EVOLUÇÃO DOS CRIMES CIBERNÉTICOS NA PANDEMIA

Orismar Teixeira dos Santos
Universidade Federal de Mato Grosso do Sul (UFMS/CPNA)
E-mail: orismar1902@gmail.com

Nathalia Pereira Nunes
Universidade Federal de Mato Grosso do Sul (UFMS/CPNA)
E-mail: nathnunees55@gmail.com

RESUMO

A humanidade passou por grandes avanços tecnológicos ao longo do tempo, sendo a internet, um dos maiores. Possui alta capacidade de comunicação e integração social, de nível global, e com uma conectividade praticamente instantânea. No entanto, apesar dos seus inúmeros benefícios, traz consigo perigos, como os crimes cibernéticos (cibercrime), que tem tomado grandes proporções a cada ano. Durante o período de pandemia do Covid-19 foram adotadas medidas de isolamento social, e boa parte dos trabalhadores puderam executar suas atividades remotamente, na modalidade *home office*, propiciando um aumento massivo de aparelhos informáticos conectados simultaneamente, favorecendo ainda mais a prática do cibercrime. Este trabalho tem como objetivo mostrar o contexto histórico do crime cibernético; examinar as legislações dos crimes digitais e a proteção no âmbito digital; analisar os crimes digitais ocorridos na pandemia, e evidenciar a exposição aos mais diversos tipos de riscos ao acessar redes desconhecidas, ou compartilhar informações sem a adesão de medidas adequadas de segurança. Para desenvolvimento deste trabalho foi realizada uma pesquisa bibliográfica, e pesquisa documental. Neste estudo foi possível observar a fragilidade e vulnerabilidade dos usuários dessas tecnologias, sendo que a maior parte dos crimes virtuais ocorre por meio do *phishing*, utilizando-se de engenharia social. É possível concluir também como a interação digital sem o devido cuidado e segurança, contribuí para um aumento significativo de delitos digitais.

Palavras-chave: Crimes Cibernéticos; Internet; Pandemia; TCIs.

ABSTRACT

Humanity has undergone great technological advances over time, with the internet being one of the greatest. It has a high capacity for communication and social integration, at a global level, and with virtually instantaneous connectivity. However, despite its numerous benefits, it brings with it dangers, such as cybercrime, which has taken on huge proportions each year. During the period of the Covid-19 pandemic, social isolation measures were adopted, and most workers were able to carry out their activities remotely, in the home office modality, providing a massive increase in simultaneously connected computer devices, further favoring the practice of cybercrime. This work aims to show the historical context of cybercrime; examine digital crime legislation and protection in the digital realm; analyze the digital crimes that occurred during

the pandemic, and highlight exposure to the most diverse types of risks when accessing unknown networks, or sharing information without adhering to adequate security measures. For the development of this work, a bibliographical and documental research was carried out. In this study, it was possible to observe the fragility and vulnerability of the users of these technologies, and most of the virtual crimes occur through phishing, using social engineering. It is also possible to conclude that digital interaction without due care and security has contributed to a significant increase in digital crimes.

Keywords: Cybercrime; Internet; Pandemic; TCIs.

1. INTRODUÇÃO

A cibercriminalidade se deu originalmente em uma necessidade de obter informações sigilosas, dando origem aos primeiros especialistas com capacidades em quebrar códigos criptografados da história.

Segundo Aras (2001), são empregadas várias nomenclaturas para nomear os atos ilícitos virtuais, com uma maior recorrência dos termos crimes informáticos ou crimes de informática, ou cibercrime. Crimes telemáticos ou cibercrime são expressões mais apropriadas para nomear as infrações que atingem redes de computadores à internet, ou quem a usa como meio para praticar tais atos criminosos.

A sociedade em consequência do avanço da tecnologia e a globalização contemporânea intensificada, se beneficiou do aperfeiçoamento da internet e meios de comunicações, que possibilitaram a sua modernização, permitindo facilidades, comodidades e agilidades, jamais previstas. A interação humana se intensificou de tal maneira que reformulou por completo o seu modo de acessibilidade à informação.

Com o acesso à informação sendo aprimorado, simultaneamente também ocasionou a propagação de condutas criminosas, afetando a segurança social e financeira das vítimas, os cibercrimes são cometidos por criminosos que aproveitam do anonimato do meio digital para utilizar e desenvolver ferramentas como: *malware*, *ransomware*, *spyware*, entre outras, em conjunto com uma rede de computadores ou mesmo dispositivos celulares conectados a uma rede de internet, para encontrar brechas nos *hardwares* ou *softwares* e assim poderem praticar seus crimes, sem se importarem com a natureza de suas vítimas sejam elas pessoas físicas ou jurídicas, órgãos governamentais entre outros.

De acordo com Alves (2020), a internet propiciou a geração de um novo perfil de criminoso que com conhecimentos técnicos em informática consideráveis, conduziram a maneira de execução dos delitos convencionais para moldes mais tecnológicos. Os *hackers* são exemplos de praticantes deste tipo de delito, mas não é algo que se deva generalizar, pois é um termo genérico e pejorativo, haja visto que existem *hackers* que utilizam do seu conhecimento para praticar boas ações, sendo contratados pelas próprias organizações para melhorem os seus sistemas de segurança, encontrando seus pontos de vulnerabilidade para que possam impedir

roubos de identidade e informações sigilosas, ou outros tipos de crimes cibernéticos, antes que outros criminosos percebam as falhas em seu sistema.

Se torna um desafio tentar equilibrar à cultura do compartilhamento, da socialização, da criação de conteúdo e às questões de proteção, segurança, confidencialidade e privacidade. Quanto mais tecnologia integramos em nosso cotidiano, torna-se essencial que possamos ter conhecimento de elementos virtuais para suportar toda essa modernização (SYDOW, 2009). Nas palavras de Canongia e Júnior (2009) a respeito das tecnologias da informação e da comunicação (TICs):

> É marcante a presença da alta tecnologia atrelada a constantes inovações com o domínio das empresas de países desenvolvidos. Esta convergência tecnológica vem nos bombardeando com novidades inimagináveis, como, por exemplo, o acesso à internet pelo celular, permitindo o envio de e-mails, a realização de transações financeiras, além de múltiplas aplicações, serviços e negócios que as TICs vêm proporcionando, e que são crescentes mundialmente.

É essencial assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações que circulam e são transmitidas pela rede. São necessárias mudanças e adequações na legislação que não acompanham tamanha complexidade e velocidade digital, não garantindo a segurança e proteção aos milhões de usuários das redes, que acabam se tornando presas fáceis e suscetíveis as mais variadas categorias de crimes cibernéticos. No Brasil, não existem leis específicas para crimes nessa categoria, contudo, dispõe de legislações que tipificam tais atos criminosos, prevendo suas penas.

Conforme levantamento da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), publicada no portal do governo brasileiro, o Brasil ocupa a 5ª posição no *ranking* mundial de países que mais consomem internet com 78,3% da população brasileira estando conectada à rede de internet (BRASIL, 2021). Por consequência, na proporção que os números progridem, a probabilidade de ocorrerem incidências de cibercrimes é na mesma proporção, sendo essencial que os usuários estejam atentos para que não sejam vítimas de tais atos.

O presente trabalho tem como objetivo mostrar o contexto histórico do crime cibernético; examinar as legislações aos crimes digitais e à proteção no âmbito digital; analisar os crimes digitais ocorridos na pandemia, evidenciando como a interação digital sem o devido cuidado e segurança, contribuí para um aumento significativo desses delitos no meio digital.

2. METODOLOGIA

No desenvolvimento deste trabalho foi realizada uma pesquisa bibliográfica, e pesquisa documental. Para Marconi e Lakatos (2019), a pesquisa bibliográfica usa de diferentes fontes de documentos que exigem do pesquisador a manipulação e procedimentos investigativos diferentes e compreende oito fases distintas: escolha do tema; elaboração do plano de trabalho; identificação; localização; compilação; fichamento; análise e interpretação; redação. A análise documental busca identificar informações factuais nos documentos a partir de questões e hipóteses de interesse (CAULLEY apud LÜDKE e ANDRE, 1986).

3. CONTEXTO HISTÓRICO DOS CRIMES CIBERNÉTICOS

No intuito de compreender a ligação existente entre a internet e os crimes digitais, é necessário abranger eventos notórios da respectiva história da internet e do uso da criptografia, em alguns aspectos.

A criptografia pode ser conceituada na prática de esconder ou mascarar informações através de uma linguagem codificada, protegendo-as para que possam ser visualizadas somente pelo seu emissor e destinatário. Existem relatos do uso dessa tática desde o período dos conflitos entre os Gregos e Persas devido às suas necessidades de transmitirem informações sigilosas, ocultando-as de forma que somente o seu destinatário seria capaz de compreender e decifrar seu conteúdo. Ao tentar realizar a quebra desse sigilo, entende-se que a cibercriminalidade se originou dessa necessidade de obter informações confidenciais.

Ao longo da Segunda Guerra Mundial, Alan Turing, cientista, matemático e criptoanalista britânico, conhecido como "pai da computação", tornou-se eventualmente o criador de uma série de técnicas capazes de quebrar os códigos usados pela rede de inteligência alemã. Alan Turing foi o maior responsável pelo avanço da ciência criptográfica, sendo diretamente responsável pelo aperfeiçoamento dos sistemas usados na época, com os avanços na criptografia apresentou os primeiros vislumbres do que seria conhecida como internet.

Os primeiros casos de crimes informáticos, tiveram ocorrência em meados da década de 1960, eram delitos de manipulação, sabotagem, espionagem ou abuso de computadores. Em meados da década de 1980, com as novas transformações no âmbito social e econômico, começou um aumento de ações criminosas na internet, refletindo em manipulações de caixas bancários, pirataria de programa e pornografia infantil, abusos de telecomunicação, fatores que começaram preocupar os cidadãos da época (OLIVEIRA JÚNIOR, 2013).

Somente ao final da década de 1990, o termo "cibercrime" se tornou notório, durante uma reunião do G-8 onde foi discutido como combater as práticas ilícitas na internet, e quais a possíveis prevenções e punições a serem adotadas. A partir desta reunião, o termo começou a ser empregado para designar infrações penais praticadas no meio digital. A evolução destes crimes está em paralelo com a evolução constante da tecnologia, dificultando bastante o combate desses crimes. De acordo com Pinheiro (2000):

> Com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente se percebe que nem todos a utilizam de maneira sensata e, acreditando que a internet um espaço livre, acabam por e ceder em suas condutas e criando novas modalidades de delito: os crimes virtuais.

Segundo Zanellato (2002), a internet é um suporte ou meio que permite a troca de correspondência, arquivos, ideias, comunicação em tempo real e compras de produtos. É uma rede de escala mundial de armazenamento, dados e informações de milhões de pessoas de todo o mundo.

A utilização da engenharia social não é restrita ao universo da tecnologia de informação, o crescimento do mundo digital possibilitou sua aplicação como estratégia de consecução de

informações relevantes, tanto de pessoas quanto de empresas. As práticas que utilizam são estratégias de persuasão, manipulação e influenciada pela conduta humana para obtenção dessas informações sigilosas de enorme valor (LOTUFO, 2021).

De acordo com Tupinambá (2021), as ações criminosas dentro do ambiente digital possuem um modus operandi, técnicas além da engenharia social que são amplamente utilizadas para obtenção de informações. Uma das mais aplicadas é o chamado *phishing* ou *phishing scam* que teve seu início na década de 1990 e considerado ainda o mais expressivo meio de ataque e fraudes digitais, sendo executado em sua maioria por meio de e-mail, mais atualmente, SMS, redes sociais, páginas da web, aplicativos maliciosos, documentos digitais ou outro meio digital que permita a execução dessa "pescaria".

Outra técnica delituosa utilizada pelos criminosos é o *malware* um *software* malicioso que tem como objetivo a obtenção de informações importantes, além da capacidade de controlar a máquina, servidor, dispositivo, como também a rede vinculada de modo remoto. Nos dias atuais, o propósito da aplicação do *malware* é o sequestro de informações com pedidos de resgate, o que caracteriza a extorsão, entre outros objetivos (TUPINAMBÁ, 2021).

As informações digitais são na maioria das vezes o propósito desses criminosos, utilizando infinidades de espécies de *malware*, tais como *spyware*, código espião, identificados como *keyloggers*. Conforme Jesus e Milagre (2016), *keyloggers* são responsáveis por gravar dados digitados pelos usuários ao acessarem normalmente sites como do internet *banking* ou de comércio eletrônico.

De acordo com CERT.BR (2012), *ransomware* é um tipo de código malicioso, *malware* que tornam inacessíveis os dados armazenados em um equipamento, utilizando criptografia e exigindo pagamento para restabelecer o seu acesso a eles, além de infectar o equipamento, o *ransomware* também busca por outros dispositivos conectados à rede, e os criptografa. O pagamento solicitado para o resgate das informações, é via bitcoins, por serem difíceis de rastrear. Existem dois tipos de *ransomware*: o *Locker*, que impede o acesso ao equipamento infectado; e o *Crypto*, que impede o acesso aos dados armazenados no equipamento infectado geralmente, através de criptografia.

4. ASPECTO JURÍDICO

É perceptível que a jurisdição brasileira em relação aos crimes cibernéticos não acompanhou tal evolução, pois gradativamente, vão surgindo novos tipos penais, em comparação a inúmeras práticas ilegais no mundo virtual. A falta de leis especificas ou da ineficácia do sistema judiciário, dificulta a punição desses criminosos.

Os crimes digitais são considerados condutas ilícitas, sendo previstas na legislação, e praticadas com uso da tecnologia. Sendo caracterizado pelo uso de algum dispositivo digital e não a internet, apesar de ela ser um meio e está diretamente relacionada a prática dos crimes digitais. No âmbito jurista os crimes virtuais são definidos em dois tipos: os próprios e os impróprios/mistos. Os crimes digitais próprios são praticados contra os sistemas de informática e sistemas de dados, visando atacar outros computadores, servidores, como *hackers* que tentam

acessar e modificar dispositivos, programas de empresas, instituições bancárias ou órgãos governamentais. Os crimes digitais impróprios ou mistos são praticados por intermédio da tecnologia, mas com intuito de cometer outros crimes já tradicionais e previsto pela legislação, como crimes contra a honra ou pornografia infantil.

No Brasil, as questões envolvendo o direito sobre crimes cibernéticos só foram tipificadas em 2012, com a alteração do Código Penal, pela Lei n° 12.737, de 30 de Novembro de 2012 que tipificou os crimes de invasão de computadores no intuito obter vantagem ilícita, falsificação de cartões e de documentos particulares e interrupção de serviços eletrônicos de utilidade pública (BRASIL, 2012). Essa lei ficou conhecida como Lei Carolina Dieckman, a atriz brasileira que teve o seu celular invadido e suas fotos pessoais divulgadas na rede por um *hacker*. O artigo 154-A do respectivo código penal, foi inserido na lei n° 12.737/12, que estabelece:

> Art. 154-A: Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

A intenção do crime previsto do artigo 154-A do Código Penal apresenta dois centros de conduta: invadir ou instalar, basta apenas uma conduta, ainda que ocorram as duas, o agente responde por crime único. Na instalação de vulnerabilidades, deve coincidir com o propósito de obtenção de vantagem, seja econômica, como a obtenção de senhas de contas bancárias, ou, simplesmente, para romper a segurança. O artigo 154-B do respectivo código, foi inserido na lei 12.737/12, estabelece:

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

Conforme previsão do art. 154-B, a ação penal é pública condicionada à representação, exigindo-se para desencadear a persecução penal a manifestação de vontade da vítima à autoridade competente. Porém, se o crime for cometido contra a administração pública direta ou indireta da União, Estados, Distrito Federal ou Municípios e contra empresas concessionárias de serviços públicos, a ação penal será pública incondicionada.

O direito digital e a liberdade de expressão, possuem uma conexão próxima, tendo uma das relações jurídicas mais conflituosas no ambiente virtual, tendo a necessidade de apoio do direito digital. A internet durante muito tempo foi vista como uma terra sem lei, onde as pessoas poderiam ofender, ameaçar e cometer outros crimes, devido a certeza da não punição. Essa realidade mudou com a consolidação do direito digital. Na qual o Marco Civil da Internet Lei 12.965 de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. O principal fundamento, é o “respeito à liberdade de expressão”.

O Marco Civil, regulamenta o uso da rede mundial de computadores no país e reforça o direito penal para criminalizar, disciplinar e estabelecer os direitos e deveres cibernéticos.

Vigorando a Lei nº 12.965/2014, após uma sequência de ataques a *websites* oficiais do governo e empresas públicas, legislação na qual, dispõe as garantias, direitos e deveres para o uso da Internet no Brasil. Determinando e garantindo que os provedores não podem violar o direito à intimidade e vida privada dos seus usuários, não podendo monitorar os dados trafegados pela rede ou mesmo divulga-los, resguardado mediante um livre consentimento ou caso exista alguma ordem judicial. De acordo com o artigo 5º inciso X da CF/88:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Além da liberdade de expressão nos limites legais e combate a censura, tornando o ambiente virtual mais seguro e democrático para todos seus usuários sem distinção. Como é resultado nos artigos 3°, 7° e 19°:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I – garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II – proteção da privacidade.
> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei.
> Art. 19° Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

A lei tem como missão proteger os dados pessoais dos usuários disponíveis nas redes para que não sejam usados indevidamente. Garantindo aos usuários o direito de acesso ao processamento de seus dados e à responsabilidade por possíveis danos, visando garantir que sem diferenciação, esses usuários tenham uma condição digna e saudável no âmbito digital, para desenvolverem sua personalidade e exercitarem a sua cidadania.

5. CRIMES CIBERNÉTICOS NA PANDEMIA

O período de pandemia gerou preocupações com o Covid-19, crise política e econômica no país, instabilidade financeira e emocional, e a ocorrência dos crimes digitais foi mais um fator inquietante, especialmente devido a expansão do e-commerce. Procon (2022) após um levantamento de dados junto a Confederação Nacional do Comércio (CNC), relatou que em junho de 2020 houve um aumento de 73% nas vendas em e-commerce se comparado ao mesmo período de 2019, crescimento explicado pelas medidas restritivas de combate a Covid-19. Em 2021, a alta foi de 48,2% em relação a 2020, e as pequenas e médias empresas tiveram um faturamento de mais de R$ 2,3 bilhões em vendas *online*.

Conforme relatório global divulgado pela Symantec Endpoint Protection, antes da pandemia, em 2019, o Brasil ocupava o terceiro lugar no ranking dos países que sofrem mais ataques cibernéticos, ficando atrás apenas da China e dos Estados Unidos. Porém, no ano de 2020, os números de casos de ciberataques cresceram, consideravelmente. Ainda, de acordo com a Fortinet Threat Intelligence Insider Latin America, em relatório sobre ciberataques no Brasil, o país sofreu mais de 3,4 bilhões de tentativas de ataques na internet, de janeiro a setembro de 2020, conforme o site Crypto ID (PROCON ALAGOAS, 2022).

A FortiGuard Labs (2021), em relatório, mostrou que o Brasil no decorrer do ano de 2020 sofreu com 8,5 bilhões de tentativas de ataques cibernéticos, sendo 5 bilhões ocorrendo nos últimos três meses do ano (outubro, novembro e dezembro). No ano de 2021 o Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos, um crescimento de mais de 950% com relação a 2020 que foi de 8,5 bilhões. O Brasil ocupou a segunda posição em número de ataques na América Latina e Caribe, atrás apenas do México (com 156 bilhões). A alta nos índices foi contínua durante o período, e ocorrendo em toda a região, registrando até 289 bilhões de ataques no total.

Através de dados obtidos por Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos (CNDCC, 2022), os crimes de: Maus Tratos contra Animais, LGBTFobia; Neo Nazismo; Pornografia Infantil; Intolerância Religiosa; Xenofobia; Racismo; Violência ou Discriminação contra Mulheres; Tráfico de Pessoas e Apologia e Incitação a crimes contra a Vida, obtiveram em 2019, entre denúncias anônimas recebidas e processadas uma quantidade de 75.671, envolvendo 39.864 páginas (URLs) distintas, foram identificadas e removidas 24.319 páginas que estavam escritas em 9 idiomas e hospedadas em 8.015 domínios diferentes, de 161 diferentes TLDs (Lista de Domínios de Lista Superior) e conectadas à Internet através de 7.258 números IPs distintos, atribuídos para 65 países em 6 continentes.

No período de 2020, a CNDCC (2022) informou que foram recebidas e processadas 156.692 denúncias anônimas de 74.011 páginas (URLs) distintas, sendo removidas 43.316 páginas que estavam escritas em 10 idiomas e hospedadas em 9.236 domínios diferentes, de 173 diferentes TLDs e conectadas à Internet através de 8.524 números IPs distintos, atribuídos para 63 países em 6 continentes. Em 2021, foram recebidas e processadas 150.095 denúncias anônimas envolvendo 71.095 páginas (URLs) distintas, onde foram removidas 32.538 páginas escritas em 10 idiomas e hospedadas em 8.926 domínios diferentes, de 170 diferentes TLDs e conectadas à Internet através de 9.900 números IPs distintos, atribuídos para 68 países em 6 continentes.

Os crimes cibernéticos ocorrem através de *malwares* sequestrando dados, sendo distribuído por intermédio de publicidade enganosa, sites maliciosos e campanhas de *phishing* via e-mail, que tentam roubar informações para atos maliciosos ou vender a outros criminosos para ações futuras.

O *Phishing* é um dos crimes digitais mais elaborados, os criminosos criam sites, aplicativos digitais e enganando diversos usuários, das mais diferentes formas, enviando e-mail ou SMS as vítimas, com links ou arquivos contaminados, levando o usuário a acessar um site,

enganando-a para que forneça suas informações pessoais. Um exemplo atual dessa prática é a clonagem do WhatsApp onde o criminoso encaminha um código de acesso para o celular da vítima, entrando em contato com ela se passando por alguma pessoa conhecida ou empresa.

De acordo com uma pesquisa da Confederação Nacional de Dirigentes Lojistas (CNDL) e do Serviço de Proteção ao Crédito (SPC Brasil), o crescimento das compras online e avanço do uso de meios digitais em meio à pandemia de coronavírus, trouxe aumentos significativos nas fraudes ocorridas pela internet. A pesquisa foi realizada em parceria com o Sebrae, onde foram entrevistados 949 internautas com idade igual ou maior a 18 anos, de todas as classes econômicas, em todas as capitais do país, com margem de erro de 3 pontos percentuais para um intervalo de confiança de 95%. A coleta foi feita entre 15 de abril a 30 de abril de 2021. 59% dos internautas sofreram algum tipo de fraude financeira nos últimos 12 meses, contra 46% em 2019. Correspondendo a um contingente de 16,7 milhões de brasileiros (ALVARENGA, 2021).

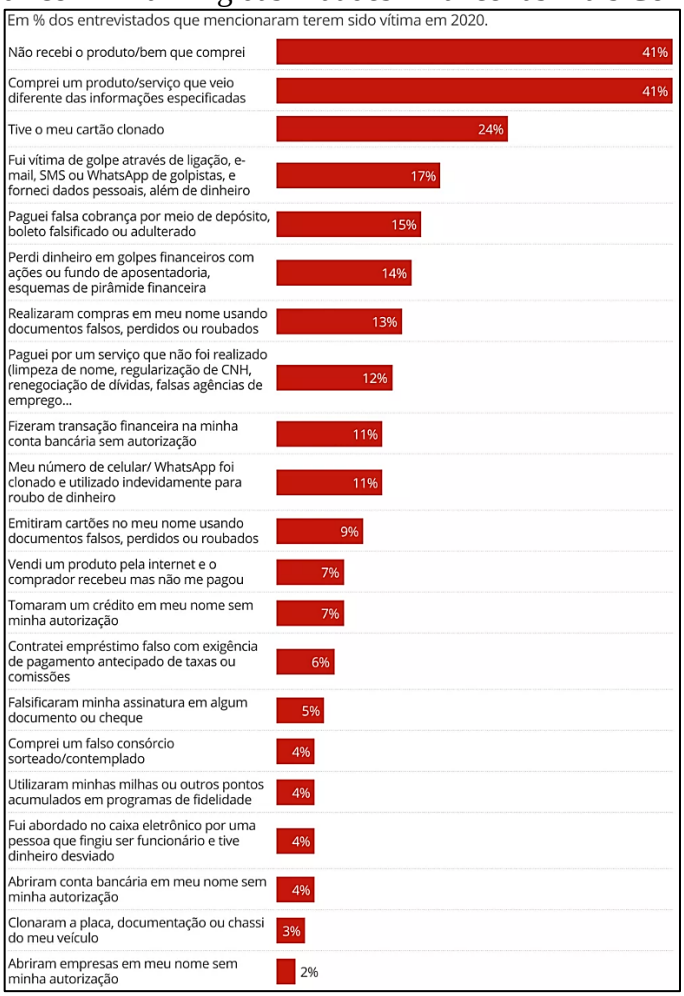
A pesquisa da CNDL e SPC Brasil mostrou que 51% das vítimas foram mulheres, 49% homens e 56% pertenciam à classe C, enquanto que 44% eram da classe A/B. A idade média dos internautas que sofreram fraude no de 2020 era de 39 anos, sendo que mais da metade das vítimas (53,6%) tem ao menos o ensino médio completo. Considerando o ranking das fraudes mais comuns, o não recebimento de produto ou serviço, a clonagem de cartão e os golpes através de ligações ou mensagens representaram as maiores porcentagens, conforme observado no Gráfico 1.

Com o estudo foi possível estimar que o prejuízo decorrente de fraudes financeiras sofridas no universo dos internautas brasileiros chegou a R$ 2,7 bilhões nos últimos 12 meses, incluídos os gastos na busca de reparação do problema. O valor médio do prejuízo por conta da fraude foi de R$ 512,4 sendo que 20% dos entrevistados mencionaram um valor acima de R$ 800 (ALVARENGA, 2021).

Dentre os principais locais onde os golpes aconteceram, as lojas online foram as que tiveram maior incidência com 38,8%, seguida pelos sites de compra e venda de produtos novos ou usados (15%), bancos (8,9%) e financeiras (7,1%).

O estudo também mostrou que as descobertas das fraudes ocorrem principalmente através do recebimento de SMS informando compras no cartão que não foram realizadas pelo titular, com 12,6%, outros 9% só descobriram compras indevidas quando no recebimento da fatura do cartão. Entre outras formas de descoberta mencionadas foram o contato de uma empresa de cobrança de dívidas (8,5%); o surgimento de valores estranhos no extrato bancário (8,3%); o não recebimento do produto comprado (7,2%) e a impossibilidade de sacar valores investidos (7%). Somente 65% dos entrevistados conseguiram recuperar ao menos uma parte da quantia que perdeu, sendo que 43% recuperaram todo o valor, percentual que cresceu 11 pontos na comparação com 2019 (32%).

Gráfico 1 – Ranking das Fraudes Financeiras Mais Comuns.



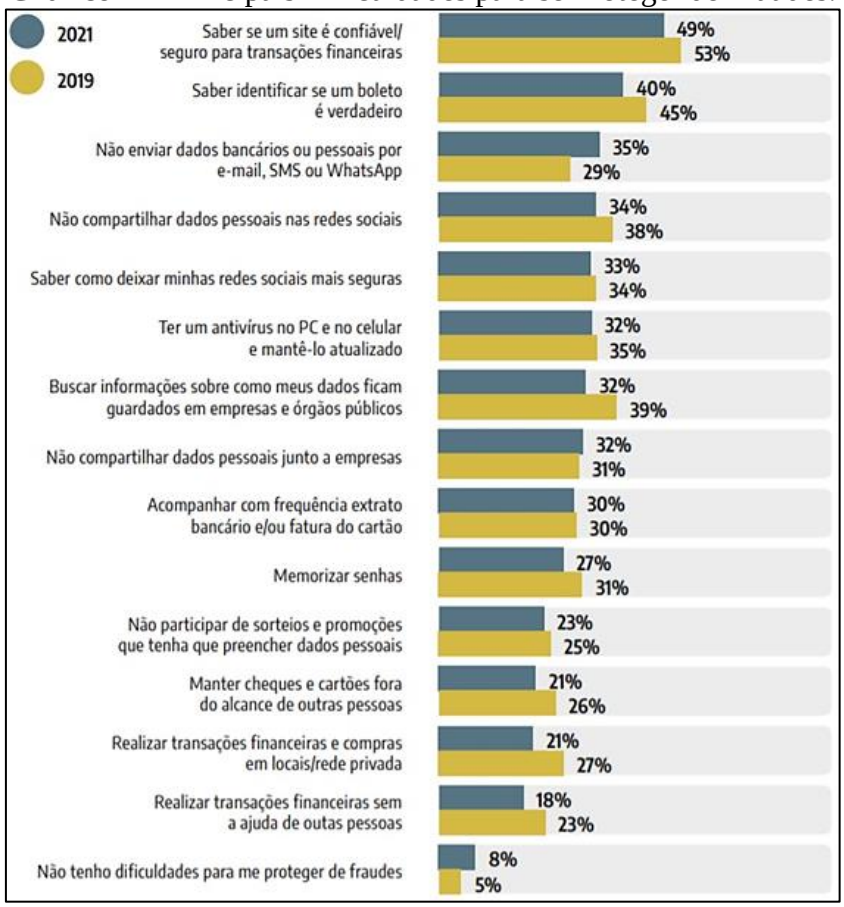
Fonte: Alvarenga (2021).

Das vítimas que sofreram fraude, a pesquisa aprontou que 27% disseram que conseguiram a resolução do problema em menos de um mês, 24% levaram entre 1 mês e seis meses, 7% resolveram num prazo entre 7 a 12 meses, e 29% ainda não conseguiram uma solução. As principais medidas adotadas para solucionar o problema e reparar os danos foram realizar contato com o banco e administradora de cartão (27%), negociação com a empresa, pessoa ou instituição financeira (18%); a abertura de boletim de ocorrência na polícia (16%); e a procura de órgão de defesa do consumidor (12%).

Outros destaques apontados pela pesquisa, mostraram que 19% dos internautas vítimas de fraude foram incluídos nos cadastros de devedores, sendo que 12% conseguiram resolver e 7% ainda permaneceram com restrição no nome; 47% relataram terem sofrido stress por causa da fraudes e 11% relataram depressão, ansiedade e outros problemas psicológicos; 92% dos consumidores admitiram dificuldades para se proteger contra fraudes financeiras; 62% dos entrevistados se consideram mais preparados para evitar esse tipo de crime após ter sofrido uma fraude; 91% das vítimas adotaram algum tipo de medida como não responder a e-mails ou telefonemas que solicitam informações pessoais (39%), não abrir mensagens de pessoas

desconhecidas ou suspeitas (37%), fazer compras somente em locais confiáveis (37%) e não compartilhar dados pessoais nas redes sociais (36%). O Gráfico 2 mostra as principais dificuldades apontadas pelos internautas para se protegerem de fraudes, relativo aos anos de 2019 e 2021:

Gráfico 2 – Principais Dificuldades para se Proteger de Fraudes.



Fonte: Alvarenga (2021).

Tais crimes executados no meio digital utilizam artifícios das técnicas de *phishing*, *malware*, *keyloggers*, engenharia social, que foram amplamente facilitadas com o desenvolvimento das TICs e o advento da rede mundial de computadores e seu avanço no cotidiano das pessoas ao redor do mundo.

6. CONSIDERAÇÕES FINAIS

Atualmente, vive-se na era da sociedade da informação, onde há dependência da tecnologia, e a segurança cibernética é um assunto de vitalidade para ser pautado nas esferas pública e privada, assim como nos âmbitos pessoal e profissional. Essa grande incidência de ataques aos usuários da internet para prática de atos ilícitos e crimes informáticos implica no fenômeno da criminalidade cibernética, que é crescente e globalizado.

O desenvolvimento das relações no ciberespaço propiciou o surgimento desse novo gênero de criminalidade, sendo impulsionado pela sensação de anonimato e liberdade que a internet e a realidade virtual proporcionam aos seus usuários, especialmente o público mais jovem. Através de um computador, é possível criar e assumir múltiplas faces, mascarando intenções, podendo qualquer pessoa com conhecimento médio de informática, ser capaz de praticar crimes que não exigem uma grande complexidade nesse mundo cibernético, delitos de furto ou injúria racial, e uso da liberdade de expressão como artifício para atacar a vida pessoal de outros indivíduos.

É possível identificar através das pesquisas realizadas, que a maior parte dos crimes virtuais ocorre por meio do *phishing*, utilizando-se de engenharia social. Os cibercriminosos aproveitam das vulnerabilidades tecnológicas e humanas das vítimas.

Os investimentos atuais em infraestrutura ainda não são suficientes para a redução dos crimes virtuais. Sendo que a conscientização dos usuários sobre os riscos do mundo digital e a orientação sobre a forma correta de utilização dos recursos tecnológicos são indispensáveis.

Fica evidente que a migração dos crimes para a esfera digital teve um aumento, e que os direitos existentes carecem de uma revisão. Cabe ao Estado atualizar sua legislação de forma a acompanhar a contínua evolução da tecnologia e dos crimes praticados por meio da rede digital, a exemplos da Lei n° 14.132, de 31 de Março de 2021, que tipificou o crime de *stalking* aumentando a proteção das vítimas que passam por este tipo de crime e da Lei nº 14.155, de 27 de Maio de 2021, que deixou mais rígidas as penas de crimes como o estelionato, reforçando a segurança dos dados pessoais nas redes, evitando que fiquem expostos à mercê de criminosos a exemplo da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709, de 14 de Agosto de 2018.

Os principais desafios no combate aos crimes cibernéticos é a punição dos infratores com a mesma eficiência que se pune àqueles que cometem crimes no mundo físico. Não existe um ambiente totalmente seguro. Quando existir um equilíbrio entre o investimento em tecnologia e a educação dos usuários, será possível utilizar os recursos tecnológicos disponíveis com maior confiança, sendo possível o melhor aproveitamento para à sociedade.

É necessário aprofundar o conhecimento sobre os meios tecnológicos, para que se tenha uma utilização saudável, adequada e segura, se atentando aos limites legais e o da nossa própria liberdade de expressão, para não violar-se nenhum direito alheio, pois como é de conhecimento comum: “o direito de um termina, onde o do outro começa”.

7. REFERÊNCIAS

ALVARENGA, Darlan. Cresce número de consumidores vítimas de fraudes financeiras no Brasil. **G1 - Globo**. Disponível em <https://g1.globo.com/economia/noticia/2021/06/24/cresce-no-de-consumidores-vitimas-de-fraudes-financeiras-no-brasil-veja-ranking-das-mais-recorrentes.ghtml#>. Acesso em: 13 out. 2022.

ALVES, Matheus de Araújo. **Crimes Digitais:** análise da criminalidade digital sob a perspectiva do Direito Processual Penal e do Instituto da Prova. Editora Dialética, 2020. 1ª ed. São Paulo, SP: Editora Dialética, 2020.

ARAS, Vladimir. **Crimes de informática:** uma nova criminalidade. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: <http://jus.com.br/artigos/2250/crimes-de-informatica>. Acesso em: 13 out. 2022.

BRASIL. **Brasil está entre os cinco países do mundo que mais usam internet.** 2021. Disponível em: <https://www.gov.br/pt-br/noticias/transito-e-transportes/2021/04/brasil-esta-entre-os-cinco-paises-do-mundo-que-mais-usam-internet>. Acesso em: 13 abr. 2023.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos.** Brasília. 2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 13 abr. 2023.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Brasília. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 13 out. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.** Brasília. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 11 abril. 2023.

BRASIL. Lei nº 14.132, de 31 de março de 2021. **Tipificando o crime de perseguição (stalking).** Brasília. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm>. Acesso em: 11 abril. 2023.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. **Crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet.** Brasília. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm>. Acesso em: 11 abril. 2023.

CANONGIA, Claudia; JUNIOR, Raphael Mandarino. **Segurança cibernética: o desafio da nova Sociedade da Informação**. Disponível em: <http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342>. Acesso em: 26 set. 2022.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança No Brasil (Org.). **Cartilha de Segurança para Internet.** 2º. ed. São Paulo: Comitê Gestor da Internet

No Brasil, 2012. 140 p. Disponível em: <https://cartilha.cert.br/livro/>. Acesso em: 14 out. 2022.

CNDCC. Central Nacional De Denúncias De Crimes Cibernéticos. **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos.** Disponível em: <https://indicadores.safernet.org.br/>. Acesso em: 14 out. 2022.

FORTIGUARD LABS. **Relatório sobre ciberataques no Brasil.** 2021. Disponível em: <https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021>. Acesso em: 28 mai. 2022.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016. 208 p.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica**. 8ª ed. São Paulo, SP: Atlas, 2019.

LEI n° 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos;** altera o Decreto-Lei n° 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União, Brasília, 30 nov. 2012.

LOTUFO, Larissa. Engenharia Social. In: SLEIMAN, Cristina et al. **Segurança digital:** proteção de dados nas empresas. São Paulo, 2021a. 247 p. cap. 7, p. 95-101.

LÜDKE, M.; ANDRÉ, M.E.D.A. **Pesquisa em educação:** abordagens qualitativas. São Paulo: EPU, 1986.

PINHEIRO, Reginaldo César. **Os cybercrimes na esfera jurídica brasileira.** Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 5, n. 44, 1 ago. 2000. Disponível em: <https://jus.com.br/artigos/1830>. Acesso em: 25 mai. 2022.

PROCON. **Compras realizadas através da internet durante a pandemia elevam número de crimes virtuais.** 2022. Disponível em:<https://tribunahoje.com/noticias/economia/2022/02/07/97217-compras-realizadas-atraves-da-internet-durante-a-pandemia-elevam-numero-de-crimes-virtuais>. Acesso em 03 out. 2022.

PROCON ALAGOAS. **Golpes Digitais**: Procon alagoas dá orientações para evitar fraudes. 2022. Disponível em: <https://procon.al.gov.br/noticia/22-randomicas/218-golpes-digitais-procon-alagoas-da-orientacoes-para-evitar-fraudes>. Acesso em 07 out. 2022.

SANTOS, Rosangela dos. **Criminalidade digital em tempos de pandemia:** principais ocorrências em Sergipe no ano de 2020. São Cristóvão, 2021. Monografia (graduação em Direito) – Departamento em Direito, Centro de Ciências Sociais Aplicadas, Universidade Federal de Sergipe, São Cristóvão, SE, 2021.

SCHECHTER, Luis Menasche. **A Vida e o Legado de Alan Turing para a Ciência.** Publicado pelo Departamento de Ciência da Computação/UFRJ, 2016. Disponível em <https://www.cos.ufrj.br/seminarios/2015/slides/slides_luis.pdf >. Acesso em 03 mai. 2017.

SILVA, Fernanda Tatiane da.; PAPANI, Fabiana Garcia. **Um pouco da história da criptografia**. Publicado em Anais da XXII Semana Acadêmica de Matemática da Unioeste, 2016. Disponível em <http://projetos.unioeste.br/cursos/cascavel/matematica/xxiisam/artigos/16.pdf>. Acesso em: 28 set. 2022.

SILVA, João Pedro Alves Tomaz Silva; MARINHO, Luiz Eduardo Arruda. **O aumento dos crimes virtuais na pandemia e os limites da liberdade de expressão**. Orientadora: Danielle Freitas de Lima Oliveira. 2022. 28 f. TCC (Graduação) – Curso de Direito, Centro de Ciências Jurídicas, Universidade Potiguar, Natal, 2022. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/25232/1/O AUMENTO DOS CRIMES VIRTUAIS NA PANDEMIA E OS LIMITES DA LIBERDADE DE EXPRESS%C3%83O.pdf>. Acesso: 26 set. 2022.

SILVA, Ricardo Leopoldo da.; VIEIRA, Anderson. **Segurança cibernética: o cenário dos crimes virtuais no Brasil.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 06, Ed. 04, Vol. 07, pp. 134-149. Abril de 2021. ISSN: 2448-0959, Link de acesso: <https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais, DOI: 10.32749/nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais>.

SYDOW, Spencer Toth. **Delitos informáticos próprios:** uma abordagem sob a perspectiva vitimodogmática. 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/delitos_informaticos_proprios_uma_abordagem_sob_a_perspectiva_vitimodogmatica.pdf>. Acesso em: 26 set. 2022.

TUPINAMBÁ, Marcos. Ataques e crimes cibernéticos. **Segurança Digital:** proteção de dados nas empresas. São Paulo: Atlas, 2021. 247 p. cap. 3, p. 15-30.

ZANELLATO, Marco Antônio. **Condutas Ilícitas na sociedade digital,** Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, Direito e Internet, julho de 2002.