Universidade de Brasília

Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas - FACE

Departamento de Gestão de Políticas Públicas - GPP

WANDERSON KLEBER DE LIMA ALVES

CRIMES CIBERNÉTICOS NA PANDEMIA: O Impacto na Segurança Digital da pessoa idosa e o Papel da Política Nacional de Segurança Cibernética

Brasília – DF

2025

WANDERSON KLEBER DE LIMA ALVES

CRIMES CIBERNÉTICOS NA PANDEMIA: O Impacto na Segurança Digital da pessoa idosa e o Papel da Política Nacional de Segurança Cibernética

Projeto de Monografia a ser apresentado ao Departamento de Gestão de Políticas Públicas como requisito parcial à obtenção do título de Bacharel em Gestão de Políticas Públicas.

Professor/a Orientador: Marcelle Gomes Figueira

Brasília – DF

2025

Dedico este trabalho a Deus, por me permitir escrevê-lo; a todos que se preocupam com seus idosos em casa; e ao meu jovem eu, pela coragem de seguir em frente, mesmo quando os desafios pareciam grandes demais.

AGRADECIMENTOS

A Deus, pela força e sabedoria concedidas nos momentos de dificuldade. À minha família, por ser o pilar de amor e força que me sustentou.

Agradeço profundamente ao meu pai, que me ensinou o verdadeiro valor da honestidade. Seu exemplo de esforço e integridade moldou minha visão de mundo e me inspirou a buscar a excelência em tudo o que faço. Sua orientação e princípios foram fundamentais para meu crescimento pessoal.

Sou igualmente grato à minha mãe, cuja dedicação e amor me mostraram o significado do esforço e da perseverança. Seus ensinamentos sobre a integridade e o compromisso com nossos princípios foram cruciais para a formação do meu caráter. Seu apoio constante e suas palavras de encorajamento foram uma fonte vital de motivação ao longo de minha trajetória.

Agradeço a minha companheira, cuja presença tem sido um suporte inestimável e cuja força e amor foram fundamentais em cada passo desta jornada. Sem seu apoio, a conclusão desta etapa seria muito mais desafiadora. Sua influência foi verdadeiramente transformadora, e sou imensamente grato por ter você ao meu lado.

Agradeço também aos amigos, por serem a fonte constante de apoio e alegria que iluminaram meus dias.

Expresso minha gratidão à Universidade de Brasília, por ser um farol de esperança e excelência em educação. Seu compromisso em promover uma educação de qualidade e o desenvolvimento acadêmico foram essenciais para a realização deste trabalho.

Agradeço ainda aos professores, especialmente à minha orientadora, que abraçou meu projeto com entusiasmo e dedicação, contribuindo de maneira crucial para a sua realização.

Obrigado a todas as pessoas que contribuíram para o meu sucesso e para o meu crescimento como pessoa, sou o resultado da confiança e da força de cada um de vocês.

“A insatisfação é o primeiro passo para o progresso de um homem ou uma nação”.

- Oscar Wilde

RESUMO

Este estudo examina o papel da Política Nacional de Segurança Cibernética (PNCiber), os crimes cibernéticos e o impacto na segurança pública, e como essas transgressões afetaram a população idosa durante a pandemia de COVID-19. A pesquisa foca na análise do impacto desses delitos na segurança pública, destacando as implicações específicas para a pessoa idosa e as respostas adotadas pelas autoridades. Além disso, a investigação aborda a vulnerabilidade da pessoa idosa no mundo digital, explorando como o nível de familiaridade com tecnologias e a consciência sobre segurança cibernética contribuem para sua exposição a fraudes online.

Com a pandemia forçando um aumento no uso de tecnologias digitais, muitas pessoas idosas passaram a enfrentar novos riscos cibernéticos. Este trabalho propõe uma abordagem para melhorar a segurança digital entre as pessoas idosas, sugerindo estratégias de educação e conscientização para mitigar a exploração e fortalecer a proteção contra crimes cibernéticos. A pesquisa visa contribuir para uma maior compreensão e resposta às ameaças digitais que afetam esse grupo etário, promovendo uma proteção mais eficaz e informada.

Palavras-chave: Política Nacional de Segurança Cibernética, Crimes Cibernéticos, Idosos.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A essencialidade da internet alcançou tamanha magnitude que passou a ser algo intrínseco à interação social dos indivíduos, a globalização trouxe consigo diversas mudanças em meio aos avanços tecnológicos. Atualmente a maioria das pessoas, físicas ou jurídicas, “depende de um dispositivo informatizado, seja um celular, tablet ou até um computador com banco de dados que processa inúmeras informações sigilosas de uma empresa multinacional” (BRITO, 2013, p. 7).

Devido a essa fácil conectividade, os crimes cibernéticos se tornaram mais recorrentes, e difíceis de serem combatidos. Os delitos que estarão enfoque neste trabalho são considerados populares no ambiente virtual e também ilustram uma debilidade pungente a uma faixa etária especifica, os idosos, caracterizada pelo abandono governamental, educacional e parental no âmbito do conhecimento cibernético.

As preocupações com a segurança cibernética envolvendo as pessoas idosas raramente são discutidas e, na maioria das vezes, esse assunto é negligenciado. As generalidades das pesquisas costumeiramente se concentram em questões relacionadasa grupos padrões de usuários, como jovens e adultos. Dentre os trabalhos no campo literário, existe uma certa carência de obras que enfatizam as questões relacionadas as pessoas idosas, especialmente em segurança cibernética.

O próprio termo “Segurança Cibernética” sofre variações de significado entre diferentes pesquisadores. Neste documento, alinhando-se à visão de Craigen (2014), o termo refere-se à "organização e ao conjunto de recursos, processos, mecanismos e estruturas usados para proteger o ciberespaço e os sistemas habilitados para o ciberespaço contra ocorrências que desalinhem os direitos de propriedade de jure e de fato".

Nesse contexto, o Brasil implementou a Política Nacional de Segurança Cibernética (PNCiber) como uma resposta estratégica para enfrentar as ameaças digitais. A PNCiber busca fortalecer a proteção do ambiente virtual, promovendo diretrizes que envolvem a colaboração entre governos, empresas e sociedade civil. Contudo, as ações voltadas as pessoas idosas ainda são incipientes, evidenciando a necessidade de políticas mais direcionadas.

No dia 11 de março de 2020, a Organização Mundial da Saúde (OMS) decretou em nível mundial a pandemia, sendo essa caracterizada pela magnitude na contaminação por doença infecciosa em diversas regiões espalhadas geograficamente pelo mundo e não pela gravidade em si.

Em decorrência do isolamento social e os "*lockdowns"*, impostos pela pandemia todos tiveram que se adaptar rapidamente à nova realidade, transferindo funcionários, estudantes e demais atores externos para o sistema de trabalho remoto (Home Office). Resultando, em um curto período, o surgimento exponencial de novos usuários tecnológicos.

A pandemia de COVID-19 criou um cenário global de fragilidade e vulnerabilidade. nesse contexto de quarentena, indivíduos mal-intencionados não ficaram inativos; ao contrário, encontraram no caos oportunidades para agir e passaram a explorar novas formas de cometer delitos virtuais, denominados como crimes cibernéticos.

1.1 Contextualização do problema

Para Deibert e Rohozinski (2010 apud BRASIL et al, 2017), tornar o ciberespaço um ambiente seguro seria uma das principais preocupações políticas globais do século XXI. Contudo, pouco se menciona sobre os riscos ou as implicações políticas a ele relacionadas. Embora a globalização traga novos desafios, ela também incentiva o uso de novas tecnologias e a adoção de formas inovadoras de coordenação mundial para combater esses perigos. O alcance global dos crimes que envolvem as telecomunicações coloca desafios particulares às forças policiais, uma vez que, nessa nova conjuntura, atos criminosos conduzidos num dado país têm o poder de fazer vítimas em todo o mundo (GIDDENS, 2008).

O crime de "invasão de equipamentos de informática" teve como primeira notável contramedida a tipificação no Código Penal pela Lei 12.737, de 30 de novembro de 2012, e é disciplinado da seguinte forma: "[...] invasão de equipamentos eletrônicos, interligados ou não a rede de computadores, com objetivo de obter, sem o consentimento expresso ou tácito do proprietário do equipamento, alterar ou destruir dados ou informações, ou instalar vulnerabilidades para ganho ilícito. (BRASIL, 2012)

Ademais, dentre as contravenções penais mencionadas anteriormente, algumas sofreram alteração na redação constitucional para que fossem inclusas e serão apresentados a seguir de forma breve.

Primeiramente, a Lei n° 14.155, de 27 de maio de 2021, que alterou a redação do artigo 154-A, do Código Penal, abrangendo mais condutas virtuais ilícitas, como extorsão, extorsão digital e *Ransomware*[1]. A Lei supracitada inclui também a fraude eletrônica (§ 2º-A. e § 2º-B)

[1] *Ransomware* é um software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo.

no dispositivo que disciplina sobre o estelionato, o qual será utilizado para enquadrar o *phishing*[2], tratando por foco a pessoa idosa e sua fragilidade ante este cenário.

Ademais, a Lei 14.132, de 31 de março de 2021, inseriu no Código Penal, o artigo 147-A, que dispõe sobre o crime de perseguição que será tratado sobre o viés cibernético, o *ciberstalking*.

Outro marco relevante é a Lei Geral de Proteção de Dados Pessoais (LGPD 13.709/2018) que se apresenta com o objetivo de proteger os direitos fundamentais à liberdade, à privacidade e ao desenvolvimento da personalidade de cada indivíduo. A lei regula o tratamento de dados pessoais, independentemente de estarem armazenados em meio físico ou digital, e se aplica tanto a pessoas físicas quanto jurídicas, de direito público ou privado. Ela abrange um vasto conjunto de operações realizadas, sejam elas manuais ou digitais. Com o objetivo de assegurar a proteção dos dados pessoais dos cidadãos em território nacional, a LGPD entrou em vigor em setembro de 2020. (BRASIL, 2019).

Ainda em prol deste cenário a **Política Nacional de Segurança Cibernética (PNCiber)**, instituída para fortalecer a proteção contra crimes cibernéticos e promover ações estratégicas que englobam a cooperação entre governos, sociedade civil e setor privado se apresenta com diretrizes para a prevenção de ataques cibernéticos, a mitigação de danos e a conscientização pública, com especial atenção aos grupos vulneráveis, como as pessoas idosas. Ela também busca alinhar as legislações nacionais às demandas globais de segurança cibernética, reconhecendo a complexidade do ciberespaço e a necessidade de resposta rápida e eficaz.

O Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br) apurou mais de 800 mil notificações de incidentes de segurança em 2019 e mais de 300 mil casos apenas na primeira metade de 2020, dentre as notificações destacam-se golpes, fraudes, *spams*, *phishing* e invasões por *Worms*[3]. Contudo, esses relatórios são registrados

---

[2] *Phishing*, (pronunciado: fishing) é uma expressão originaria da língua inglesa, da palavra fishing (pescaria). Esse método de "pescar dados" é utilizado pelos cibercriminosos que coletam informações pessoais de suas vítimas por meio de ferramentas, como e-mails, aplicativos e sites enganosos, para que, dessa maneira, eles possam roubar o dinheiro ou a identidade dessas vítimas sendo possível, coletar dados pessoais, tais como, números de cartão de crédito e informações bancárias.

[3] Worms expressão originaria da língua inglesa, que significa verme. São um tipo de malware autorreplicador (é um tipo de vírus) que entra nas redes explorando vulnerabilidades, movendo-se rapidamente de um computador para o outro.

facultativamente e, portanto, não exprimem com exatidão real número de transgressões de segurança identificados. Além disso, a empresa de segurança cibernética Kaspersky divulgou recentemente uma pesquisa apontando que os ataques cibernéticos no Brasil cresceram cerca de 23% em 2021. Nesse cenário, o estelionato figura como um dos delitos mais comuns do Código Penal Brasileiro, devido à sua versatilidade na execução, adaptando-se facilmente a diferentes contextos. Em prol deste cenário, a segurança digital converteu-se em um tema de destaque no Estado e urge por uma demanda crescente de análise e intervenção.

1.2 Pergunta de pesquisa

Para entender o impacto dos crimes cibernéticos na segurança pública durante a pandemia de COVID-19, com foco na população idosa, a questão de pesquisa pode ser formulada assim:

De que maneira a Política Nacional de Segurança Cibernética (PNCiber) se relaciona com os desafios enfrentados pelas pessoas idosas no campo digital durante a pandemia de COVID-19 e sua exposição a crimes cibernéticos?

1.3 Objetivos da pesquisa

O objetivo desta pesquisa é analisar o impacto dos crimes cibernéticos na segurança pública, com foco na população idosa durante a pandemia de COVID-19. A pesquisa busca analisar vulnerabilidades e fatores de risco que contribuem para o envolvimento das pessoas idosas em crimes cibernéticos, incluindo padrões de uso da Internet, nível de conhecimento em tecnologia e conscientização sobre segurança digital, propondo medidas para aumentar a conscientização alinhadas às diretrizes da Política Nacional de Segurança Cibernética (PNCiber) sobre segurança cibernética entre as pessoas idosas, visando educá-los a fim de reduzir a exploração em crimes cibernéticos. Conforme será explicitado posteriormente na etapa do referencial teórico.

Os objetivos específicos da pesquisa indicados para explanação, pautados na pergunta norteadora são os seguintes:

a) **Analisar o Impacto dos Crimes Cibernéticos na Segurança Pública:**

- Examinar como o aumento dos crimes cibernéticos afetou a segurança pública, com foco específico nas consequências para a população idosa.

b) **Avaliar a Vulnerabilidade Digital da Pessoa Idosa:**

- Analisar como a falta de conhecimento em tecnologia e a baixa conscientização sobre segurança cibernética contribuem para a vulnerabilidade das pessoas idosas a crimes cibernéticos.

c) **Idealizar uma Estrutura de Conscientização e Educação para Pessoas Idosas.**

- Propor uma estrutura de conscientização e educação sobre segurança cibernética para pessoas idosas, com base na análise dos padrões de uso da Internet e das lacunas de conhecimento identificadas, com o objetivo de prevenir e mitigar a exploração em crimes cibernéticos.

1.4 Justificativa

Delimitada a pergunta norteadora e os objetivos de pesquisa, concerne ressaltar a relevância da pesquisa.

Com o avanço da tecnologia e a crescente digitalização das interações sociais e econômicas, o governo federal tem buscado fortalecer as regulamentações sobre segurança digital. Nesse contexto, a **Política Nacional de Segurança Cibernética (PNCiber)** desempenha um papel estratégico, incentivando corporações, instituições públicas e a sociedade civil a implementar e manter políticas robustas de segurança cibernética. Contudo, a natureza global da Internet, que transcende fronteiras nacionais, representa um desafio significativo para as autoridades, dificultando a investigação, o combate e a prevenção de crimes no ambiente virtual.

A problemática central desta pesquisa reside na dificuldade de rastrear, investigar e produzir provas contra crimes cibernéticos. Essa barreira é amplificada pela facilidade com que criminosos podem criar perfis falsos, apagar rastros e explorar ferramentas tecnológicas destinadas a mascarar atividades ilícitas. Ao mesmo tempo em que empresas investem no fortalecimento da segurança digital de seus sistemas, criminosos desenvolvem novas técnicas para explorar vulnerabilidades, criando um ciclo de ameaças e adaptações constantes.

Este estudo é especialmente relevante para compreender o impacto dos crimes cibernéticos na segurança pública durante a pandemia de COVID-19, com ênfase na população idosa, pois durante o período de isolamento social, muitas pessoas idosas foram obrigadas a se adaptar rapidamente ao uso de tecnologias digitais, aumentando sua exposição a fraudes, golpes de *phishing* e outros delitos cibernéticos. A fragilidade desse grupo no ambiente digital, está associada à falta de familiaridade com ferramentas tecnológicas e à baixa conscientização sobre segurança cibernética, o que agrava consideravelmente sua vulnerabilidade, apesar de todas as faixas etárias estarem sujeitas a isso.

Além disso, a crescente sofisticação dos ataques cibernéticos representa uma ameaça não apenas a indivíduos, mas também a dados sigilosos armazenados em bancos de dados pessoais, jurídicos e federativos. Essa capacidade de corromper informações sensíveis ou estratégicas gera impactos globais e enfatiza a necessidade de políticas públicas e ações coordenadas para fortalecer a segurança cibernética.

Assim, a presente pesquisa contribui para a análise das implicações dos crimes cibernéticos na segurança pública e para a tentativa de formulação de estratégias que mitiguem os riscos enfrentados pelas pessoas idosas.

2 REFERENCIAL TEÓRICO

A internet é uma estrutura em constante evolução, servindo como alicerce para a interconexão de redes de aparelhos distribuídos globalmente. O acesso do usuário ocorre por meio de um equipamento conhecido como modem, em conjunto com a utilização de aplicativos. Ao contrário das ligações telefônicas tradicionais, na internet não se restringe a apenas um caminho para a troca de dados entre dois aparelhos. Existem diversas rotas disponíveis, sendo pouco comum, mas eventualmente possível, que um pacote de dados se extravie em uma determinada rota. (TEIXEIRA, 2020, p. 14).

Considerando essa perspectiva, é possível conceber a internet como uma ponte que conecta todos os aparelhos vinculados a ela por meio de várias modalidades de conexão. Essa interligação contribui para a agilidade, rapidez e avanço tecnológico na comunicação das pessoas.

O Marco Civil da Internet (Lei n. 12.965, de 23 de abril de 2014), art. 5º, I, delimita a internet como um sistema composto por protocolos racionais, organizados globalmente para uso público e sem limitações, com o intuito de viabilizar a comunicação de dados entre terminais. (Nucci, 2021)

Com o avanço das novas tecnologias impulsionando a globalização, e a propagação de conveniências aos usuários por intermédio da internet, como a possibilidade do comércio eletrônico, transações financeiras e trocas de informações, a rede se tornou um ambiente muito atrativo também para atividades criminosas. (Nurse, 2018).

Pinheiro (2021, p.18) sugere que na década de 1970, emerge a ideia de uma sociedade da informação. Essa sociedade, originada da abundância de informações, caracteriza-se pela coexistência entre o mundo físico e digital, demandando que seus membros acessem informações de forma crescente, buscando de maneira inconsequente cada vez mais informações, ultrapassando fronteiras do saudável ou razoável ao indivíduo.

Ferreira (TEIXEIRA, 2020, p. 214) aponta que:

> A informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos, cujo alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução.

2.1 Classificação dos crimes cibernéticos

Antes de explorar o conceito de *cibercrimes*, é relevante destacar que os delitos informáticos podem ser categorizados em crimes contra o computador, ou outros dispositivos eletrônicos, como tablets e smartphones, nos quais o aparelho é o alvo, como no crime de invasão de dispositivo informático, conforme estabelecido pelo artigo 154-A do Código Penal, ou crimes por meio da utilização do dispositivo eletrônico, nos quais o dispositivo atua como instrumento para a prática do crime, sendo utilizados pelos *cibercriminosos* como meio para a execução de práticas criminosas, como ocorre, por exemplo, nos crimes contra a honra.

Segundo Vladimir Aras, os crimes de informática são conhecidos como:

> Delitos computacionais, crimes de informática, crimes de computador, crimes eletrônicos, crimes telemáticos, crimes informacionais, ciberdelitos, cibercrimes. Não há um consenso quanto ao nomen juris genérico dos delitos que ofendem interesses relativos ao uso, à propriedade, à segurança ou à funcionalidade de computadores e equipamentos periféricos (hardwares), redes de computadores e programas de computador (estes denominados softwares).

> Dentre essas designações, as mais comumente utilizadas têm sido as de crimes informáticos ou crimes de informática, sendo que as expressões "crimes telemáticos" ou "cibercrimes" são mais apropriadas para identificar infrações que atinjam redes de computadores ou a própria Internet ou que sejam praticados por essas vias. Estes são crimes à distância stricto sensu. Como quer que seja, a criminalidade informática, fenômeno surgido no final do século XX, designa todas as formas de conduta ilegais realizadas mediante a utilização de um computador, conectado ou não a uma rede, que vão desde a manipulação de caixas bancários à pirataria de programas de computador, passando por abusos nos sistemas de telecomunicação. (ARAS, 2015).

O autor também caracteriza os crimes informáticos como ato típico e antijurídico, cometido por meio da informática, ou contra um sistema, ou contra uma rede de dispositivos, em que a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo direito penal.

Nesse contexto, Vieira (2021) adicionalmente explana que é válido destacar que os delitos virtuais podem ser classificados como próprios e impróprios. Os crimes próprios referem-se a condutas que têm como alvo o sistema, violando sua confiabilidade, integridade ou disponibilidade. Já os crimes impróprios caracterizam-se por condutas criminosas consideradas comuns, no sentido de que podem ser executadas com o auxílio de mecanismos informáticos, embora pudessem ocorrer de outras maneiras.

2.1.1 Crimes cibernéticos e a Pandemia de Covid-19

Os estudos sobre os crimes cibernéticos na pandemia ainda são relativamente recentes. Contudo o pesquisador Alexandre Júnior (2019) alega que, com o avanço da tecnologia, o ambiente virtual se tornou um dos componentes fundamentais para o progresso das atividades humanas. O anonimato ilusório oferecido pela internet propicia um terreno conveniente para a prática de comportamentos ilícitos, conhecidos como cibercrimes.

Os delitos eletrônicos ou cibernéticos, em sua maioria, são crimes que envolvem o meio digital; no entanto, crimes perpetrados por *crackers*[4], são restritos ao ambiente virtual, efetivando a conduta criminosa exclusivamente através deste meio. Em determinadas situações,

[4] *Cracker* é um termo específico para indivíduos que têm como objetivo quebrar sistemas de segurança e realizar atividades maliciosas, em contraste com hackers, que podem ter intenções variadas, tanto éticas quanto não éticas. Embora frequentemente sejam usados de forma intercambiável, há uma diferença sutil entre os dois termos. "*Hacker"* é geralmente associado a indivíduos que exploram sistemas de forma ética e legal, ou que visam melhorar a segurança, enquanto crackers são conhecidos por suas atividades prejudiciais e ilegais.

porém, o crime pode transcender o ambiente virtual. Os crimes eletrônicos apresentam diversas modalidades, variando conforme o bem jurídico protegido pela norma. A internet atua apenas como um facilitador, e, portanto, as considerações relacionadas ao conceito de crime e outros termos são as mesmas aplicadas ao direito penal. (PINHEIRO, 2009, p. 225-226).

Arruda e Justino (2020), dissertam que o Brasil possui mecanismos jurídicos suficientes para combater as ameaças digitais, porém possui grande falha por parte dos profissionais de segurança pública e a sociedade em geral no que diz respeito a prevenção dos crimes cibernéticos.

Para Nagli (2020), o aumento no número de casos de COVID-19 criou novas oportunidades para a ação de criminosos digitais, uma vez que as empresas foram forçadas a mudar suas operações, especialmente com a alocação de um grande número de trabalhadores em regime de home office, o que aumentou exponencialmente a exposição de trabalhadores e suas famílias aos perigos da internet.

De acordo com estudo realizado pela Interpol (2020), em um período de quatro meses (janeiro a abril), cerca de 907.000 mensagens de spam, 737 incidentes relacionados a malware e 48.000 URLs maliciosos - todos relacionados ao vírus Covid-19 - foram detectados. Para o Secretário Geral da Interpol, os cibercriminosos estão desenvolvendo e aumentando seus ataques em um ritmo alarmante, explorando o medo e a incerteza causados pela situação social e econômica instável criada pelo vírus (JURGEN, 2020).

2.2 A pessoa idosa

O envelhecimento da população é uma realidade global. Com o aumento da longevidade, busca-se constantemente alternativas para melhorar a qualidade de vida na terceira idade. O mundo está em constante transformação, e as pessoas idosas, especialmente aqueles abordados neste estudo, precisam se adaptar a essas mudanças. Isso gera a necessidade de desenvolver novas políticas públicas mais abrangentes, com leis específicas e rigorosas para garantir proteção ao longo de toda a vida. A terceira idade marca o início de uma nova fase, na qual muitas pessoas idosas requerem acompanhamento, afeto e cuidados adequados. Dito isso, quem é considerado idoso? A definição de pessoa idosa vai além da aparência ou das condições sociais.

Segundo Lima (2019):

> Em nosso país, artigo 1° da Lei nº 10.741 de outubro de 2003, denominada “Estatuto do Idoso”, traz o conceito de idoso em seu Art. 1º: É instituído como sendo idosa a

> pessoa com idade igual ou superior a 60 (sessenta) anos. Já na França, considerado um país desenvolvido o parâmetro de idade é maior, sendo considerado idoso aquele que atinge os 65 (sessenta e cinco) anos.

Nesse contexto, o Censo de 2022 do Instituto Brasileiro de Geografia e Estatística (IBGE) revela que o Brasil conta com aproximadamente 34,2 milhões de pessoas com 60 anos ou mais, sendo 58% mulheres (19,8 milhões) e 42% homens (14,4 milhões), o que corresponde a 16% da população brasileira (IBGE, 2022).

Em resultante dos traços que marcam a vulnerabilidade desse grupo, verificam-se várias práticas de violação de seus direitos fundamentais, tais como os citados por Gilmar F. Mendes (2017, p.489): negligência, abuso financeiro e econômico, discriminação, violência psicológica, sexual, física e institucional. Nesse sentido, é válido ressaltar a gravidade do impasse, visto que muitos dos direitos oprimidos, são garantidos por norma constitucional (art. 5°, CF/88).

Na contemporaneidade, é notável que uma das principais formas de violação dos direitos fundamentais das pessoas idosas é através de estelionatos cibernéticos. Solange Duarte Barros e Paula Torales Leite (2019, p. 4) apontam que, nos últimos anos, tem-se observado um aumento significativo na participação das pessoas idosas no ambiente virtual, onde eles se comunicam com familiares e utilizam tecnologias para lazer. No entanto, o crescimento proporcional do número de usuários idosos também resultou no aumento desses indivíduos como vítimas de crimes cibernéticos. Segundo as autoras, as principais causas desse fenômeno incluem a redução das capacidades cognitivas e fisiológicas associadas ao envelhecimento, juntamente com o desconhecimento sobre o uso seguro das tecnologias e os riscos associados. Isso torna as pessoas idosas particularmente vulneráveis a crimes informáticos.

2.3 Políticas Públicas

Políticas públicas são um conjunto de ações e decisões tomadas por instituições governamentais destinadas a resolver problemas coletivos e promover o bem-estar da população. Elas envolvem a formulação, implementação e avaliação de programas e normas que visam atender às necessidades sociais, econômicas e culturais da sociedade. Segundo Souza (2017), políticas públicas são “instrumentos essenciais para a regulação e a coordenação das relações sociais, buscando atender aos interesses públicos e garantir a justiça social” (SOUZA, 2017, p. 45).

De acordo com a abordagem de Peters (2015), as políticas públicas podem ser vistas como o resultado de um processo político e administrativo que envolve a interação de múltiplos

atores, incluindo governo, sociedade civil e setores privados. Peters (2015) enfatiza que “as políticas públicas são frequentemente moldadas por negociações e compromissos entre diferentes grupos de interesse, refletindo a complexidade das relações sociais e políticas” (PETERS, 2015, p. 123).

Ambos os pontos de vista ressaltam aspectos cruciais da natureza das políticas públicas, desde sua função regulatória e de atendimento às necessidades sociais até a complexidade dos processos políticos envolvidos em sua formulação e execução. Esses enfoques fornecem uma compreensão abrangente das políticas públicas e são fundamentais para a análise crítica e a avaliação de sua eficácia e impacto.

As políticas públicas de segurança digital no Brasil têm se consolidado por meio de diversas iniciativas e programas destinados a enfrentar os desafios impostos pelos crimes cibernéticos. O Gabinete de Segurança Institucional (GSI), por meio do Centro de Defesa Cibernética (CDC), desempenha um papel crucial na proteção da infraestrutura crítica e na resposta a incidentes cibernéticos (GSI, 2023). Da mesma forma, a Secretaria Nacional de Segurança Pública (SENASP) coordena políticas que visam fortalecer a segurança pública com um enfoque crescente na segurança cibernética (SENASP, 2024).

De acordo com Azevedo (2021), a criação e o fortalecimento desses programas refletem a crescente preocupação com a proteção de dados e sistemas críticos no Brasil. O autor destaca que a Estratégia Nacional de Segurança Cibernética (ENSC) estabelece diretrizes que promovem a coordenação entre órgãos e a implementação de melhores práticas de segurança, essenciais para a proteção contra ameaças cibernéticas emergentes. Azevedo argumenta que, apesar desses avanços, ainda há lacunas significativas na conscientização e na educação digital, especialmente entre populações vulneráveis como as pessoas idosos.

Por outro lado, Silva (2022) aponta que, embora a Lei Geral de Proteção de Dados (LGPD) e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) tenham contribuído para a segurança digital, a eficácia dessas políticas pode ser comprometida pela falta de integração entre as iniciativas governamentais e o setor privado. Silva (2022) sugere que a ausência de um enfoque mais robusto na capacitação contínua de profissionais e na implementação de tecnologias de ponta pode limitar a eficácia das ações de segurança cibernética no país.

Portanto, enquanto as políticas públicas de segurança digital no Brasil têm evoluído com o objetivo de melhorar a proteção contra crimes cibernéticos, é crucial abordar as deficiências identificadas na conscientização e capacitação para garantir uma defesa eficaz contra as ameaças digitais (GSI, 2023; SENASP, 2024; Azevedo, 2021; Silva, 2022).

É relevante destacar a importância de se compreender as políticas públicas como instrumentos dinâmicos e contextuais, que evoluem de acordo com as demandas da sociedade e as mudanças no cenário político, econômico e social. Segundo Dye (2013), as políticas públicas podem ser definidas como "tudo aquilo que os governos escolhem fazer ou não fazer" (DYE, 2013, p. 24), o que enfatiza o papel estratégico do governo na priorização de ações e na alocação de recursos para atender às necessidades da população.

A formulação de políticas públicas geralmente ocorre em etapas interdependentes que incluem a identificação de problemas, a definição de agendas, a elaboração de alternativas, a tomada de decisões, a implementação e a avaliação. Kingdon (2011) propõe o modelo de múltiplos fluxos, destacando que a formulação de políticas surge da convergência de três componentes principais: problemas, soluções e política. Essa interação é fortemente influenciada pelo papel dos atores envolvidos, pelos contextos institucionais e pela abertura de "janelas de oportunidade" que permitem a implementação de mudanças.

Na análise da segurança cibernética, a Política Nacional de Segurança Cibernética (PNCiber) emerge como um exemplo paradigmático de política pública voltada para um problema específico que ganhou relevância nos últimos anos: os crimes cibernéticos. Instituída pelo governo brasileiro, a PNCiber tem como objetivos principais a proteção do ambiente digital e a redução da vulnerabilidade de indivíduos e instituições diante de ameaças cibernéticas. Sua formulação baseou-se em diretrizes estratégicas que envolvem a cooperação interinstitucional, a capacitação técnica e o desenvolvimento de tecnologias de segurança avançadas.

Conforme explica Pereira (2020), a PNCiber representa uma iniciativa essencial para mitigar os riscos associados ao uso de tecnologias digitais em um mundo cada vez mais interconectado. No entanto, a eficácia dessa política depende de sua implementação e da capacidade dos órgãos responsáveis em monitorar, prevenir e responder às ameaças cibernéticas de forma eficiente e inclusiva. É nesse ponto que surge a necessidade de ampliar a abordagem da política pública para grupos mais vulneráveis, como as pessoas idosos, que enfrentam barreiras específicas no acesso e no uso seguro das tecnologias digitais.

2.4 Política Nacional de Segurança Cibernética (PNCiber)

A Política Nacional de Segurança Cibernética (PNCiber) representa um marco na estratégia brasileira para enfrentar os desafios da cibersegurança em um cenário de crescente digitalização. Instituída pelo Decreto nº 10.222, de 5 de fevereiro de 2020 (BRASIL, 2020), a

PNCiber foi criada para substituir iniciativas fragmentadas que, até então, tratavam a segurança cibernética de forma setorial e desarticulada. Antes de sua implementação, as medidas de proteção digital no Brasil eram majoritariamente conduzidas por órgãos específicos, como o Gabinete de Segurança Institucional (GSI) e o Comando de Defesa Cibernética (ComDCiber), mas careciam de uma abordagem integrada que englobasse atores diversos e setores complementares (GOLDONI et al., 2020).

A criação da PNCiber foi impulsionada pela crescente percepção de que a conectividade digital, embora essencial para o desenvolvimento econômico e social, havia se tornado um vetor crítico de vulnerabilidades. A ausência de diretrizes unificadas resultava em esforços duplicados, lacunas na proteção de setores estratégicos e uma limitada capacidade de resposta a incidentes. Segundo Goldoni et al. (2020), o Brasil necessitava de um marco regulatório abrangente e articulado para consolidar sua capacidade de prevenção e mitigação de riscos cibernéticos.

Em maio de 2023, o GSI publicou um projeto de lei que propunha a criação da Política Nacional de Cibersegurança. A minuta era detalhada e abordava a criação da PNCiber, além da criação da Agência Nacional de Cibersegurança (ANCiber), do Comitê Nacional de Cibersegurança (CNCiber) e do Gabinete de Gestão de Crise Cibernética (GSI, 2023). Um dos principais objetivos mencionados no projeto era "unificar a 'colcha de retalhos' regulatória existente no país" (GSI, 2023, p. 1). No entanto, ao analisar o documento de forma mais atenta, é possível perceber que ele não faz referência à Política Nacional de Segurança da Informação (PNSI) ou à Política Nacional de Segurança de Infraestrutura Crítica (PNSIC).. Isso sugere que as normas anteriores poderiam estar sendo substituídas ou, possivelmente, já não estavam em vigor.

Embora os objetivos do projeto de lei fossem amplos e ambiciosos, o documento não detalhava como seriam atingidos. A proposta incluía a criação de uma estratégia nacional de cibersegurança, a elaboração de um plano nacional e a implementação da ANCiber, mas sem especificar claramente os mecanismos ou ações práticas para atingir essas metas.

A política final, promulgada por meio do Decreto nº 11.856 em 26 de dezembro de 2023, foi mais concisa, totalizando cerca de quatro páginas. Sua promulgação por decreto, ao invés de um projeto de lei, sugere que o tema não recebeu a devida atenção no Congresso Nacional. A comparação entre os objetivos do projeto de lei e os do Decreto revela algumas mudanças notáveis. A seguir, na **Figura 1**, estão os objetivos apresentados na minuta do projeto de lei e os objetivos que foram mantidos ou modificados no Decreto nº 11.856 (2023):

Figura 1 - Objetivos da PNCiber

Objetivos Apresentados na Minuta	Objetivos no Decreto nº 11.856 (2023)
I – Garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade dos ciberativos de interesse da sociedade brasileira	**I** – Promover o desenvolvimento de produtos, serviços e tecnologias de caráter nacional destinados à segurança cibernética
II – Fomentar a ciberproteção e a ciber-resiliência do Poder Público, dos ciberativos de interesse e da sociedade como um todo	**II** – Garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações
III – Desenvolver na sociedade brasileira a cultura de cibersegurança	**III** – Fortalecer a atuação diligente no ciberespaço, especialmente das crianças, dos adolescentes e dos idosos
IV – Fomentar a articulação do intercâmbio de informações de cibersegurança entre: a) as esferas do governo; b) o setor privado; e c) a sociedade em geral	**IV** – Contribuir para o combate aos crimes cibernéticos e às demais ações maliciosas no ciberespaço
V – Promover a autonomia produtiva e tecnológica na área de cibersegurança	**V** – Estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos
VI – Fomentar a participação do Brasil na cadeia produtiva global de produtos e serviços voltados à cibersegurança	**VI** – Incrementar a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos
VII – Promover o uso ético de ciberativos e das tecnologias a eles associadas no País	**VII** – Desenvolver a educação e a capacitação técnico-profissional em segurança cibernética na sociedade
VIII – Fomentar o combate ao cibercrime	**VIII** – Fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética
IX – Promover ações que contribuam para a segurança e para a estabilidade do ambiente digital global	**IX** – Incrementar a atuação coordenada e o intercâmbio de informações de segurança cibernética entre: a) a União, os Estados, o Distrito Federal e os Municípios; b) os Poderes Executivo, Legislativo e Judiciário; c) o setor privado; e d) a sociedade em geral
X – Incrementar a projeção internacional do Brasil e inserir o País em processos decisórios internacionais, para fazer valer os valores e os interesses nacionais	**X** – Desenvolver mecanismos de regulação, fiscalização e controle destinados a aprimorar a segurança e a resiliência cibernéticas nacionais
XI – Implementar estratégias de colaboração para desenvolver a cooperação internacional em segurança cibernética	**XI** – (Sem correspondente específico no Decreto)

Fonte: Decreto n. 11.856 (2023) GSI (2023, p. 14).

A PNCiber trouxe consigo a proposta de uma governança descentralizada e colaborativa, alinhada ao modelo *bottom-up*. Essa abordagem reconhece que a segurança cibernética é um desafio que transcende as capacidades exclusivas do Estado, exigindo a participação ativa de empresas, universidades e da sociedade civil (PETERS, 2015). Assim, a política é estruturada com base em três eixos fundamentais: prevenção, resiliência e resposta a incidentes (BRASIL, 2020). Esses pilares visam não apenas proteger os sistemas digitais estratégicos, mas também fomentar a conscientização pública e a educação digital, criando uma cultura de segurança compartilhada.

A estrutura da PNCiber reflete essa visão integrada. O Gabinete de Segurança Institucional (GSI) é o órgão central responsável pela coordenação estratégica, mas sua atuação é complementada por outras instâncias, como o Comitê de Governança Digital (CGD) e o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov). Além disso, o setor privado desempenha um papel crucial no fornecimento de expertise técnica, enquanto a academia contribui com pesquisa e inovação tecnológica. Esse modelo integrado permite que a política aborde desde ameaças sofisticadas, como ataques de *ransomware* contra grandes empresas, até crimes cibernéticos que afetam diretamente indivíduos, como fraudes bancárias e golpes em pessoas idosas (GOLDONI et al., 2020).

A implementação da PNCiber também substituiu projetos anteriores, como o Programa Nacional de Proteção ao Conhecimento Sensível e a Estratégia Nacional de Defesa Cibernética. Esses programas, embora relevantes em seus contextos, tinham limitações claras, especialmente no que tange à integração de esforços e à coordenação intersetorial. A PNCiber veio para consolidar essas iniciativas sob uma única política nacional, otimizando recursos e eliminando redundâncias (GOLDONI et al., 2020).

No contexto da pandemia de COVID-19, a PNCiber demonstrou sua importância ao lidar com a explosão de crimes cibernéticos, especialmente os que vitimaram populações vulneráveis, como pessoas idosos. O isolamento social forçou milhões de brasileiros a dependerem de plataformas digitais para tarefas cotidianas, como compras, interações sociais e consultas médicas. Esse cenário expôs lacunas na proteção cibernética e mostrou a urgência de ações coordenadas para mitigar os danos. (GOLDONI et al., 2020).

3 METODOLOGIA DE PESQUISA

Para o desenvolvimento dessa pesquisa foi definido que esta será de natureza analítica pois, segundo Gerhardt e Silveira (2009, p. 35): “Objetiva gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos. Envolve verdades e interesses

internacionais". Ainda, o método utilizado será o estudo de caso e, também, por se tratar de um procedimento técnico que aborda vários fatores relevantes para execução do trabalho como a busca para se retratar a realidade e os pontos de vista que estão inseridos dentro um cenário social. Além disso, foram utilizados elementos como a observação participante do autor para compor a estrutura de análise, com a inclusão de entrevistas semiestruturadas utilizadas como suporte para aprofundar a compreensão do tema e diários de campo. Ademais, as atividades incluíram a elaboração de relatórios baseados em visitas esporádicas a reuniões e acompanhamentos em audiências públicas promovidas por ministérios e órgãos competentes, como a Secretaria Nacional de Segurança Pública (SENASP), mantendo-se uma postura de espectador entusiasta e voluntário no processo de análise.

3.1 Pesquisa Bibliográfica

A pesquisa bibliográfica é uma abordagem metodológica fundamental que consiste na revisão e análise de literatura existente sobre um tema específico. Segundo Diehl (2004) essa metodologia visa proporcionar um embasamento teórico consistente, permitindo a contextualização e o aprofundamento do conhecimento sobre o assunto em questão. No cenário deste estudo será selecionado literaturas que balizam o comportamento de grupos de pessoas idosas, no meio virtual, estes servirão de sujeitos da pesquisa e farão parte do estudo de caso. Inicialmente serão selecionados artigos, textos e estudos de casos que se enquadrem nas características pré-estabelecidas: 60 anos ou mais e que utilizem as redes sociais. Será o grupo focal como método para a observação, pessoas idosas utilizando as redes sociais e seu comportamento frente às *fake news*, isto é, se eles conseguem ter o senso crítico de identificar que se tratam de notícias falsas e se eles as compartilham. Então, serão avaliadas as fontes de informações utilizadas pelos sujeitos, bem como os mecanismos de buscas usados, assim espera-se ser possível atuar na educação e capacitação dessa parcela vulnerável da população gerando ao final deste estudo um material didático que viabilize isso.

3.2 Observação Participante

De acordo com Minayo et al. (2002), a observação envolve a experiência direta do pesquisador com o grupo estudado, permitindo um conhecimento mais profundo e uma compreensão mais detalhada da realidade dos atores sociais em suas esferas específicas. Ao se integrar à cultura observada, o pesquisador não apenas registra ações, interações e eventos, mas

também vive essas situações de forma direta, o que possibilita a identificação de uma ampla gama de ocorrências que podem não ser facilmente reveladas por meio de perguntas.

Neste estudo, a observação participante realizada ocorreu por meio de entrevistas semiestruturadas e diários de campo. As entrevistas semiestruturadas permitiram uma coleta detalhada de dados sobre as experiências e percepções dos participantes, enquanto os diários de campo proporcionaram uma documentação contínua e reflexiva das observações e interações. Ritchie (2003) destaca que, ao experimentar os fenômenos em primeira mão, o pesquisador tem a oportunidade de analisar os eventos à medida que surgem e obter informações valiosas através de sua própria vivência

Foram identificados dois grupos principais para as entrevistas semiestruturadas: pessoas idosas e profissionais com experiência no contexto. Roteiros específicos foram elaborados para cada grupo, abordando questões sobre experiências pessoais com crimes cibernéticos, mudanças percebidas durante a pandemia e medidas de proteção adotadas. Este mapeamento inicial é fundamental para garantir uma amostra representativa e abrangente, permitindo uma análise aprofundada das experiências e percepções relacionadas aos crimes cibernéticos e à vulnerabilidade da terceira idade.

Quanto aos diários de campo Falkembac (1987) os descreve como um documento pessoal que reflete observações e reflexões para uso individual do pesquisador. De acordo com Triviños (1987), as anotações no diário abrangem desde a coleta de dados até a análise dos fenômenos sociais, promovendo uma compreensão holística da situação estudada.

O foco desta etapa está na análise dos dados de crimes cibernéticos durante a pandemia de Covid-19. Para entender o impacto das políticas existentes e identificar áreas críticas que possam exigir intervenção ou aprimoramento.

Ao concluir os diários de campo foi produzido um relatório apresentando os resultados parciais das percepções na etapa da residência do curso, experiências e preocupações relacionadas à segurança digital em uma pequena amostragem demográfica grupal vulnerável e entre profissionais que estudam ou lidam com essas questões.

Foram entrevistadas 8 pessoas idosas residentes no Distrito Federal, selecionados de forma aleatória em diferentes regiões administrativas. As entrevistas exploraram suas experiências pessoais com tecnologia durante a pandemia, incluindo incidentes de crime cibernético, medidas de segurança adotadas e suas percepções sobre vulnerabilidades online. Já dentre os especialistas foram entrevistados 5 profissionais que atuam no contexto explorado, todos com experiência no cenário brasileiro.

As entrevistas revelaram a falta de familiaridade das pessoas idosas com práticas seguras na internet e uma confiança excessiva nas informações recebidas por meios eletrônicos. Esses achados reforçam a urgência de desenvolver campanhas educativas específicas e políticas de segurança digital mais acessíveis para esse grupo demográfico.

4 ANÁLISE DE DADOS

A análise de dados é o processo de examinar, limpar e modelar dados para descobrir informações úteis, apoiar a tomada de decisões e alcançar conclusões significativas. A análise qualitativa, conforme sugerido por Minayo (2002), permite explorar a complexidade das experiências e percepções das pessoas idosos sobre crimes cibernéticos, oferecendo uma compreensão profunda das vulnerabilidades e impactos desses crimes durante a pandemia.

4.1 Sintetizando desafios da segurança cibernética para as pessoas idosas

Segundo Iyer (2006), as pessoas idosas constituem um dos grupos de usuários da Internet que mais crescem. De acordo com uma pesquisa realizada por Claar (2012), mais de 50% das pessoas idosas utilizam a Internet, e esse número está aumentando gradualmente.

Vários estudos, incluindo os de Claar (2012), Joel Holmberg (2019), Carlton (2015) e König et al. (2018), indicam que as pessoas idosas, em geral, possuem um conhecimento limitado sobre tecnologia, o que resulta em desinteresse por novos métodos de segurança digital. Esse desafio é acentuado por problemas físicos ou de saúde que dificultam o uso de novas tecnologias e a necessidade de assistência para operar dispositivos (Boral, 2020).

Como resultado, muitos dispositivos utilizados por pessoas idosas não são adequadamente protegidos. Eles frequentemente não compreendem a importância de instalar e usar softwares de segurança, como antivírus e AntiSpam, e alguns não permitem atualizações de seus dispositivos. Isso aumenta a vulnerabilidade dos dispositivos a ataques cibernéticos (Claar, 2012).

4.1.1 Fatores comportamentais

De acordo com Nurse (2018), as pessoas idosas são um grupo de usuários que têm menos probabilidade de denunciar o crime às autoridades se estiverem envolvidos em um caso de crime cibernético. Isso se deve a uma combinação de dois fatores principais. Em primeiro lugar, a maioria deles não sabe onde denunciar casos de fraude e, posteriormente, não sabe como lidar

com essas situações. Outrossim, eles também podem se sentir constrangidos com o que aconteceu com eles, por exemplo, com aqueles que se envolveram em fraudes amorosas.

4.1.2 Habilidades de segurança cibernética entre as pessoas idosas

A maioria dos aplicativos exige que o usuário faça login antes de poder continuar a navegar. Portanto, o gerenciamento de senhas entre as pessoas idosas também precisa de atenção. O fator idade também contribui para essa questão. Por exemplo, nessa idade, eles tendem a usar senhas simples em vez de complexas. A combinação complexa de senhas dificulta a memorização, especialmente se tiverem problemas de saúde como demência, conforme afirma, Nurse (2018), Brown, et al (2016). Consequentemente, eles preferem usar palavras comuns ou fáceis de "lembrar" como senhas. Além disso, tendem a usar a mesma senha para cada aplicativo que possuem.

O problema da "lacuna de habilidades" entre as pessoas idosas e sua exclusão social na sociedade da informação tem sido minimizado no ambiente de trabalho. Carlson (2006) afirma que o trabalho com as pessoas idosas "promove a mudança social, a solução de problemas nas relações humanas e capacita as pessoas para melhorar seu bem-estar". No entanto, a evolução do hardware e do software também contribui para essas lacunas. Muitas pessoas idosas ainda têm dificuldades em usar seus navegadores de forma adequada e não sabem como ajustar as configurações de segurança em seus dispositivos, gerenciar o histórico de navegação, ou limpar o cache e os cookies da Internet (Grimes et al., 2010).

A conscientização sobre a segurança cibernética é crucial para as pessoas idosas como medida preventiva contra ataques cibernéticos (Brown et al., 2016). Sem o conhecimento adequado sobre ética online e segurança cibernética, as pessoas idosas estão mais suscetíveis a exploração por invasores. Vários casos relatam os impactos devastadores de ataques cibernéticos. Por exemplo, Jones (2001) descreveu que as vítimas de roubo de identidade entre as pessoas idosas enfrentam consequências graves, incluindo:

- Perda de todas as economias de uma vida
- Desespero por serem vítimas
- Diminuição da autoconfiança
- Exacerbação de doenças, que pode incluir morte prematura

Portanto, é essencial educar as pessoas idosas sobre práticas de segurança cibernética para evitar que se tornem alvos de ataques comuns. Essa educação não só os protege, mas também serve como um guia para uma navegação segura na Internet.

4.2 Ataques cibernéticos a pessoas idosas na pandemia

Os ataques cibernéticos contra as pessoas idosas tornaram-se um problema grave atualmente, devido à falta de conscientização sobre segurança cibernética e à vulnerabilidade a ameaças online. De acordo com Boral (2020), em 2020, foram identificados quatro tipos comuns de ataques cibernéticos direcionados as pessoas idosas: *phishing*, ataques comportamentais, ataques ao consumidor e roubo de identidade. As pessoas idosas são frequentemente os alvos preferenciais de fraudadores e criminosos cibernéticos, sendo classificados como os mais vulneráveis a golpes online. A falta de familiaridade com práticas seguras na Internet torna as pessoas idosas particularmente suscetíveis a essas ameaças.

A. Golpes de *phishing*

Phishing é a prática de falsificação de sites da Internet ou e-mails com o objetivo de enganar os usuários para que revelem informações confidenciais (Othman, 2020). Um estudo conduzido por Zhao et al. (2016) investigou a propensão das pessoas idosas a ataques de *phishing* baseados em computador. Os resultados mostraram que 53,47% dos idosos tinham uma alta probabilidade de se tornar vítimas de *phishing*, o dobro da taxa observada entre adultos mais jovens, que era de 26,37%. Além disso, 47,47% das pessoas idosas eram mais suscetíveis a ataques de *phishing* e frequentemente abaixavam a guarda quando estavam em casa. A pesquisa indica que as pessoas idosas enfrentam um risco elevado de ataques de *phishing*.

A maioria das técnicas de *phishing* emprega engenharia social e manipulação emocional, utilizando táticas como medo e curiosidade. O *phishing* pode ocorrer por meio de chamadas telefônicas, envio de SMS e e-mails. De acordo com o Relatório de Crimes na Internet IC3 2018 do FBI, a fraude de suporte técnico foi o crime de fraude que mais cresceu, resultando em perdas de aproximadamente US$ 39 milhões em 2018. As vítimas mais frequentes foram pessoas com mais de 60 anos (Zhao et al., 2016).

B. Fraude de romance

De acordo com a CyberSecurity Malaysia, o aumento no número de aplicativos de namoro online tem provocado um crescimento nos incidentes de golpes, pois milhares de dados de usuários ficam vulneráveis a criminosos. Esses golpistas frequentemente iniciam o contato com a vítima online e gradualmente estabelecem uma relação de confiança. As pessoas idosas são particularmente visados por esses golpes devido ao seu menor conhecimento tecnológico e à possibilidade de solidão.

Uma das técnicas utilizadas pelos golpistas é atrair as vítimas com promessas de entregas de pacotes caros e, em seguida, persuadi-las a transferir dinheiro (Boral, 2020). A CyberSecurity Malaysia relatou um aumento de 93% nos casos de spam entre janeiro e março de 2020, em comparação com o ano anterior. Além disso, houve um aumento de 34% nos incidentes de crimes cibernéticos reportados no mesmo período, em comparação com 2019.

De acordo com o relatório IC3 do FBI, em 2018, a fraude romântica foi a sétima fraude mais relatada e se tornou o segundo golpe mais oneroso em termos de perdas financeiras e reclamações recebidas. Os golpistas empregam uma estratégia de engano baseada na construção de uma relação de confiança com a vítima idosa, muitas vezes se fazendo passar por membros da família ou interesses amorosos. Eles estabelecem um relacionamento para persuadir a vítima a fornecer informações pessoais e financeiras, a realizar transações financeiras sem saber que está lavando dinheiro, ou a enviar dinheiro e comprar presentes caros. Esse tipo de crime cibernético frequentemente visa mulheres idosas solitárias, incluindo viúvas recentes.

C. Roubo de identidade

De acordo com Carlson (2006), o roubo de identidade pode manifestar-se de diversas formas, como por exemplo, roubo de identidade e o roubo de identidade do Seguro Social. Esse tipo de crime pode ocorrer sem a presença física da vítima, utilizando plataformas online ou até mesmo por telefone. O fraudador empregará todos os métodos disponíveis para obter as informações da vítima, como exemplificado a seguir:

- **Roubo de identidade**

Um criminoso rouba as informações do cartão da vítima, utilizado em algum site de compras camuflado, para pagar serviços, fazer pagamentos fraudulentos ou até mesmo fazer uma cobrança de serviço falsa e embolsar o dinheiro. Isso faz com que as vítimas fiquem potencialmente em um alto risco de endividamento e com uma dívida de milhares de reais.

- **Roubo da Previdência Social**

Outro exemplo é o roubo do Seguro Social é um dos tipos mais comuns de golpes telefônicos administrativos, enganando agressivamente as pessoas idosas. Por meio dessa técnica, os criminosos convencem a vítima sobre uma atividade fraudulenta que envolve o número do seu Seguro Social. Os criminosos alegam que são autoridades e ameaçam a vítima com falsas acusações legais se ela não seguir determinadas exigências. Outras consequências da obtenção das informações pessoais da vítima são que o impostor pode roubar o pagamento da renda da vítima.

4.3 Análise sobre a conscientização da segurança cibernética entre as pessoas idosas

Segundo C. Crane (2019) A segurança cibernética é o processo de proteger e recuperar sistemas, redes, dispositivos e programas de computador contra ataques cibernéticos. A conscientização sobre segurança cibernética, por sua vez, envolve educar os usuários da Internet sobre os riscos e perigos da proteção online, bem como melhorar sua compreensão dos riscos digitais para que possam se dedicar completamente à segurança ao usar a web. A segurança cibernética é crucial, pois garante que dados confidenciais e informações pessoais sejam protegidos contra o uso indevido por criminosos cibernéticos. Os criminosos cibernéticos frequentemente visam as pessoas idosas devido à falta de conhecimento e conscientização sobre os riscos digitais. Portanto, as pessoas idosas precisam estar mais atentos e informados sobre os perigos e riscos associados ao envolvimento no mundo cibernético em sua vida diária.

4.3.1 A importância da conscientização para as pessoas idosas

Devido a questões relacionadas à idade, as pessoas idosas podem ser mais suscetíveis a invasores que enviam mensagens de "confiança" que parecem legítimas para eles. Sem perceber o perigo, as pessoas idosas podem acabar divulgando seus dados pessoais, incluindo informações financeiras e médicas. Portanto, a conscientização sobre segurança cibernética é crucial para esse grupo. Essa conscientização pode ser promovida por meio de campanhas com vídeos ou atividades educativas. Com isso, as pessoas idosas poderão entender melhor e adotar práticas seguras ao usar a Internet, especialmente para se proteger contra ameaças online. Assim, é essencial que governos e comunidades colaborem para garantir que as pessoas idosas estejam plenamente informados sobre os possíveis perigos, como ataques de *phishing* e o uso

de redes Wi-Fi não seguras, além de aprenderem a minimizar os impactos de ataques cibernéticos.

Sem nenhuma estratégia de prevenção, as pessoas idosas podem ser comprometidos, ter sua identidade roubada e sofrer algumas consequências. Portanto, uma abordagem eficaz causará um enorme impacto na vida das pessoas idosas (Swee-Leng,et al, 2020).

De acordo com Jones (2001), há seis fatores que podem persuadir o comportamento de segurança das informações: i) conhecimento, ii) impacto, iii) gravidade, iv) controlabilidade, v) conscientização e vi) possibilidade. Para lidar com esse problema, é preciso conscientizar-se a respeito dele.

4.3.2 Recomendações para as pessoas idosas

Uma das estratégias preventivas mais eficazes para enfrentar crimes cibernéticos é a educação. A educação digital é uma abordagem crucial, especialmente voltada para usuários comuns da internet. Apesar de muitos participantes da pesquisa possuírem conhecimentos básicos sobre ameaças cibernéticas, ainda há um número significativo de vítimas de crimes cibernéticos. Para mitigar esses riscos, especialmente entre as pessoas idosas, é essencial implementar práticas educativas que aumentem a conscientização e a capacidade de proteção pessoal.

Com base na análise, destacam-se sete recomendações que podem ajudar a proteger as pessoas idosas e garantir uma navegação mais segura na internet:

I. ***Mantenha o software atualizado*** - A instalação e o uso de programas antivírus e antispyware são fundamentais para a proteção online. Esses softwares devem ser instalados corretamente e atualizados regularmente para garantir sua eficácia contra novas ameaças. Além disso, é essencial manter o sistema operacional e outros programas sempre atualizados, pois as atualizações corrigem falhas de segurança e fornecem patches que ajudam a prevenir ataques de hackers e outras vulnerabilidades.

II. ***Acesso seguro a contas*** - Para evitar que invasores roubem informações pessoais, as pessoas idosas devem ativar a autenticação de dois fatores sempre que possível ou oferecida e evitar compartilhar informações pessoais com estranhos. Também é importante usar senhas fortes evitando palavras comuns, datas de nascimento, números de identificação ou qualquer palavra que possa ser adivinhada. As senhas fortes são uma combinação de letras maiúsculas e minúsculas, números e símbolos.

III. ***Pense duas vezes antes de clicar*** - O e-mail é uma das principais ferramentas utilizadas por invasores para roubar informações pessoais de pessoas idosas. Recomenda-se que as pessoas idosas evitem responder a e-mails que solicitem informações confidenciais e desconfiem de links suspeitos, mesmo que pareçam ser de instituições legítimas, como bancos. Instituições financeiras nunca solicitam informações pessoais por e-mail; em caso de dúvida, o contato direto com a instituição é a melhor opção.

IV. ***Compras on-line e mídias sociais*** - Realizar compras online apenas em sites confiáveis é essencial. É importante verificar avaliações e classificações de outros usuários antes de finalizar uma compra. As pessoas idosas nunca devem compartilhar detalhes de cartões de crédito ou números CVV com terceiros. Em redes sociais, como Facebook, é importante desconfiar de "amigos" desconhecidos e evitar compartilhar informações pessoais, pois criminosos podem se passar por conhecidos para obter acesso a dados confidenciais.

V. ***Sistema de suporte*** - Se precisarem de ajuda, devem recorrer a uma instituição confiável, por exemplo, ligando para o atendimento ao cliente do banco, em caso de confusão se um e-mail, comunicação ou transação parecer errado. Eles também devem continuar se atualizando com relação à conscientização sobre segurança cibernética, pois isso pode ajudar a educar as pessoas idosas sobre golpes conhecidos e táticas para manter a cautela e ganhar mais confiança no uso da tecnologia.

VI. ***Ajuste de configurações de segurança do navegador*** - Configurar o navegador para o nível máximo de segurança é outra prática recomendada. Além disso, limpar regularmente o histórico de navegação pode ajudar a proteger a privacidade dos usuários.

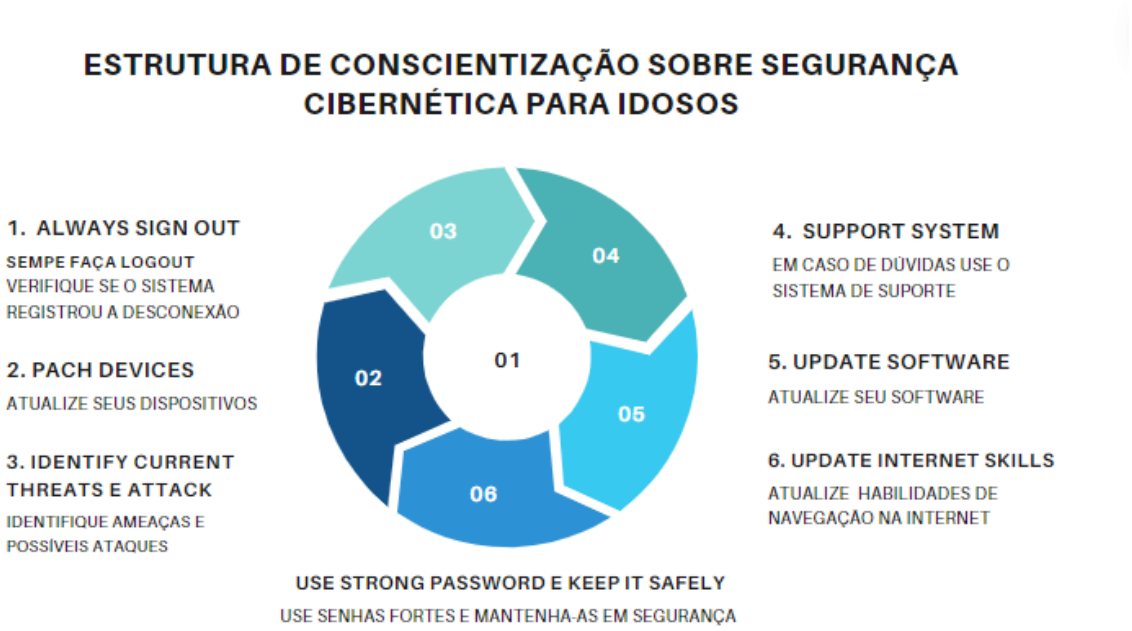
VII. ***Sair de contas e aplicativos após o uso*** - Lembrar-se de sair de aplicativos e sites ao terminar de utilizá-los é crucial. Deixar contas abertas pode expor o usuário a riscos de segurança e privacidade, facilitando o acesso de terceiros não autorizados.

4.3.3 A estrutura proposta

Após o processo de análise e síntese das informações levantadas, foi desenvolvida uma estrutura de conscientização voltada especificamente para as pessoas idosas, conforme apresentado na Figura 2. Essa estrutura trata-se de um esboço e busca abordar os principais fatores identificados como críticos para garantir que o nível de conscientização desse grupo alcance um padrão ideal. Espera-se que a estrutura sirva como base para o desenvolvimento de

políticas públicas e iniciativas educacionais mais robustas, voltadas à proteção desse público no ciberespaço. A finalidade é minimizar a incidência de crimes cibernéticos entre as pessoas idosas, promovendo uma navegação mais segura e confiante no ambiente digital. Espera-se que, no futuro, ela possa ser validada tecnicamente.

Figura 2 - Estrutura de conscientização sobre segurança cibernética para pessoas idosas



Fonte: Autoria própria (2024).

5 CONCLUSÃO

Este estudo teve como objetivo investigar a vulnerabilidade da população idosa a crimes cibernéticos durante a pandemia de COVID-19, com ênfase nas fragilidades específicas dessa faixa etária no ambiente digital. A pesquisa revelou que o aumento da participação das pessoas idosos no universo virtual expôs esse grupo a um crescimento alarmante de fraudes e crimes cibernéticos. Fatores como a redução das capacidades cognitivas, a falta de familiaridade com as tecnologias digitais e a dependência de plataformas online para interações cotidianas tornaram as pessoas idosas particularmente suscetíveis a ataques informáticos, conforme identificado por Barros e Leite (2019).

Apesar da existência de políticas públicas e iniciativas voltadas para a proteção da população idosa, a pesquisa evidenciou que a implementação prática dessas medidas enfrenta desafios substanciais, principalmente devido à velocidade das inovações tecnológicas e à constante evolução das modalidades de crimes cibernéticos. Como enfatizado por Souza

(2017), as políticas públicas devem evoluir em tempo real para responder de forma eficaz às novas ameaças. Contudo, a análise revelou um descompasso significativo entre a teoria e a prática, o que compromete a efetividade das estratégias de proteção direcionadas as pessoas idosas.

Peters (2015) afirma que políticas públicas eficazes precisam levar em consideração as complexidades do ambiente virtual e as vulnerabilidades específicas da população idosa. Para que essas políticas se tornem realmente eficazes, é essencial que seu desenvolvimento foque em soluções práticas, como a capacitação digital das pessoas idosas e campanhas educativas acessíveis e direcionadas, de modo a garantir que as medidas de segurança sejam compreendidas e aplicadas de forma efetiva.

A Política Nacional de Segurança Cibernética (PNCiber), embora representando um avanço considerável, ainda enfrenta desafios significativos para se adaptar de forma rápida e eficaz às novas ameaças digitais. Criada com o objetivo de fortalecer a segurança no ciberespaço brasileiro, a PNCiber tem o potencial de proteger a população idosa, mas sua implementação precisa ser mais eficaz e inclusiva. A estratégia de aplicação da PNCiber deve ser mais ágil, acompanhando as transformações tecnológicas de forma contínua, adotando ações específicas para proteger grupos vulneráveis, como as pessoas idosas. A ausência de uma abordagem mais direta e focada nas necessidades desse grupo impede que as políticas de segurança cheguem de forma eficiente a quem mais precisa delas.

Conclui-se que, para uma proteção digital eficaz, é imprescindível um aprimoramento urgente nas políticas de segurança cibernética voltadas para a população idosa. A PNCiber, como um instrumento central, deve ser revisada e adaptada regularmente, de modo a tornar-se mais ágil e eficiente, garantindo que as pessoas idosas possam navegar com segurança no ambiente online. As intervenções governamentais e institucionais precisam ser avaliadas e ajustadas de forma contínua, com foco na proteção digital de um grupo cada vez mais exposto às ameaças do ciberespaço.

REFERÊNCIAS BIBLIOGRÁFICAS

ABD RAHIM NH, HAMID S, KIAH ML, SHAMSHIRBAND S, FURNELL S. Uma revisão sistemática das abordagens para avaliar a conscientização sobre segurança cibernética. Kybernetes. 2015. Apr

ALEXANDRE JUNIOR, Edilson Campelo; NASCIMENTO, Volny Costa. **Mecanismos de prevenção.2020.** Disponível em: https://semanaacademica.org.br/system/files/artigos/artigo-_crimes_virtuais_edilson_campelo_alexandre_junior_e_volny_costa_do_nascimento.pdf Acesso em 29 set. 2023

ARAS, Vladimir. **Crimes de informática. Uma nova criminalidade.** 2015 Disponível em https://www.informatica-juridica.com/trabajos/crimes-de-informatica-uma-novacriminalidade/#_ftn18. Acesso em 20 out.2023

ALVES, Z. M. M. B., & Silva, M. H. G. F. D. da.. (1992). **Análise qualitativa de dados de entrevista: uma proposta. Paidéia** (ribeirão Preto), (2), 61–69. https://doi.org/10.1590/S0103-863X1992000200007. Acesso em 15 jun. 2024

AZEVEDO, L. F. **Políticas Públicas e Segurança Cibernética: Desafios e Perspectivas. Revista Brasileira de Segurança Digital**, v. 12, n. 1, p. 45-60, 2021.

BARDIN, L. (1977). **Análise de conteúdo**. Lisboa edições, 70,225.

BITENCOURT, Cezar Roberto. (**Tratado de direito penal, v. 3, p. 287**). São Paulo, Editora Saraiva, 2018. E-book. ISBN: 9788547224714 Disponível em: http://biblioteca2.senado.gov.br:8991/F/?func=itemglobal&doc_library=SEN01&doc_number=001140622. Acesso em 23 set. 2023.

BLACKWOOD-BROWN, C., LEVY, Y., TERRELL, S. (2016). **Cidadãos idosos e conscientização sobre segurança cibernética.** An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Institui a Política Nacional de Segurança Cibernética – PNCiber. Diário Oficial da União, 2020.

BRASIL. Superior Tribunal de Justiça. Súmula Vinculante. Súmula Vinculante n.48. Plenário. Brasília, data. 25 de agosto de 1992 Disponível em: https://www.coad.com.br/busca/detalhe_16/833/Sumulas_e_enunciados Acesso em 25 set. 2023

CAMPOS, J. L., Silva, T. C., & Albuquerque, U. P. (2021). **Observação participante e diário de campo: quando utilizar e como analisar. Métodos de pesquisa qualitativa** para etnobiologia. Recife: Nupeea, 95-112.

CARLSON EL. **Phishing para vítimas idosas**: à medida que os idosos migram para a Internet, surgem esquemas fraudulentos direcionados a eles. Elder LJ. 2006; 14:423.

CARLTON M, LEVY Y. **Avaliação de especialistas sobre as principais habilidades de segurança cibernética independentes de plataforma para profissionais que não são de TI**. In Southeast Con (2015) 2024 Apr 9 (pp. 1-6). IEEE.

C. CRANE, 3 Cyber Fraud Tactics Targeting Seniors and Why They are So Effective (**3 táticas de fraude cibernética que visam idosos e por que são tão eficazes**). Revista CyberCrime, 2019.Acessado em: 09.29.2023 Disponível em:https://cybersecurityventures.com/3- cyber-fraud-tactics-targeting-seniors-and-why-theyre-so-effective/

CHANG FR. Depoimento escrito do Dr. Frederick R. Chang, Presidente Distinto do Centenário Bobby B. Lyle em Segurança Cibernética da Southern Methodist University. Jun 1, 2017.

CHOO KK. **O cenário das ameaças cibernéticas**: Challenges and future research directions. Computers & security. 2011 Nov 1;30(8):719-31.

CLAAR CL, JOHNSON J. Analyzing home PC **security adoption behavior**. Journal of Computer Information Systems. 2012 Jun 1;52(4):20-9.

CRAIGEN D, DIAKUN-THIBAULT N, Purse R. **Defining cybersecurity** (Definindo a segurança cibernética). Technology Innovation Management Review. 2014;4(10).

CRESWELL, J. W. (2010). **Qualitative Inquiry and Research Design**: Choosing Among Five Approaches (2nd ed.). Sage Publications.

DEIBERT, R. J.; ROHOZINSKI, R. Risking Security: **Policies and Paradoxes of Cyberspace Security. International Political Sociology**, Toronto, v. 4, n. 1, p.15-32, 2010.

DIEHL, Astor Antônio; TATIM, Denise Carvalho. **Pesquisa em ciências sociais aplicadas**: métodos e técnicas. São Paulo: Prentice Hall, 2004.

DUARTE, D. K. B. F.; & Junior, J. A. P. D. (s.d). **Os crimes digitais sob a vertente do Código Penal brasileiro.** https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9a0000018173fbd6d4f23cdf3c&docguid=Ia6328bb085b611e4ad6a010000000000&hitguid=Ia6328bb085b611e4ad6a010000000000&spos=1&epos=1&td=158&context=5&crumb-action=append&crumblabel=Documento&isDocFG=true&isFromMultiSumm=true&startChunk=1&endChunk=1.

DYE, Thomas R. *Understanding Public Policy.* Boston: Pearson Education, 2013

FALKEMBACH EMF. 1987. **Diário de campo: um instrumento de reflexão**. Contexto Educação, Ijuí 7(2):19-24

FLICK, U. (2018). **An Introduction to Qualitative Research** (6th ed.). Sage Publications.

GIDDENS, **A. Sociologia**. Tradução de Alexandra Figueiredo; Ana Patrícia Duarte Baltazar; Catarina Lorga da Silva; Patrícia Matos; Vasco Gil. 6.ed., Lisboa: Fundação Calouste Gulbenkian, 2008.

GERHARDT, Tatiana Engel. SILVEIRA, Denise Tolfo (Org). **Métodos de pesquisa**. Porto Alegre: Editora da UFRGS, 2009. Disponível em: http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf. Acesso em 27 out. 2023.

GOLDONI, L. R. F.; RODRIGUES, K. F.; MEDEIROS, B. P. **Qual é o futuro da governança de cibersegurança no Brasil?** *Cadernos de Gestão Pública e Cidadania*, v. 25, 2020.

GRIMES GA, Hough MG, Mazur E, SIGNORELLA ML. **O conhecimento dos adultos mais velhos sobre os riscos da Internet**. Educational Gerontology. 2023 Feb 11;36(3):173-92.

GSI. Centro de Defesa Cibernética. Disponível em: https://www.gov.br/gsi/pt-br/ssic. Acesso em: 24 jun. 2024.

GUAZI, T. S. **Diretrizes para o uso de entrevistas semiestruturadas em investigações científicas**. Revista Educação, Pesquisa e Inclusão, [S. l.], v. 2, 2021. DOI: 10.18227/2675-3294repi.v2i0.7131. Disponível em: https://revista.ufrr.br/repi/article/view/e202114. Acesso em: 20 jun. 2024.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE)**.** ***Censo Demográfico 2022: Resultados Preliminares***. Rio de Janeiro, 2023. Disponível em: https://www.ibge.gov.br. Disponível em: https://www.ibge.gov.br. Acesso em: 25/10/2023.

INTERNET CRIMES COMPLAINT CENTER (IC3). **Internet crime complaint center 2018** report. Washington, D.C.: Federal Bureau of Investigation (FBI), 2018. Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2018_IC3Report.pdf. Acesso em: 20 jun 2024.

IYER R, EASTMAN JK. **The elderly and their attitudes towards the internet: the impact on internet use**, purchase, and comparison shopping. Journal of Marketing Theory and Practice. 2006 Jan 1;24(1):57-67.

JOEL HOLMBERG (2022, 23 de janeiro). Real Facts about the Elderly and the World Wide Web (**Fatos reais sobre os idosos e a rede mundial de computadores**). Disponível em: https://axesslab.com/real-facts-about- the-elderly-and-the-world-wide-web/.

JONES, T. L. (2001). Protecting the elderly. Law & Order, 49(4), 102-106

JURGEN, S. **Entrevista concedida à Interpol**. 04 ago. 2020. Disponível em: <https://www.interpol.int/News-and-Events/News/2020/INTERPOLreport-shows-alarming-rate-of-cyberattacks-during-COVID-19>. Acesso em: 06 out. 2023.

JUSTINO, P. B; ARRUDA, E. M. C. A LGPD, **os cibercrimes e a adesão do Brasil à Convenção de Budapeste** In: LIMA, P. A. L.; ARRUDA, C. M. M.; VILAR-LOPES, G.; GUIMARÃES, R. C. P. de P. (orgs). Anais. II Seminário de Segurança e Defesa Cibernética: desafios da defesa cibernética na projeção espacial brasileira. Rio de Janeiro: Universidade da Força Aérea, p. 159-184, 2020.

KASPERSKY. **Brasileiros são maiores vítimas de golpes phishing no mundo**. 2018. Disponível em: https://www.kaspersky.com.br/blog/phishing-

klsecbrasilassolini/10642/?utm_source=newsletter&utm_medium=Email&utm_campaign=kd%20weekl. Acesso em: 06 nov. 2023.

KINGDON, John W**.** *Agendas, Alternatives, and Public Policies.* 2nd ed. New York: HarperCollins, 2011.

KÖNIG, R., Seifert, A. & Doh, M. Internet use among older Europeans: an analysis based on SHARE data (**Uso da internet entre europeus mais velhos: uma análise baseada em dados do SHARE**). Univ Access Inf Soc 17, 621-633 (2024). https://doi.org/10.1007/s10209-018-0609-5

LAVILLE, C., & Dionne, J. (1999). **L'analyse documentaire** (2nd ed.). Armand Colin

LEWGOY AMB, Arruda MP. 2004. Novas tecnologias na prática profissional do professor universitário: **a experiência do diário digital**. Revista Textos e Contextos 2:115-130

LIMA, Lorenna. **Breve história dos direitos no Brasil e no mundo**, SITE. 2019, Disponível em: https://jus.com.br/artigos/71311/breve-historico-dos-direitos-dosidosos-no-brasil-e-no-mundo.>Acesso em: 4 out. 2023

LÜDKE, Menga; André, Marli E.D.A. **Pesquisa em Educação**: Abordagens Qualitativas. São Paulo: EPU, 1986.

NAGLI, L. **Pandemia na pandemia: a escalada de ataques cibernéticos pós covid-19**. Congresso Transformação Digital, 2020.

NUCCI, Guilherme de Souza. Curso de Direito Penal - Parte Especial - Vol. 2. São Paulo Grupo GEN, 2021. E-book. ISBN 9786559640157. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559640157/. Acesso em: 28 set. 2023.

NURSE, JASON. (2018). **O crime cibernético e você**: How Criminals Attack and the Human Factors That They Seek to Exploit (Como os criminosos atacam e os fatores humanos que eles procuram explorar). 10.1093/oxfordhb/9780198812746.013.35.

N.Z. OTHMAN, (2020, 14 de fevereiro). #TECH: **Muitos corações solitários ainda estão se apaixonando por falsos amantes on-line**. Novo Straits Times. Disponível em https://www.nst.com.my/lifestyle/bots/2023/06/565459/tech-many-lonely-hearts-arestill-falling-online-f ake-lovers

MENDES, G. F. (2017). Série IDP – **Manual dos direitos da pessoa idosa** - DIG. São Paulo: Editora Saraiva, p. 477-497

MENDES KDS, SILVEIRA RCCP, GALVÃO CM. Revisão integrativa: **método de pesquisa para a incorporação de evidências na saúde e na enfermagem**. Texto Contexto Enferm. 2008;17(4):758-64. doi: https://doi.org/10.1590/S0104-07072008000400018

MINAYO MCS, DESLANDES SF, NETO OC, GOMES R. 2002. **Pesquisa Social: Teoria, Método e Criatividade**. Petrópolis, Editora Vozes

MIRABETE, Julio Fabrinni; Fabrini, Renato N. Manual de Direito Penal; parte especial; 25ª Edição, Atlas, São Paulo, 2004.

MORGAN, J. A. (2015). **Exploring Senior Citizen Perceptions of Their Cyber Data Privacy and Security** (Dissertação de doutorado, Capella University

PEREIRA, Carolina da Silva. **A Política Nacional de Segurança Cibernética: desafios e perspectivas**. *Revista de Estudos de Políticas Públicas*, Florianópolis, v. 26, n. 2, p. 123-140, 2020.

PETERS, B. Guy. **American Public Policy**: Promise and Performance. 9. ed. New York: Routledge, 2015.

PINHEIRO, Patrícia. P. Direito Digital. São Paulo: Saraiva, 2021. 9786555598438. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 26 out. 2023.

PINHEIRO, PATRICIA PECK. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**– 2. ed. – São Paulo : Saraiva Educação, 2020.

RITCHIE J. 2003. **The Applications of Qualitative Methods to Social Research**. In: Ritchie J, Lewis J. (eds.) Qualitative Research Practice: A Guide for Social Science Students and Researchers. London, Sage publications. p.24-46.

S. BORAL, 4 Most Common Cyber Attacks Used Against Older People in 2020 **(4 ataques cibernéticos mais comuns usados contra pessoas idosas em 2020)**, 2020. Accessed on:09.29,2023. Disponível em: https://www.maketecheasier.com/common-cyber-attacks-used-against-senior-citizens/

SILVA, Edna Lúcia, Estera Muszkat Menezes. **Metodologia da pesquisa e elaboração de dissertação**. – 4. ed. rev. atual. – Florianópolis: UFSC, 2005.

SILVA, R. M. **A Implementação da LGPD e o Papel dos Centros de Resposta a Incidentes. Jornal de Direito e Tecnologia**, v. 8, n. 2, p. 112-130, 2022.

SOUZA, Celina. **Políticas Públicas: Conceitos, Contextos e Desafios**. 3. ed. Brasília: Editora Universidade de Brasília, 2017.

TEIXEIRA, T. **Direito Digital e Processo Eletrônico**. Editora Saraiva, 2020. , São Paulo. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555591484/. Acesso em: 17 OUT 2023.

TRIVIÑOS ANS. 1987. Introdução à Pesquisa em Ciências Sociais: **A Pesquisa Qualitativa em Educação**. São Paulo, Ática.

VIEIRA GUIMARÃES LIMA, Cláudio. **CRIMES CIBERNÉTICOS O LADO OBSCURO DA REDE**. 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/2419. Acesso em 25 out 2023.

ZHAO R, JOHN SE, KARAS S, BUSSELL CA, ROBERTS J, SIX D, ET AL. **Os ataques de phishing extremos altamente insidiosos**. Proc IEEE Int Conf Comput Commun Networks (ICCCN); 2016.