> Além das perdas financeiras, estes crimes afetam gravemente a confiança do consumidor em plataformas de comércio eletrônico. [...] A reputação de uma empresa pode ser irremediavelmente comprometida, levando a desvalorização da marca. (NOGUEIRA, 2023, p. 01).

A insegurança financeira resultante de um golpe também pode levar as vítimas a um ciclo de estresse e ansiedade, os gastos relacionados à recuperação da segurança online e a sensação de vulnerabilidade podem dificultar a tomada de decisões financeiras a longo prazo, muitas pessoas se tornam tão cautelosas que evitam realizar transações online, o que pode limitar suas oportunidades de negócios e investimentos.

Outro aspecto recorrente nas decisões judiciais é a proteção da vítima e a reparação dos danos. A jurisprudência tem reafirmado o dever de indenizar os prejuízos sofridos por vítimas de golpes virtuais, inclusive responsabilizando solidariamente plataformas digitais, instituições bancárias e intermediadores de pagamentos quando há falhas na segurança ou omissão na prestação de serviço.

Conforme o entendimento do Tribunal de Justiça de Minas Gerais:

> "Configura falha na prestação do serviço bancário a ausência de mecanismos eficazes de segurança para prevenir transações fraudulentas realizadas por terceiros, devendo a instituição financeira responder objetivamente pelos danos causados à vítima, nos termos do art. 14 do CDC." (TJMG – Apelação Cível nº 1.0024.21.196532-3/001, Rel. Des. Pedro Aleixo, 17ª Câmara Cível, julgado em 12/09/2023)

Os impactos financeiros não se restringem apenas ao indivíduo, mas também afetam as pequenas empresas que podem ser alvos de ataques, e muitas vezes, os proprietários de pequenas empresas não estão adequadamente preparados para lidar com as consequências financeiras de um golpe cibernético, isso pode incluir a perda de receita, danos à reputação da empresa e custos associados a reparos e resgates de dados.

Além disso, danos à reputação podem resultar em uma diminuição da confiança do cliente, para um pequeno negócio, a confiança do cliente é fundamental, e a percepção de que uma empresa não consegue proteger os dados de seus clientes pode levar à perda de clientela, impactando ainda mais a saúde financeira da empresa.

A recuperação após um golpe cibernético também pode envolver custos legais, as vítimas que desejam processar responsáveis pelos golpes podem encontrar-se diante de despesas jurídicas altas e incertas, o que pode ser um fardo financeiro considerável, a probabilidade de sucesso em uma ação legal também é variável, e muitas vezes as vítimas se sentem desanimadas em buscar justiça.

A educação financeira é outro aspecto afetado, muitas vítimas de golpes cibernéticos não estavam cientes dos riscos existentes, e isso pode levar a uma maior vulnerabilidade a futuros ataques, e investir em educação e conscientização sobre segurança cibernética pode representar um custo importante, mas é uma despesa necessária para evitar perdas financeiras adicionais no futuro.

Ainda no que diz respeito às consequências psicológicas, as vítimas frequentemente experimentam um impacto na sua saúde mental, que pode se traduzir em gastos com terapia e cuidados de saúde mental, o estresse financeiro, combinado com a ansiedade resultante da experiência do golpe, pode criar um ciclo vicioso que afeta tanto o bem-estar emocional quanto a situação financeira.

Com a crescente digitalização da economia, a exposição a golpes cibernéticos está em alta, e, por consequência, os impactos financeiros também aumentam o conceito de "normalização do golpe" pode ocorrer, onde as pessoas se tornam resignadas a aceitar a possibilidade de serem alvo desses crimes, isso não deve ser visto como um dado irreversível, pois a conscientização e a educação proativa podem ajudar a prevenir golpes futuros.

Outro ponto relevante é o efeito que golpes cibernéticos têm sobre a confiança na economia digital, à medida que mais pessoas se tornam vítimas, a percepção de segurança nas transações online diminui. Isso pode resultar em menos pessoas dispostas a comprar online ou utilizar serviços digitais, afetando negativamente o crescimento econômico em setores que dependem da confiança do consumidor.

Integrar medidas de segurança cibernética nas práticas financeiras se torna cada vez mais importante, as vítimas de golpes devem ser incentivadas a usar autenticação de dois fatores, criar senhas robustas e educar-se sobre as táticas utilizadas por golpistas, essas práticas não eliminam os riscos, mas podem mitigar os impactos financeiros significativos que podem ocorrer após um golpe.

É essencial que haja um esforço conjunto entre governos, empresas e instituições financeiras para abordar o problema dos golpes cibernéticos, as políticas públicas que promova a educação sobre segurança digital e ofereça suporte financeiro às vítimas podem ser passos importantes em direção à mitigação dos impactos financeiros que essas fraudes têm sobre a sociedade.

Importante ressaltar pelo Tribunal de Justiça de Minas Gerais, sobre assunto:

> EMENTA: APELAÇÃO - PORNOGRAFIA INFANTIL (ARTS. 240 E 241-B, DO ECA) - PRELIMINAR - INCOMPETÊNCIA DA JUSTIÇA ESTADUAL PARA JULGAR CRIMES CIBERNETICOS - INOCORRÊNCIA - AUSÊNCIA DE

> DISPONIBILIZAÇÃO OU COMPARTILHAMENTO DAS IMAGENS - PRELIMINAR - PROVA ILÍCITA - INOCORRÊNCIA - DESNECESSIDADE DE EXPEDIÇÃO DE MANDADO DE BUSCA E APREENSÃO - CRIME PERMANENTE - MÉRITO - ABSOLVIÇÃO - IMPOSSIBILIDADE - AUTORIA E MATERIALIDADE COMPROVADAS - CONDENAÇÃO MANTIDA. - Será da competência da Justiça Federal para processar e julgar os crimes cibernéticos, consistentes em disponibilizar ou adquirir material pornográfico envolvendo criança ou adolescente, apenas quando esses forem praticados por meio da rede mundial de computadores - Nos crimes permanentes não há necessidade de mandado de busca e apreensão quando houver flagrante, conforme disposição do artigo 5º inciso XI da Constituição Federal - Restando comprovadas a autoria e a materialidade dos delitos previstos nos arts. 240 e 241-B, do ECA, por meio de prova pericial, corroborada pelo depoimento de testemunhas, não há que se falar em absolvição por ausência de provas. (TJ-MG - APR: 10027140000624001 Betim, Relator.: Agostinho Gomes de Azevedo, Data de Julgamento: 19/12/2018, Câmaras Criminais / 7ª CÂMARA CRIMINAL, Data de Publicação: 23/01/2019)

A jurisprudência proferida pelo Tribunal de Justiça de Minas Gerais, no julgamento da apelação criminal relacionada aos crimes de pornografia infantil previstos nos artigos 240 e 241-B do Estatuto da Criança e do Adolescente (ECA), oferece importantes diretrizes para a aplicação do Direito Penal em casos de delitos cibernéticos. O acórdão analisou questões centrais como a competência jurisdicional, a validade das provas obtidas, e a comprovação dos elementos do crime, reafirmando posições fundamentais da jurisprudência atual.

No que se refere à competência, o tribunal decidiu que a Justiça Estadual possui legitimidade para processar e julgar crimes praticados por meios eletrônicos quando não há prova de que o material foi efetivamente compartilhado pela internet. A decisão estabelece que a competência da Justiça Federal está restrita aos casos em que há disponibilização do conteúdo na rede mundial de computadores, ou quando o delito atinge interesses da União, o que não se verificou no caso concreto. Essa distinção é fundamental para evitar conflitos de atribuição entre esferas judiciais.

Quanto à produção da prova, foi reconhecida a licitude das evidências obtidas sem mandado judicial, uma vez que se tratava de crime permanente , ou seja, cuja consumação se prolonga no tempo, enquanto o agente mantém o conteúdo ilícito em sua posse. Em situações como essa, a Constituição Federal autoriza a entrada em domicílio sem mandado, desde que em flagrante delito, o que justifica a atuação dos agentes públicos no caso analisado.

A condenação do réu foi mantida, tendo em vista que tanto a autoria quanto a materialidade do crime foram claramente demonstradas. Exames periciais

confirmaram o conteúdo ilegal armazenado, e os demais elementos colhidos no processo reforçaram a existência do crime, ainda que não tenha havido o compartilhamento das imagens, a decisão, portanto, demonstra que a simples posse ou armazenamento de material pornográfico envolvendo menores já configura infração penal, independentemente de haver divulgação.

Essa jurisprudência é relevante por reafirmar o compromisso do Judiciário com a proteção de crianças e adolescentes, sobretudo frente aos riscos do ambiente virtual, ao mesmo tempo, reforça a possibilidade de atuação estatal eficaz mesmo diante das particularidades dos crimes digitais, garantindo a aplicação da lei penal sem violação aos direitos fundamentais, o posicionamento adotado contribui para consolidar parâmetros seguros na repressão aos crimes cibernéticos, promovendo segurança jurídica e efetividade no combate a esse tipo de delito.

Com relação aos impactos financeiros resultantes de golpes cibernéticos são complexos e multifacetados, e eles vão desde perdas diretas imediatas até consequências a longo prazo que envolvem custos adicionais, estresse e uma evasão de oportunidades financeiras, as vítimas frequentemente se veem em um cenário desfavorável, onde a recuperação financeira se torna uma luta árdua, tratando não apenas das finanças, mas também do abalo mental e emocional que esses golpes trazem.

A conscientização sobre os impactos financeiros dos golpes cibernéticos é crucial para ajudar as pessoas a se protegerem e agirem rapidamente em caso de ataque, os programas de educação financeira que incluam tópicos de segurança digital podem ser extremamente benéficos, capacitando os indivíduos a reconhecerem e evitar potenciais ameaças.

Além disso, as instituições financeiras devem proporcionar um suporte mais robusto às vítimas, oferecendo aconselhamento e recursos que ajudem na recuperação das perdas financeiras.

As consequências financeiras dos golpes cibernéticos também demonstram a necessidade de uma abordagem coletiva para a segurança cibernética, as empresas devem investir mais em tecnologia de proteção e em treinamento de funcionários para evitar que se tornem inadvertidamente parte do problema, a

colaboração entre o setor público e privado é essencial para compartilhar informações sobre ameaças e desenvolver estratégias eficazes para mitigar os riscos.

No futuro, é de extrema importância que a sociedade leve a sério a segurança cibernética como um aspecto intrínseco da vida financeira o aprendizado contínuo e a adaptação às novas tecnologias e métodos de ataque podem não apenas proteger os ativos financeiros, mas também fortalecer a confiança nas interações digitais, ao criar um ambiente mais seguro, podemos melhorar a nossa saúde financeira coletiva e individual.

O impacto financeiro dos golpes cibernéticos é uma questão que deve ser abordada com seriedade e proatividade, cada vítima tem uma história que revela a realidade alarmante dos riscos que enfrentamos no mundo digital. Ao unir esforços para educar, proteger e apoiar as vítimas, podemos reduzir os efeitos devastadores que esses crimes têm sobre a vida das pessoas e da economia como um todo.

A luta contra o crime cibernético deve ser constante e envolve a participação de todos na sociedade, além de um compromisso em promover um ambiente digital mais seguro e resiliente.

3. OS IMPACTOS SOCIAIS DECORRENTES DOS GOLPES CIBERNÉTICOS

Os golpes cibernéticos têm se tornado uma preocupação crescente em nossa sociedade hiper conectada, esses crimes virtualizados não apenas afetam indivíduos, mas também impactam comunidades, instituições e até mesmo países inteiros.

Tocantins explica que:

> Com o avanço da tecnologia e a crescente interconexão proporcionada pela internet, os crimes cibernéticos se tornaram uma preocupação cada vez mais relevante na sociedade contemporânea. Esses delitos cometidos por meio de dispositivos eletrônicos e redes digitais, representam uma gama diversificada de atividades ilícitas que afetam indivíduos, empresas e governos em escala global. (TOCANTINS, 2023, p. 01).

Um dos impactos sociais mais evidentes dos golpes cibernéticos é o aumento da desconfiança entre as pessoas, quando um grupo ou indivíduo é vítima de um ataque, a confiança nas interações online e nas transações financeiras pode diminuir significativamente, isso pode levar a um isolamento social, onde as pessoas se tornam mais relutantes em se envolver em atividades virtuais.

Para Tocantins:

> A rápida evolução tecnológica trouxe consigo a conveniência e a eficiência, mas também abriu portas para novas formas de criminalidade. Os criminosos cibernéticos se aproveitam de brechas na segurança digital e ingenuidade dos usuários para cometer crimes que podem causar prejuízos financeiros, emocionais e psicológicos significativos. (TOCANTINS, 2023, p. 01).

Os ataques cibernéticos também influenciam negativamente a saúde mental das vítimas, a sensação de violação de privacidade, a perda de bens financeiros e a insegurança constante podem causar estresse, ansiedade e depressão, infelizmente, essas questões de saúde mental não apenas afetam os indivíduos, mas também seus relacionamentos e a dinâmica familiar.

No âmbito econômico, os golpes cibernéticos têm um impacto devastador, empresas que sofrem ataques podem enfrentar custos significativos relacionados à recuperação dos dados, processos legais e perda de receita, além disso, a reputação de uma empresa pode ser seriamente danificada, resultando em perda de clientes e até mesmo falência, o que afeta muitas famílias que dependem dessas empresas para seu sustento.

Os golpes cibernéticos também têm um impacto na democracia e na confiança nas instituições públicas, quando informações sensíveis de cidadãos, organizações e governos são comprometidas, a confiança nos sistemas democráticos pode ser prejudicada, as pessoas podem se sentir desiludidas com a capacidade de suas instituições em proteger suas informações e garantir sua segurança.

Além das consequências diretas, os golpes cibernéticos muitas vezes alimentam a desigualdade social, os grupos mais vulneráveis, como idosos e pessoas com menos acesso à educação financeira, são frequentemente as principais vítimas desses crimes. Isso perpetua um ciclo de desigualdade, onde os já marginalizados se tornam ainda mais vulneráveis.

Tocantins explica ainda que:

> [...] os crimes cibernéticos representam uma ameaça significativa na era digital atual, exigindo ações coordenadas e esforços em constantes evolução. A conscientização, a educação, a regulamentação adequada e a implementação e medidas de segurança são fundamentais para proteger indivíduos, organizações e a sociedade como um todo, contra os impactos prejudiciais destes delitos. (TOCANTINS, 2023, p. 01).

A educação e conscientização também são abordagens sociais influenciadas pelos golpes cibernéticos, para mitigar os riscos, instituições educacionais e organizações governamentais têm investido em programas de alfabetização digital, isso não apenas empodera os cidadãos, mas também ajuda a construir uma sociedade mais resiliente à criminalidade cibernética.

Tocantins esclarece que:

> A cooperação entre setores públicos e privado, a troca de informações e a colaboração internacional de informações são elementos chave na luta contra os crimes cibernéticos, visando a mitigação de ameaças, a proteção dos dados pessoais e o fortalecimento da segurança cibernética global. (TAOCANTINS, 2023, p. 01).

Os golpes cibernéticos podem levar a um aumento nas regulamentações e legislações relacionadas à segurança cibernética, quando ocorrem grandes ataques, pode haver uma pressão social significativa sobre os governantes para proteger os cidadãos, essa necessidade de proteção resulta em um enfoque mais sério sobre a necessidade de políticas de segurança cibernética.

O impacto social dos golpes cibernéticos também se estende ao campo da tecnologia, a demanda por soluções de segurança digital aumentou, levando ao crescimento da indústria de cibersegurança, isso não apenas cria empregos, mas também estimula a inovação tecnológica na busca por métodos mais eficazes de proteção contra-ataques cibernéticos.

Além disso, há um efeito psicológico em larga escala, onde a narrativa dos golpes cibernéticos alimenta uma cultura de medo e vigilância, isso pode levar a um estado constante de alerta entre os cidadãos, criando uma sociedade que vive com insegurança constante, ao mesmo tempo, essa cultura pode resultar em violação da privacidade, com indivíduos se sentindo forçados a adotar medidas de segurança excessivas.

Os golpes cibernéticos também podem provocar uma resposta social em forma de solidariedade e apoio comunitário, e muitas vezes, as comunidades se reúnem para ajudar as vítimas, oferecendo suporte emocional e prático, essa solidariedade pode fortalecer laços comunitários, transformando uma experiência negativa em uma oportunidade de união.

Os jovens, cada vez mais inseridos no mundo digital, também são impactados, a exposição a fraudes online e cyberbullying pode afetar o desenvolvimento social e emocional das crianças e adolescentes, as instituições educacionais têm ajudado a proteger seus alunos, mas a responsabilidade também recai sobre os pais e responsáveis para ensiná-los sobre segurança online.

Além disso, golpes cibernéticos podem ser usados como ferramentas de manipulação nas redes sociais, afetando a forma como as pessoas se comunicam e interagem. Isso pode levar ao fortalecimento de grupos extremistas e à disseminação de desinformação, impactando ainda mais o tecido social e a coesão comunitária.

Os golpes cibernéticos também são uma ameaça à liberdade de expressão, especialmente em regimes autoritários, a vigilância e controle sobre informações podem silenciar vozes dissidentes e entorpecer o debate público, isso resulta em uma sociedade menos informada e mais suscetível a manipulações.

O impacto social dos golpes cibernéticos ressalta a necessidade de uma abordagem colaborativa e global para a segurança cibernética os governos, empresas e cidadãos precisam trabalhar juntos para criar um ambiente digital mais seguro, somente através da colaboração podemos efetivamente enfrentar os desafios que os golpes cibernéticos impõem e promover um espaço online que proteja os direitos de todos os usuários.

Essa colaboração deve incluir a troca de informações sobre ameaças, o desenvolvimento de melhores práticas para segurança cibernética e o investimento em tecnologia que permita uma resposta rápida a incidentes, além disso, é essencial que as políticas públicas sejam constantemente atualizadas para enfrentar novos tipos de fraudes e para proteger, especialmente, aqueles que são mais vulneráveis.

A educação continua a ser uma ferramenta poderosa na luta contra os golpes cibernéticos, os programas de workshop e conscientização voltados para diferentes faixas etárias e níveis de habilidade digital podem ajudar a construir uma comunidade mais informada, a medida que as pessoas se tornam mais cientes dos riscos e das técnicas usadas pelos golpistas, elas estão mais capacitadas a se protegerem.

Da mesma forma, as empresas precisam adotar uma postura proativa em relação à segurança cibernética, isso não significa apenas investir em tecnologia; também envolve a criação de uma cultura de segurança dentro da organização, onde cada funcionário entende seu papel na proteção contra-ataques cibernéticos, os treinamentos regulares e simulações de incidentes podem preparar melhor as equipes para responder rapidamente a ameaças.

Os golpes cibernéticos não são apenas problemas técnicos, mas questões sociais complexas que exigem uma abordagem holística, a promoção de um ambiente digital mais seguro não apenas protege os indivíduos, mas também fortalece as comunidades e a sociedade como um todo, garantindo que todos tenham acesso à informação e à educação adequadas, podemos construir um futuro em que a inovação e a interconexão não venham com o alto custo da vulnerabilidade.

Construir esse futuro requer um esforço conjunto e a compreensão de que, em um mundo digital, a segurança de um é a segurança de todos, portanto, ao nos unirmos em solidariedade e ação, podemos enfrentar os desafios dos golpes cibernéticos e criar um espaço online mais confiável e seguro para todos.

3.3 A RESPONSABILIDADE PENAL DOS AGENTES

A responsabilidade penal dos agentes envolvidos em crimes cibernéticos é um tema de grande relevância no contexto jurídico atual, uma vez que a crescente digitalização e o uso intensivo da tecnologia refletem a multiplicação de crimes que ocorrem no ambiente virtual, esses delitos variam de fraudes e invasões de privacidade a ataques de ransomware e disseminação de malware, trazendo à tona a necessidade de uma discussão aprofundada sobre a imputabilidade penal.

É fundamental entender que a responsabilidade penal envolve a possibilidade de um agente ser responsabilizado por suas ações em função de comportamentos que atentem contra a lei, no que diz respeito aos crimes cibernéticos, a tipificação destes delitos é de extrema importância para garantir que os responsáveis possam ser processados e punidos de acordo com a gravidade de suas ações.

Os crimes cibernéticos, em sua essência, são cometidos com o uso de computadores ou sistemas de informação. Isso inclui não apenas o ataque a redes e dados, mas também a utilização de dispositivos para fraudes financeiras e a invasão

da intimidade de indivíduos, como é o caso do hacking, cada um desses atos traz consigo uma responsabilidade penal que deve ser considerada.

De acordo com os códigos penais de diversos países, as penas para crimes cibernéticos podem variar bastante, enquanto alguns países possuem legislações específicas que tipificam e penalizam tais delitos, outros ainda se baseiam em legislações mais gerais e antigas que não contemplam adequadamente as particularidades do ambiente virtual, isso acaba gerando lacunas legais que podem ser exploradas pelos infratores.

Um dos desafios da responsabilidade penal em crimes cibernéticos é a identificação dos agentes, no mundo digital, é comum que os criminosos utilizem métodos para ocultar suas identidades, como o uso de VPNs, endereços IP falsificados e criptomoeda, dificultando a localização e a responsabilização dos autores, esse anonimato pode levar a um ambiente de impunidade, onde os criminosos se sentem encorajados a agir.

Quando os agentes de crimes cibernéticos são identificados, é imprescindível que a legislação estabeleça claramente quais são as consequências de suas ações, a tipificação adequada dos delitos cibernéticos não só ajuda na responsabilização dos infratores, mas também serve como medida preventiva, inibindo futuras condutas delituosas, assim, a criação e atualização constante de leis específicas é vital.

Além disso, a responsabilidade penal não recai apenas sobre o agente individual que comete o delito, em muitos casos, haverá a responsabilização de empresas ou organizações que falham em adotar medidas de segurança adequadas, se uma empresa negligenciar sua obrigação de proteger dados de clientes, poderá ser responsabilizada por danos causados por um crime cibernético.

A responsabilidade penal por crimes cibernéticos também levanta questões sobre a tentativa e a conivência, em algumas situações, um indivíduo pode não ter concluído o ato criminoso, mas ainda assim ser responsabilizado pela tentativa, da mesma forma, aqueles que auxiliam ou encobrem ações criminosas podem ser considerados coautores do delito, mesmo que não estejam diretamente envolvidos no ato final.

Um aspecto importante a considerar é o direito à defesa do acusado. Agentes que são acusados de crimes cibernéticos têm direito a um processo justo, o que implica a possibilidade de provar sua inocência ou contestar as provas apresentadas contra si, essa é uma garantia fundamental em qualquer sistema jurídico, mas pode se tornar complexa em casos que envolvem tecnologia e manipulação de sistemas digitais.

A aplicação de penas para crimes cibernéticos, assim como em qualquer esfera de conduta criminosa, deve levar em consideração diversos fatores, como a gravidade do crime, o impacto social e econômico, e as circunstâncias pessoais do agente, o princípio da proporcionalidade é essencial para garantir que as sanções aplicadas sejam justas e adequadas ao caso específico.

Além do aspecto punitivo, a responsabilidade penal também deve contemplar a possibilidade de reabilitação do agente, os programas que ofereçam educação e reintegração social podem ser aplicados em casos de delitos não violentos, facilitando uma segunda chance e, ao mesmo tempo, desencorajando a reincidência.

A cooperação internacional é outro ponto fundamental na luta contra crimes cibernéticos. Devido à natureza global da internet, muitos crimes têm ramificações que atravessam fronteiras nacionais, a colaboração entre diferentes jurisdições é essencial para investigar e processar indivíduos que operam em escala internacional, além de assegurar que normas penais e mecanismos de extradição estejam harmonizados.

No Brasil, os delitos cibernéticos tornaram-se uma realidade mais evidente a partir de 2012, quando o Código Penal foi modificado pela Lei nº 12.737, a qual introduziu os artigos 154-A, 154-B, 266 e 298, marcando a aprovação da norma conhecida como “Lei Carolina Dieckman”.

A investigação e a penalização dos crimes cibernéticos ganharam importância, especialmente pelo fato de as legislações relacionadas a esses assuntos serem ainda recentes, vale ressaltar que somente em 2012 foi promulgada a primeira legislação a tratar especificamente dos delitos cibernéticos, a Lei nº 12.737/2012, que

reformulou o Código Penal em resposta ao caso do vazamento de fotos íntimas da atriz Carolina Dieckman.

Barbosa aponta que:

> [...] mais recentemente, foi sancionada a lei n 14.155/2021, buscando sanções mais rígidas para aqueles que praticam delitos cibernéticos, a qual deu nova redação ao Código Penal para estabelecer a agravante para o furto qualificado por meio eletrônico, com ou sem violação do mecanismo de segurança ou utilização de programa malicioso, ou qualquer outro meio fraudulento similar, apenado com pena de reclusão de quatro a oito anos e multa. (BARBOSA, 2023, p. 22).

A Lei nº 12.737/2012 representa um significativo progresso no sistema jurídico brasileiro ao lidar com os crimes cibernéticos, essa legislação estipula penas de reclusão que variam de seis meses a dois anos para indivíduos que obtenham segredos comerciais e industriais ou informações privadas mediante a violação de sistemas de segurança de equipamentos de informática.

Babosa elucida que:

> [...] a lei nº 12.965/2014, introduziu o Marco Civil da Internet e ainda que não trate especificamente dos crimes cibernéticos, no Brasil, encontra previsão no Código Penal nas Leis 12.735 e 12.737 de 2012. É este o diploma legal que trata de crimes informáticos. Logo, contribui para o acesso a informações que auxiliam na apuração da autoria de crimes cibernéticos, cometidos na seara do aparente anonimato. (BARBOSA, 2023, p. 20).

Além disso, a norma também pune quem controlar remotamente um dispositivo conectado à internet sem a devida autorização, com a possibilidade de aumentar a pena em 1/3 a 2/3 se houver a divulgação, comercialização ou transmissão dessas informações para terceiros, vale ressaltar que também será considerado crime "aquele que criar, oferecer, distribuir, vender ou divulgar um software destinado a facilitar a invasão de computadores ou dispositivos como smartphones e tablets".

Barbosa explica que:

> [...] não poderia se falar em invasão, quando o proprietário consentindo ou não, autorizasse a entrada do agente, como, por exemplo, o que ocorre quando o agente envia e-mails ou instala vulnerabilidades, onde o próprio proprietário do dispositivo instala realizando uma suposta autorização de acesso. Contudo, e como sabido, há situações em que o consentimento se dá de forma consciente. (BARBOSA, 2023, p. 20).

Da mesma maneira, a pena será majorada de um sexto a um terço caso a invasão cause danos econômicos; e será acrescida de um terço até a metade se o

delito for cometido contra figuras públicas, incluindo a presidente da República, governadores, entre outros.

Barbosa conclui que:

> Resta claro, do aqui exposto, que a punição dos crimes cibernéticos no Brasil caminha a lentos passos, pois enquanto as novas tecnologias ganham espaço a cada dia, tornando a internet um terreno fértil para a prática dos mais diversos delitos, a atividade legislativa não consegue acompanhar, sendo a regulamentação ainda incipiente, evidenciando os desafios para a efetiva responsabilização criminal dos responsáveis. (BARBOSA, 2023, p. 22).

A responsabilidade penal também deve incluir a proteção das vítimas, muitas vezes, os crimes cibernéticos causam danos significativos e duradouros a indivíduos e empresas portanto, é fundamental que o sistema jurídico não apenas puna os infratores, mas também ofereça suporte às vítimas, facilitando seu acesso à justiça e à reparação pelos danos sofridos.

3.3.3 PROPOSTAS DE POLÍTICAS PÚBLICAS PARA COMBATER GOLPES CIBERNÉTICOS

A crescente incidência de golpes cibernéticos tem levantado a necessidade urgente de políticas públicas eficazes para proteger cidadãos, empresas e instituições o desenvolvimento de uma estratégia abrangente para combater esses crimes é vital para garantir a segurança digital e a integridade das informações, assim, as propostas de políticas públicas devem ser elaboradas para atender a vários aspectos do problema.

Santos esclarece que:

> No Brasil, há um planejamento jurídico para regular e disciplinar a matéria e as leis trazem, entre outros pontos, a tipificação de atitudes empreendidas dos aparelhos e sistemas informáticos, significados de alguns termos importantes a análise dos casos concretos, garantias, direitos e deveres dos usuários e prestadores de serviços, e alguns princípios norteadores. (SANTOS, 2020, p. 07).

Uma das primeiras medidas a serem implementadas é a criação de campanhas de conscientização sobre segurança cibernética, essas campanhas teriam como objetivo educar o público geral sobre os riscos associados ao uso da internet, métodos comuns de fraudes e boas práticas de segurança online, a promoção de eventos, workshops e a distribuição de materiais informativos pode

ajudar os cidadãos a se tornarem mais críticos e cautelosos em suas interações digitais.

Santos explica que:

> Políticas Públicas são ferramentas de ação definidas como elo entre a teoria apresentada pelo Estado e sua eficácia perante a sociedade, tratando de pautas referentes a assuntos que possuem significativa relevância social em um determinado tempo e espaço. (SANTOS, 2020, p. 16).

Além disso, a formação de parcerias entre o governo, o setor privado e organizações não governamentais (ONGs) é fundamental, a colaboração pode facilitar a troca de informações sobre ameaças emergentes, métodos de ataque e técnicas de defesa, por meio dessas parcerias, seria possível criar uma rede de segurança cibernética que unisse expertise e recursos de diferentes setores para enfrentar os desafios impostos pelos golpistas.

Uma proposta fundamental é a atualização e adequação da legislação relacionada a crimes cibernéticos, muitas legislações existentes não acompanham a velocidade das inovações tecnológicas e os métodos utilizados pelos criminosos, a criação de um marco legal específico que aborde fraudes online, phishing, ransomware e outras práticas delituosas é essencial para permitir que as autoridades processem e punam adequadamente os infratores.

A capacitação de profissionais em cibersegurança também deve ser uma prioridade nas políticas públicas, investir em programas de formação e certificação para policiais, promotores e juízes é fundamental para garantir que as autoridades responsáveis pela aplicação da lei tenham o conhecimento necessário para lidar com crimes cibernéticos, a inclusão de disciplinas de segurança digital nas escolas e universidades também pode contribuir para a formação de uma nova geração de especialistas na área.

Outro aspecto importante é o fortalecimento das ferramentas de denúncia e apoio às vítimas de golpes cibernéticos, estabelecer linhas diretas de comunicação, centros de apoio e plataformas digitais para relatar incidentes pode encorajar as vítimas a se manifestar e buscar ajuda, além disso, o atendimento rápido e eficiente às denúncias é fundamental para a coleta de evidências e para a identificação de padrões de criminalidade.

Santos acredita que:

> [...] o Direito Penal apresenta dificuldades para se moldar aos crimes cibernéticos, pois não consegue acompanhar a rapidez com que a tecnologia evolui e o surgimento de novas infrações, já que suas regras foram desenvolvidas baseando-se em outro tipo de ambiente, com outros bens jurídicos sendo objeto de proteção e com outras formas de transgressão das normas, o que tem resultado hoje, em um ambiente desregrado e sem fronteiras, no qual os usuários se sentem impunes independentemente de suas condutas. (SANTOS, 2020, p. 09).

A promoção de investimentos em tecnologia e infraestrutura de cibersegurança também deve ser considerada nas propostas de políticas públicas, os governos precisam apoiar o desenvolvimento de soluções inovadoras que protejam as informações de cidadãos e empresas, isso pode incluir a implementação de sistemas robustos de proteção de dados e a adoção de tecnologias emergentes, como inteligência artificial, para identificar e responder a ameaças em tempo real.

A implementação de medidas de segurança nas empresas, especialmente aquelas que lidam com grandes volumes de dados, é outra proposta importante, criar incentivos para que as empresas adotem práticas de segurança robustas e cumpram regulamentações de proteção de dados pode ajudar a minimizar os riscos de ataques cibernéticos, os programas de auditoria e certificação de segurança podem garantir que as empresas estejam atualizadas em relação às melhores práticas do setor.

Além disso, as políticas públicas devem considerar a importância da cooperação internacional na luta contra os golpes cibernéticos, já que muitos destaques operam em escala global, o trabalho conjunto entre países para o compartilhamento de informações e o fortalecimento das regras de extradição pode melhorar significativamente a eficácia das investigações, a criação de redes internacionais de cibersegurança pode facilitar a resposta rápida a incidentes que atravessam fronteiras.

A própria ONU (2024) acredita que: “[...] é fundamental componente de apoio e assistência técnica no acesso a dados e evidencias eletrônicas para a responsabilização dos que cometem crimes no espaço cibernético”.

A implementação de políticas públicas eficazes para combater os golpes cibernéticos é um trabalho em andamento que requer constante avaliação e adaptação. A tecnologia está em evolução rápida, assim como as táticas empregadas pelos criminosos, portanto, é essencial que os formuladores de políticas mantenham um diálogo contínuo com especialistas e a sociedade civil, garantindo que as medidas adotadas permaneçam relevantes e eficazes na proteção contra ameaças

cibernéticas, esse esforço colaborativo não apenas protege os indivíduos, mas também ajuda a construir uma sociedade digital mais segura e resiliente.

CONCLUSÃO

A análise dos golpes cibernéticos revela um fenômeno complexo e multifacetado que afeta profundamente tanto as vítimas quanto a sociedade como um todo. A definição e os diversos tipos de golpes cibernéticos, juntamente com os mecanismos de atração utilizados para capturar as vítimas, demonstram a sofisticação crescente das táticas empregadas pelos criminosos.

Esses golpes não apenas resultam em perdas financeiras, mas também desencadeiam uma série de impactos psicológicos significativos. As vítimas frequentemente enfrentam o desenvolvimento de transtornos psicológicos, como ansiedade e depressão, que, por sua vez, tornam o processo de recuperação um desafio que demanda suporte psicológico adequado.

Além dos efeitos individuais sobre a saúde mental, os golpes cibernéticos têm repercussões sociais amplas. O sentimento de insegurança e desconfiança gerado por essas fraudes denota a fragilidade das interações sociais em um mundo cada vez mais digital, onde as relações humanas estão mediadas por telas e dispositivos.

A responsabilidade penal dos agentes envolvidos nas fraudes cibernéticas se torna um ponto crucial nesse contexto, pois a fiscalização e punição adequadas não apenas visam a reparação para as vítimas, mas também a dissuasão de futuras infrações.

A implementação de políticas públicas eficazes para combater os golpes cibernéticos é uma necessidade urgente. Inspirar a conscientização pública, promover a educação digital e fortalecer a legislação são passos essenciais para garantir um ambiente online mais seguro.

A união de esforços entre governos, empresas e a sociedade civil é fundamental para construir um futuro em que os riscos associados ao mundo digital sejam minimizados e em que as vítimas recebam o suporte necessário para se recuperar de suas experiências. Em suma, é necessário um esforço coletivo para enfrentar os desafios impostos pelos golpes cibernéticos, promovendo a segurança, a responsabilidade e o bem-estar social no ambiente digital.

REFERÊNCIAS BIBLIOGRÁFICAS

ABIN. **Engenharia Social:** Guia para proteção de conhecimentos sensíveis. 2021.

ALVES. Mateus de Araujo. **Crimes Digitais:** Análise da criminalidade digital sob a perspectiva do direito processual penal e do instituto da prova. São Paulo: Ed. Dialética, 2020.

ALVES, Marisa de Abreu. **Estresse:** 10 impactos causados por traumas na vida de uma pessoa. Disponível em: https://www.marisapsicologa.com.br/estresse.html. Acessado em: 18/08/2024.

BARBOSA, Mariely Ribeiro. **Crime Cibernético e a vulnerabilidade da pessoa idosa na rede mundial de computadores.** PUC-GO: Artigo científico. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/3849/1/MARIELY%20RIBEIRO%20BARBOSA.pdf. Acessado em: 18/08/2024.

BARNHILL, John. **Transtorno de Estresse pós-traumático (TEPT).** Disponível em: https://www.msdmanuals.com/pt-br/profissional/transtornos-psiqui%C3%A1tricos/ansiedade-e-transtornos-relacionados-a-estressores/transtorno-de-estresse-p%C3%B3s-traum%C3%A1tico-tept. Acessado em: 18/08/2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acessado em: 18/08/2024.

BRASIL. Decreto Lei nº 3.689 de 03 de outubro de 1941. **Código de Processo Penal**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm Acessado em: 19/08/2024.

BRASIL. Decreto Lei nº 2.848 de 07 de dezembro de 1940. **Código Penal**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm Acessado em: 19/08/2024.

COLAÇO, Janize. **Golpes Financeiros:** Fraude via WhatsApp explode em 5 anos. Veja como se proteger. Disponível em: https://einvestidor.estadao.com.br/educacao-financeira/golpes-whatsapp-estelionato-virtual-vitimas-seguro/. Acessado em: 18/08/2024.

DEUS, Pérsio de; MUNHOS, Rafael. **Transtorno do estresse pós-traumáticos (TEPT):** Sintomas e Tratamentos. Disponível em: https://www.minhavida.com.br/saude/temas/transtorno-do-estresse-pos-traumatico Acessado em: 18/08/2024.

FEBRABAN. Por que tantas pessoas caem em golpes financeiros? Disponível em: https://meubolsoemdia.com.br/Materias/porque-cair-em-golpe. Acessado em: 18/08/2024.

JOHNSTONE Mike; PSAROULIS Geórgia. **As armas Psicológicas que os golpistas usam, e como se proteger delas**. Disponível em: https://www.bbc.com/portuguese/articles/cn4nv22p6rlo Artigo Publicado na BBC. de Mike Johnstone e Geórgia Psaroulis, da Edith Cowan University, 2024. Acessado em: 18/08/2024.

KASPERSKY. **O que são golpes em aplicativos de namoro e como evita-los**. Disponível em: https://www.kaspersky.com.br/resource-center/threats/beware-online-dating-scams Acessado em: 18/08/2024.

MPSP. **Roteiro de Atuação:** Crimes Cibernéticos. 3ª ed. 2016. Disponível em: https://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Biblioteca_Virtual/Livros_Digitais/MPF%203186_Crimes_Ciberneticos_2016.pdf. Acessado em: 18/08/2024.

NOGUEIRA, Hamilton. **Golpes Virtuais:** 1,8 milhão de vítimas no Brasil em 2023. Disponível em: https://www.opovo.com.br/noticias/tecnologia/opovotecnologia/2024/09/09/golpes-virtuais-18-milhao-de-vitimas-no-brasil-em-2023.html. Acessado em: 18/08/2024.

OLIVEIRA, Wellington Antério de. **Os crimes cibernéticos e a prática do estelionato por meios eletrônicos**. Artigo Científico da Universidade São Judas Tadeu. Disponível em: https://repositorio.animaeducacao.com.br/bitstreams/2cf07f88-c42b-4798-9f9e-3d701824f60f/download. Acessado em: 18/08/2024.

ONU. **Proposta de convenção quer criar estrutura legal contra crimes cibernéticos**. Disponível em: https://news.un.org/pt/story/2024/08/1835991 acessado em: 19/08/2024.

ROQUE, Sérgio Marcos. **Criminalidade Informática**: Crimes e criminosos do computador. São Paulo: ADPESP, 2007.

ROSA, Fabrízio. **Crimes de Informática**. Campinas: Ed. Bokseller. 2002.

SÁ, Lucas das Mercês. **Violência nas Redes:** Impactos legais e psicológicos. RevistaIbero Americana de Humanidades, Ciências e Educação. Disponível em: https://doi.org/10.51891/rease.v9i10.12408. Acessado em: 18/08/2024.

SANTOS, Liara Ruff; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. **O Cibercrime e o direito a segurança jurídica:** Uma análise da legislação vigente no cenário brasileiro, 2020.

SANTOS, Letícia Dutra de Oliveira. **Políticas Públicas de educação digital:** Prevenção e combate aos crimes cibernéticos. Disponível em: http://repositorio.aee.edu.br/bitstream/aee/10044/1/LET%C3%8DCIA%20DUTRA%20DE%20OLIVEIRA%20SANTOS.pdf Acessado em: 19/08/2024.

SILVA. Gilsimar Pinheiro da. **Crimes Digitais:** Evolução dos crimes e a aplicação do direito. Universidade 2021. Potiguar: Artigo científico. Disponível em:

https://repositorio.animaeducacao.com.br/bitstreams/65597262-4fec-4790-8267-65d7f57bb5ed/download Acessado em: 18/08/2024.

TOCANTINS, Hortência Matos. **Crimes Cibernéticos na atualidade**: Desafios e impactos na sociedade moderna. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-na-atualidade-desafios-e-impactos-na-sociedade-moderna/2104354886. Acessado em: 18/08/2024.

PONTIFICIA UNIVERSIDADE CATÓLICA DE GOIAS
PRÓ-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
TRABALHO DE CURSO I E II – JUR 1051 E JUR 1052

TERMO DE AUTORIZAÇÃO DE PUBLICAÇÃO DE PRODUÇÃO ACADÊMICA

O(A) estudante Guilherme Araújo Silva
do Curso de Direito, matrícula 2020100010263-6
telefone: 62 99306-0102, e-mail guilhermesilva2103@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado Os impactos psicológicos e sociais nos golpes cibernéticos nas vítimas sob responsabilidade no Direito Penal., gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JEPG): Som (WAVE, MPEG, AIFF, SNS); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 20 de março de 2025.

Assinatura do(s): autor(es): Guilherme Araújo Silva

Nome completo do autor: Guilherme Araújo Silva.

Assinatura do professor- orientador:

Nome completo do professor-orientador: Cesar Costa de Paula