ISBN: 978-85-61702-73-1

DOI: 10.46943/X.CIEH.2023.01.067

DEEPFAKE E CIBERSEGURANÇA DAS PESSOAS IDOSAS: CONTRIBUIÇÕES DA PSICOGERONTECNOLOGIA

Davi Ítalo Souza Barbosa da Silva[1]
Gabriel Medeiros[2]

RESUMO

Introdução: O termo *deepfake* refere-se à criação ou edição de conteúdo audiovisual falso, por meio da aplicação de algoritmos de inteligência artificial, para simular de forma realista situações que não ocorreram originalmente. A proliferação dos *deepfakes* apresenta um desafio considerável no campo da cibersegurança, sobretudo para a parcela idosa da população. A crescente digitalização da sociedade expõe as pessoas idosas a riscos substanciais devido à sua menor familiaridade com as tecnologias digitais e sua predisposição à confiança, tornando-os alvos propensos a fraudes *online*. Este estudo tem como objetivo analisar o impacto dos *deepfakes* na cibersegurança das pessoas idosas, identificando as ameaças específicas e propondo estratégias para mitigar esses riscos. **Metodologia:** Foi realizada uma revisão narrativa da literatura sobre *deepfakes*, cibersegurança e envelhecimento digital. **Resultados:** Observamos que a população idosa são alvos vulneráveis de golpes de phishing baseados em *deepfakes*, resultando em perdas financeiras e invasões de privacidade. Além disso, a literatura demonstra uma lacuna no conhecimento das pessoas idosas sobre *deepfakes* e táticas de engenharia social, bem como sua tendência a confiar em

1 Mestre em Psicologia Clínica pela Universidade Católica de Pernambuco - PE, davi.2022605169@unicap.br;

2 Doutor e mestre em Psicologia, Docente pela Faculdade Frassinetti do Recife - PE, antonioa@prof.fafire.br;

ISBN: 978-85-61702-73-1

informações *online* sem verificação. A conscientização emerge como uma ferramenta-chave na mitigação dos riscos de *deepfakes*. Iniciativas educativas direcionadas são essenciais para capacitá-los a identificar conteúdo falso e adotar comportamentos de segurança *online*. **Considerações:** A interseção entre deepfakes e cibersegurança exige ação imediata e coordenada. O estudo destaca a necessidade de estratégias educativas e tecnológicas para fortalecer a resiliência, a autonomia e a autoeficácia da população idosa na era digital, assegurando sua proteção e bem-estar em um ambiente tecnológico em constante evolução.

Palavras-chave: Deepfake, Cibersegurança, Ciberpsicologia, Psicogerontecnologia

ISBN: 978-85-61702-73-1

INTRODUÇÃO

A psicogerontecnologia é um campo interdisciplinar que visa aplicar tecnologias, principalmente da área de informação e comunicação, para atender às necessidades da população idosa e melhorar sua qualidade de vida. Essa abordagem combina princípios da psicologia, gerontológica com inovações tecnológicas, reconhecendo as dimensões psicológicas do envelhecimento (MELO *et al.,* 2022).

No contexto da assistência à saúde, a psicogerontecnologia pode se manifestar por meio de monitoramento da saúde, telemedicina e dispositivos que auxiliam na administração de medicamentos. Na esfera da comunicação e interação social, utiliza redes sociais, videochamadas e plataformas digitais para mitigar o isolamento social comum em idosos. Além disso, oferece soluções para treinamento cognitivo, como aplicativos e jogos destinados a preservar e aprimorar as habilidades cognitivas (MELO *et al.,* 2022).

Facilitar o acesso à informação é outra vertente importante, proporcionando às pessoas idosas meios de explorar notícias, serviços online e recursos educacionais. A psicogerontecnologia também se dedica à adaptação residencial, implementando tecnologias que tornam os ambientes mais seguros, como sistemas de alerta e automação residencial. No âmbito do entretenimento, desenvolve conteúdos adaptados, como filmes, músicas e jogos, adequados às preferências e limitações dos idosos (MELO *et al.,* 2022).

A acessibilidade é uma preocupação constante, com a adoção de tecnologias que tornam dispositivos eletrônicos e interfaces mais amigáveis, levando em consideração aspectos como visão, audição e destreza manual. Integrando psicologia e tecnologia, a psicogerontecnologia busca criar soluções culturalmente sensíveis, respeitando a autonomia e a dignidade dos idosos, e proporcionando uma experiência enriquecedora no processo de envelhecimento (MELO *et al.,* 2022).

Nas últimas décadas, a introdução e a rápida expansão das Tecnologias Digitais de Informação e Comunicação (TDICs) alteraram substancialmente o contexto mundial. As TDICs incluem uma ampla

ISBN: 978-85-61702-73-1

gama de tecnologias, como smartphones, tablets, computadores, redes sociais, jogos online, entre outras. Nesse sentido, podemos compreender as TDICs tanto no âmbito dos *hardwares* quanto *softwares*.

O surgimento e a disseminação dessas tecnologias foram impulsionadas, principalmente, pela inovação tecnológica e pela globalização. A popularização da internet, o desenvolvimento de dispositivos móveis e o advento das redes sociais contribuíram para uma interconectividade sem precedentes (SCHEMER et al., 2021).

As TDICs são multifuncionais, sendo utilizadas para diversos propósitos, desde a comunicação com amigos e familiares até o acesso a informações, entretenimento e educação. A presença das redes sociais, como o WhatsApp, Facebook, Instagram e TikTok, consolidou-se como um meio fundamental para a construção de identidade e socialização dos indivíduos. (FERNANDEZ; DONARD, 2016).

No entanto, entre os grupos que mais experimentaram essa revolução, destaca-se a população idosa. Muitas vezes, eles são considerados "imigrantes digitais", uma vez que entraram no mundo das TDICs em uma fase posterior da vida em comparação aos chamados "nativos digitais" que já nasceram em um ambiente naturalmente tecnológico. O uso crescente de TDICs por pessoas idosas têm apresentado impacto significativo na qualidade de vida e na comunicação (SCHUARTZ; SARMENTO, 2020).

O advento das TDICs propiciou benefícios para a população idosa. O acesso à internet e o uso de dispositivos móveis possibilitaram a comunicação mais rápida e eficaz com familiares e amigos, independentemente da distância. Isto pode reduzir sentimentos de solidão e isolamento, uma preocupação importante nesta população. Além disso, as TDICs oferecem oportunidades de aprendizado contínuo e entretenimento, com uma infinidade de recursos, como cursos *online*, jogos interativos e redes sociais, mantendo o cérebro ativo e mais engajado nas atividades. A telemedicina também tem desempenhado um papel vital ao permitir consultas médicas à distância, tornando o acesso à assistência médica mais conveniente (NÄSI; KOIVUSILTA, 2013).

No contexto brasileiro, o uso de TDICs entre os idosos está aumentando. Segundo o Comitê Gestor da Internet no Brasil (CGI.br), a pesquisa

ISBN: 978-85-61702-73-1

TIC Domicílios realizada pelo Núcleo de Informação e Coordenação do Ponto Brasil (2019) revelou que 58% dos brasileiros com 60 anos ou mais usavam a internet, o que representa um aumento significativo em relação a anos anteriores. O acesso à internet permite que os idosos acessem informações, serviços e recursos valiosos que podem melhorar sua qualidade de vida. Além disso, pela maior familiaridade, o celular tende a ser a TDIC mais acessível (GAMA-VIEIRA et al., 2022).

Entretanto, o padrão de uso das TDICs entre os idosos brasileiros varia consideravelmente. Alguns são ávidos consumidores de conteúdo *online*, enquanto outros podem usar a tecnologia apenas de forma esporádica. Além disso, a literacia digital entre a população idosa pode variar, influenciando a eficácia e a segurança de seu uso. Alguns fatores como ao baixo letramento digital, falta de acessibilidade e as limitações físicas e cognitivas atreladas à idade são alguns dos responsáveis pelas resistências ao uso das TDIC's pelas pessoas idosas (GAMA-VIEIRA *et al.,* 2022*).*

Apesar dos benefícios, as TDICs também apresentam riscos, com a população idosa potencialmente vulnerável. Um risco emergente é a disseminação de *deepfakes*, que são manipulações de áudios e vídeos usando inteligência artificial para criar conteúdo enganoso e realista. Essa tecnologia pode ser usada para espalhar informações falsas e enganosas, tornando os idosos alvos de golpes e fraudes *online*. À medida que os *deepfakes* se tornam mais sofisticados, a capacidade de discernir entre informações reais e falsas se torna uma tarefa cada vez mais desafiadora (WANG, 2022).

Os *deepfakes* representam uma faceta notável da inteligência artificial, sendo a criação ou manipulação de conteúdo audiovisual, como vídeos e áudios, de forma a simular situações que não ocorreram originalmente. A base para a elaboração de *deepfakes* reside na aplicação de algoritmos de aprendizado profundo, que permitem a sobreposição de características faciais e vocais de uma pessoa em um conteúdo existente. Isso resulta em representações extremamente realistas, muitas vezes indistinguíveis de gravações autênticas. Essa tecnologia tem encontrado usos tanto positivos quanto negativos (WANG, 2022).

ISBN: 978-85-61702-73-1

Em relação aos usos adaptativos, os *deepfakes* têm demonstrado potencial em áreas como o entretenimento, permitindo a criação de dublagens precisas e revivendo a memória de artistas falecidos. No campo da educação, a tecnologia pode ser utilizada para simular aulas com professores ilustres ou facilitar o aprendizado de idiomas. Além disso, no setor de saúde, os *deepfakes* podem ser empregados para melhorar terapias de fala e comunicação. Contudo, a mesma tecnologia que oferece essas oportunidades também traz consigo riscos significativos, e a população idosa está particularmente vulnerável a esses riscos (CHADHA, 2021).

O aumento da digitalização da sociedade tem exposto o público idoso a ameaças à segurança. Estas englobam a criação de mensagens de *phishing* altamente convincentes, levando as pessoas idosas a fornecer informações pessoais e financeiras sensíveis. *Phishing* pode ser definido como uma prática fraudulenta online que envolve a tentativa de enganar usuários para obter informações pessoais e sensíveis, como senhas, detalhes de cartões de crédito e outras informações confidenciais (KWOK; KOH, 2021).

Geralmente, os criminosos cibernéticos se passam por entidades confiáveis, como bancos, empresas ou órgãos governamentais, e enviam mensagens eletrônicas persuasivas, como e-mails ou mensagens de texto, induzindo as vítimas a clicar em links maliciosos ou fornecer suas informações diretamente. O objetivo final do phishing é realizar atividades fraudulentas, como roubo de identidade, acesso não autorizado a contas ou instalação de malware nos dispositivos das vítimas. Além disso, as vítimas de *deepfakes* frequentemente sofrem perdas financeiras substanciais, uma vez que a identidade falsa do golpista é quase indistinguível da de uma pessoa legítima, tornando difícil para as vítimas identificarem o engano (KWOK; KOH, 2021).

Os *deepfakes* também podem ser utilizados para a criação de vídeos falsos com alto grau de realismo, resultando em invasões de privacidade. Estes, frequentemente difamatórios e prejudiciais, podem impactar negativamente a imagem e a reputação das pessoas idosas, causando danos significativos. Além disso, a literatura científica demonstra que as

ISBN: 978-85-61702-73-1

pessoas idosas frequentemente possuem conhecimento limitado sobre *deepfakes* e as técnicas de engenharia social envolvidas na criação deste tipo de conteúdo. Soma-se a isso sua tendência a confiar em informações *online* sem realizar verificações adequadas, tornando-as particularmente vulneráveis a essas ameaças (RANA, 2022).

Diante desse cenário desafiador, é crucial desenvolver estratégias eficazes para proteger a população idosa dos riscos associados às TDICs e, em particular, aos *deepfakes*. Para mitigar tais ameaças, é necessário um enfoque abrangente e interdisciplinar, combinando cibersegurança com princípios da psicogerontologia, que se debruçam sobre os aspectos psicológicos do envelhecimento.

A educação pode desempenhar um papel central na proteção das pessoas idosas contra os perigos *online*, especialmente em relação aos *deepfakes*. Iniciativas educacionais direcionadas podem ser desenvolvidas para capacitá-los a identificar conteúdo falso, reconhecer tentativas de phishing e adotar comportamentos de segurança digital. Essa abordagem educacional personalizada pode ser considerar as características específicas da população idosa, levando em conta fatores como literacia digital e confiança nas informações disponibilizadas virtualmente.

Ao integrar a psicogerontologia nesse contexto, é possível compreender melhor as nuances psicológicas que tornam idosos mais suscetíveis a certos tipos de ataques. Considerar aspectos cognitivos, emocionais e sociais pode fortalecer a resiliência, a autonomia e a autoeficácia na era digital.

A cibersegurança, por sua vez, pode desempenhar um papel crucial na identificação, prevenção e resposta a ataques *online*. A constante evolução das tecnologias exige que as medidas de segurança se adaptem para enfrentar ameaças emergentes, como os *deepfakes*.

Estratégias de autenticação robustas, sistemas de detecção de fraudes e aprimoramentos na segurança das plataformas *online* são essenciais para garantir a proteção das pessoas idosas.

Uma abordagem interdisciplinar que combina cibersegurança e psicogerontologia pode fornecer soluções abrangentes para fortalecer a resiliência, a autonomia e a autoeficácia da população idosa na era

ISBN: 978-85-61702-73-1

digital. Nesse sentido, este estudo tem como objetivo analisar o impacto dos *deepfakes* na cibersegurança das pessoas idosas, identificando as ameaças específicas e propondo estratégias para mitigar esses riscos.

METODOLOGIA

Este estudo constitui uma pesquisa de revisão narrativa sobre o impacto dos *deepfakes* na cibersegurança de pessoas idosas, além das contribuições da psicogerontecnologia nesta discussão. Uma revisão narrativa é um método de análise e interpretação de evidências disponíveis em um determinado fenômeno, empregando uma estratégia de pesquisa exploratória (CORDEIRO et al., 2007).

O principal propósito de uma revisão narrativa é fornecer uma visão abrangente e contextualizada de um tema específico, integrando uma variedade de fontes, como estudos de pesquisa, teorias e conceitos relevantes. Essa abordagem possibilita aos pesquisadores explorar a complexidade e diversidade de um campo particular, considerando diferentes perspectivas, metodologias e resultados (CORDEIRO et al., 2007) .

A revisão narrativa, ao contrário de revisões sistemáticas mais estruturadas, oferece uma flexibilidade que permite uma análise mais holística e contextualizada do tema. Isso se alinha perfeitamente ao propósito deste estudo, visto que buscamos compreensão holística da complexidade subjacente à interação entre os *deepfakes*, cibersegurança e o público idoso, além da literatura escassa sobre o tema.

A coleta de dados ocorreu no período de 02 a 30 de agosto de 2023, utilizando as bases de dados Literatura Latino-Americana e do Caribe em Ciências da Saúde (LILACS-BVS), *Scientific Eletrônic Library Online* (SCIELO) e *National Library of Medicine* (PUBMED). Foram identificados um total de 10 artigos em periódicos, considerando os descritores relacionados a *deepfakes* e cibersegurança de pessoas idosas em variantes em inglês e português.

O critério de inclusão adotado foi a publicação dos artigos entre os anos de 2002 e 2023, devido à percepção de uma lacuna na abordagem desse tema nesse intervalo temporal. Como critério de exclusão,

ISBN: 978-85-61702-73-1

foram descartados artigos incompletos, resumos de congressos, resumos expandidos e trabalhos que não guardavam relação com o tema central deste estudo ou que fugiam da linha de interesse.

RESULTADOS E DISCUSSÕES

Os *deepfakes* emergem como uma crescente tensão de ciber risco, representando uma ameaça significativa para a segurança digital de todas as pessoas. No entanto, as pessoas idosas se destacam como uma população particularmente suscetível a esses ataques, demandando uma atenção especial devido à sua menor familiaridade com as tecnologias digitais e maior propensão à confiança. Pesquisas recentes, como o estudo de Jin (2020), destacam que a suscetibilidade dos idosos a ciberataques por *deepfake* está intrinsecamente ligada à falta de conhecimento sobre as tecnologias digitais e às suas práticas *online*. Além disso, essas pessoas muitas vezes tendem a confiar em informações *online* sem a devida verificação, tornando-as alvos propensos a fraudes digitais (CRIPPEN, 2023).

A conscientização dos riscos digitais é fundamental para fortalecer a cibersegurança da população idosa, especialmente diante da crescente ameaça representada pelos *deepfakes*. Autores como Sudhakar e Shanthi (2023) ressaltam que a falta de conhecimento sobre os perigos digitais contribui significativamente para a vulnerabilidade de pessoas idosas a ataques cibernéticos, incluindo a manipulação por meio de *deepfakes*. Programas educacionais específicos para essa faixa etária, conforme proposto por Bray et al. (2023), têm emergido como estratégia eficaz.

Esses programas abrangem desde a identificação de *deepfakes* até a compreensão mais ampla dos riscos associados à divulgação de informações pessoais *online*. A pesquisa destaca a importância não apenas de informar, mas de capacitar os idosos, permitindo que tomem decisões mais conscientes em seu envolvimento digital. Além disso, a conscientização direcionada à identificação de conteúdo falso se mostra crucial. Estratégias práticas, como exemplos específicos e simulações, são incorporadas aos programas educacionais para aprimorar a capacidade dos

ISBN: 978-85-61702-73-1

idosos em discernir entre informações autênticas e fraudulentas, especialmente quando se deparam com *deepfakes* (BRAY et al., 2023).

Outro ponto relevante destacado pela pesquisa, também evidenciado por Chi et al. (2021), é a necessidade de promover práticas seguras digital. Isto inclui orientações práticas, como a configuração de senhas robustas, a atualização regular de software e o uso de medidas de segurança. Ao abordar esses aspectos, a conscientização não apenas possibilita proteção contra ameaças cibernéticas, mas também capacitação para usufruto dos benefícios da era digital com confiança e segurança.

Desta forma, a conscientização dos riscos digitais emerge como uma ferramenta valiosa na promoção da cibersegurança para as pessoas idosas. Integrando conhecimento específico, orientações práticas e uma mentalidade crítica, esses programas têm o potencial de fortalecer uma postura defensiva no ambiente digital, contribuindo para uma experiência segura e confiável.

O aumento da autoeficácia digital em pessoas idosas também pode desempenhar um papel crucial na promoção da cibersegurança, especialmente diante das ameaças representadas pelos *deepfakes*. A autoeficácia digital refere-se à confiança e competência de um indivíduo ao lidar com tarefas relacionadas à tecnologia e ao ambiente digital (ARPASI, 2022).

Estudos como o de Pacherrez (2022) destacam que a autoeficácia digital está diretamente associada à capacidade de enfrentamento eficaz diante dos desafios cibernéticos. Em um contexto de *deepfakes*, onde a manipulação de conteúdo visual e auditivo pode induzir confusão e desinformação, a autoeficácia digital torna-se uma defesa essencial. Programas de capacitação digital, como sugerido por Manyam (2022), visam não apenas fornecer conhecimento técnico, mas também desenvolver a confiança dos idosos em suas habilidades de navegação e discernimento *online*. A literatura destaca que a autoeficácia digital não é apenas uma competência técnica, mas uma atitude psicológica que influencia a disposição de um indivíduo para enfrentar desafios digitais.

Estratégias que visam o aumento da autoeficácia digital incluem a criação de ambientes de aprendizado personalizados, fornecendo feedback positivo e encorajador, e integrando experiências práticas no uso

ISBN: 978-85-61702-73-1

de tecnologias digitais. Nesse sentido, Wang *et al.* (2021) ressaltam a importância de abordagens que levem em consideração a autoeficácia percebida, ou seja, a crença do indivíduo em sua capacidade de realizar tarefas específicas relacionadas à tecnologia.

Ao fortalecer a autoeficácia digital, os idosos se tornam mais resilientes diante de potenciais ameaças, como *deepfakes*. A confiança em suas habilidades de discernimento e a capacidade de adotar medidas preventivas são essenciais para uma participação segura e confiante no mundo digital. Portanto, o aumento da autoeficácia digital em pessoas idosas não apenas contribui para a proteção contra ciberataques, mas também promove uma integração mais positiva e proveitosa no ambiente digital, capacitando os idosos a usufruir dos benefícios da tecnologia de maneira segura e eficaz.

A interação e apoio entre gerações em pessoas idosas pode desempenhar um papel fundamental na promoção da cibersegurança, especialmente diante das crescentes ameaças representadas pelos *deepfakes*. Essa abordagem reconhece a importância das relações familiares e sociais na defesa contra possíveis riscos cibernéticos, proporcionando um ambiente de suporte e colaboração. Pesquisadores como Gonçalves e Patrício (2010) destacam que a interação intergeracional pode funcionar como uma linha de defesa eficaz contra ameaças *online*. A transmissão de conhecimento digital de geração para geração cria um ambiente em que os idosos podem se beneficiar da experiência e habilidades digitais dos membros mais jovens da família.

A pesquisa de Colibaba e Gheorghiu (2015) salienta que a presença de relações de apoio nas interações *online* pode ser um fator crucial para aumentar a segurança digital. Quando os idosos têm acesso a uma rede de apoio, que pode incluir filhos, netos ou outros membros da família, tornam-se mais capacitados a reconhecer e responder a possíveis ameaças, como *deepfakes*. Programas de treinamento intergeracionais, nos quais os membros mais jovens da família auxiliam os idosos na navegação segura na internet e na identificação de possíveis riscos, podem ser. Essa abordagem pode não apenas aumentar a conscientização sobre cibersegurança, mas também fortalece os laços familiares e a sensação de

ISBN: 978-85-61702-73-1

apoio, fatores essenciais para o bem-estar digital dos idosos (PATRÍCIO; OSÓRIO, 2011).

O apoio intergeracional não se limita apenas ao aspecto técnico, mas também abrange o desenvolvimento de habilidades críticas, como a avaliação de conteúdo *online* e a promoção de comportamentos seguros na internet. A criação de um ambiente em que os idosos se sintam vontade para buscar orientação e apoio contribui significativamente para sua resiliência contra ameaças digitais. Nesse sentido, a interação e apoio entre gerações emergem como uma estratégia valiosa na promoção da cibersegurança de pessoas idosas. Essa abordagem não apenas fortalece a capacidade técnica dos idosos, mas também promove um senso de comunidade digital, tornando-os mais preparados e protegidos no ambiente *online* em constante evolução (PATRÍCIO; OSÓRIO, 2011).

Em síntese, a discussão destaca que os *deepfakes* representam uma ameaça crescente à segurança digital, com os idosos sendo particularmente suscetíveis devido à sua menor familiaridade com tecnologias digitais e maior propensão à confiança. Estudos, como o de Jin (2020) e Crippen (2023), enfatizam a falta de conhecimento dos idosos sobre tecnologias digitais e suas práticas *online*, tornando-os alvos fáceis para fraudes. A conscientização emerge como uma ferramenta vital na promoção da cibersegurança, com programas educacionais específicos, como proposto por Bray et al. (2023), capacitando pessoas idosas a tomar decisões mais conscientes em seu envolvimento digital.

Além disso, estratégias que visam o aumento da autoeficácia digital, conforme indicado por Pacherrez (2022) e Manyam (2022), revelam-se essenciais para fortalecer a capacidade dos idosos em enfrentar desafios cibernéticos, como os apresentados pelos *deepfakes*. A interação e apoio entre gerações, como destacado por Gonçalves e Patrício (2010) e Colibaba e Gheorghiu (2015), não apenas fortalecem as habilidades técnicas dos idosos, mas também promovem um ambiente de suporte crucial para sua resiliência digital.

Essas estratégias, quando integradas, não apenas protegem as pessoas mais velhas contra ciberataques, mas também podem promover uma participação mais segura e confiante no mundo digital, capacitando-os a

ISBN: 978-85-61702-73-1

usufruir dos benefícios da tecnologia. A conscientização, a autoeficácia digital e o apoio intergeracional surgem como componentes interconectados e complementares na construção de uma defesa robusta contra as ameaças representadas pelos *deepfakes*, contribuindo para uma experiência *online* mais segura e enriquecedora.

CONSIDERAÇÕES FINAIS

Diante da crescente ameaça representada pelos *deepfakes*, que emergem como uma preocupação significativa para a segurança digital em geral e, especialmente, para os idosos, é crucial refletir sobre as contribuições da psicogerontecnologia na promoção da cibersegurança nessa faixa etária. Os resultados dos estudos desenvolvidos indicam três áreas de intervenção essenciais: conscientização dos riscos digitais, aumento da autoeficácia digital e fomento à interação e apoio entre gerações.p

A conscientização dos riscos digitais é fundamental como um aprendizado na defesa contra ciberataques. A falta de conhecimento sobre os perigos digitais contribui significativamente para a vulnerabilidade dos idosos, tornando programas educacionais específicos uma estratégia eficaz. Esses programas não apenas informam, mas capacitam os idosos, permitindo decisões mais conscientes em seu envolvimento digital.

Além disso, a conscientização direcionada à identificação de conteúdo falso se mostra crucial, com estratégias práticas, como simulações, aprimorando a capacidade dos idosos em discernir entre informações autênticas e fraudulentas. A promoção de práticas seguras *online*, como configuração de senhas robustas e atualização regular de *software*, não só protege contra ameaças cibernéticas, mas também capacita os idosos a usufruir dos benefícios da era digital com confiança e segurança.

O aumento da autoeficácia digital em pessoas idosas desempenha um papel crucial na promoção da cibersegurança, especialmente diante das ameaças representadas pelos *deepfakes*. Programas de treinamento digital específicos para idosos visam não apenas fornecer conhecimento técnico, mas também desenvolver a confiança dos idosos em suas habilidades de navegação e discernimento *online*.

ISBN: 978-85-61702-73-1

Estratégias para aumentar a autoeficácia digital incluem a criação de ambientes de aprendizado personalizados, feedback positivo e encorajador, e a integração de experiências práticas no uso de tecnologias digitais. Ao fortalecer a autoeficácia digital, os idosos se tornam mais resilientes diante de ameaças potenciais, como os *deepfakes*, promovendo uma participação segura e confiante no mundo digital.

A interação e apoio entre gerações em pessoas idosas emergem como uma estratégia valiosa na promoção da cibersegurança. Essa abordagem aborda a importância das relações familiares e sociais na defesa contra possíveis riscos cibernéticos, proporcionando um ambiente de suporte e colaboração. Programas de treinamento intergeracionais, nos quais os membros mais jovens da família auxiliam os idosos na navegação segura na internet, têm se mostrado eficazes.

Essa abordagem não apenas aumenta a conscientização sobre a cibersegurança, mas também fortalece os laços familiares e a sensação de apoio, fatores essenciais para o bem-estar digital dos idosos. O apoio intergeracional, ao abranger não apenas o aspecto técnico, mas também o desenvolvimento de habilidades críticas, contribui significativamente para a resiliência dos idosos contra ameaças digitais.

Apesar dessas abordagens promissoras, é crucial considerar as limitações deste estudo. A revisão narrativa da literatura pode introduzir subjetividade na seleção e interpretação dos estudos, limitando a generalização dos resultados. Além disso, o cenário tecnológico está em constante evolução, exigindo estudos longitudinais para adaptar estratégias às mudanças.

Para pesquisas futuras, recomendamos aprofundar a eficácia de programas educativos, adaptar estratégias às mudanças tecnológicas, explorar fatores culturais e sociais, e desenvolver ferramentas específicas para identificação de *deepfakes*. Essas considerações refletem a complexidade do desafio, destacando a necessidade contínua de abordagens inovadoras na interseção entre psicogerontecnologia e cibersegurança.

Concluindo, ao fortalecer os pilares da conscientização dos riscos digitais, aumentar a autoeficácia digital e a interação entre gerações, é possível não apenas proteger os idosos contra ciberataques, mas também

ISBN: 978-85-61702-73-1

criar uma comunidade digital mais segura e resiliente. Capacitando-os para explorar o mundo digital com confiança, essa abordagem integrada promove uma participação positiva e proveitosa no ambiente *online*, proporcionando benefícios da tecnologia de maneira segura e eficaz.

REFERÊNCIAS

ARPASI, B. D. A.; ACUÑA, C. S. P.; MAYORGA, R. J. C. Autoeficacia y competencia digital universitaria en tiempos de Covid-19. **PsiqueMag**, [S. l.], v. 11, n. 2, p. 50–59, 2022. DOI: 10.18050/psiquemag.v11i2.2110. Disponível em: https://revistas.ucv.edu.pe/index.php/psiquemag/article/view/2110. Acesso em: 15 set. 2023.

BRASIL, Núcleo de Informação e Coordenação do Ponto. Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros : **TIC Domicílios 2019**. [s.l.]: Núcleo de Informação e Coordenação do Ponto BR, 2020.

BRAY, S. D; JOHNSON, S. D; KLEINBERG, B.. Testing human ability to detect 'deepfake' images of human faces**. Journal of Cybersecurity**, v. 9, n. 1, p. tyad011, 2023. Disponível em: <https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyad011/7205694>. Acesso em: 07 ago. 2023.

CHADHA, A. ; KUMAR, V. ; KASHYAP, S.; et al. Deepfake: An Overview. In: SINGH, Pradeep Kumar; WIERZCHOŃ, Sławomir T.; TANWAR, Sudeep; et al (Orgs.). **Proceedings of Second International Conference on Computing, Communications, and Cyber-Security**. Singapore: Springer, 2021, p. 557–566. (Lecture Notes in Networks and Systems).

CHI, Hongmei; MADUAKOR, Udochi; ALO, Richard; et al. Integrating Deepfake Detection into Cybersecurity Curriculum. In: ARAI, Kohei; KAPOOR, Supriya; BHATIA, Rahul (Orgs.). **Proceedings of the Future Technologies Conference (FTC) 2020**, Volume 1. Cham: Springer International Publishing, 2021, p. 588–598. (Advances in Intelligent Systems and Computing).

ISBN: 978-85-61702-73-1

COLIBABA, A.; GHEORGHIU, I. BRIDGING THE DIGITAL DIVIDE: INTERGENERATIONAL LEARNING. **INTED2015 Proceedings**, p. 4513–4518, 2015. Disponível em: <https://library.iated.org/view/COLIBABA2015BRI>. Acesso em: 15 nov. 2023.

CORDEIRO, Alexander Magno; OLIVEIRA, Glória Maria De; RENTERÍA, Juan Miguel; et al. Revisão sistemática: uma revisão narrativa. **Revista do Colégio Brasileiro de Cirurgiões**, v. 34, n. 6, p. 428–431, 2007. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-69912007000600012&lng=p t&tlng=pt>. Acesso em: 15 set. 2023.

CRIPPEN, Matthew. Conceptual and moral ambiguities of deepfakes: a decidedly old turn. **Synthese**, v. 202, n. 1, p. 26, 2023. Disponível em: <https://doi.org/10.1007/s11229-023-04250-y>. Acesso em: 02 nov. 2023.

FERNANDEZ, E. M. C., & DONARD, V. **O psicólogo frente ao desafio tecnológico: novas identidades, novos campos, novas práticas**. UFPE. 2016.

GAMA-VIEIRA, Osana Alexia; GABRIEL, Antônio; ARAÚJO-PIMENTEL-DE-MEDEIROS, Antônio Gabriel; et al. Reflexões Sobre a adaptação tecnológica para intervenções on-line com idosos. **Revista Brasileira de Terapias Cognitivas**, v. 18, n. 1,2022. Disponível em: <http://www.rbtc.org.br/detalhe_artigo.asp?id=349>. Acesso em: 20 nov. 2023.

GONÇALVES, V.; PATRÍCIO, M. INFORMATION TECHNOLOGY FOR GRANDPARENTS AND GRANDCHILDREN. **ICERI2010 Proceedings**, p. 3328–3332, 2010. Disponível em: <https://library.iated.org/view/GONCALVES2010INF>. Acesso em: 15 nov. 2023.

JIN, Lu. **Cheated by deepfakes? deepfake detection ability, people's reactions, and ethical implications**. 2020. Disponível em: <https://hdl.handle.net/2152/84814>. Acesso em: 10 nov. 2023.

ISBN: 978-85-61702-73-1

KWOK, Andrei O. J.; KOH, Sharon G. M. Deepfake: a social construction of technology perspective. **Current Issues in Tourism**, v. 24, n. 13, p. 1798–1802, 2021. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/13683500.2020.1738357>. Acesso em: 14 set. 2023.

MANYAM, Sowjanya. Artificial Intelligence's Impact on Social Engineering Attacks. **All Capstone Projects**, 2022.

MELO, Raissa Guerra de Magalhães; FERREIRA, Telma Mariza de Souza; SILVA, Cirlene Francisca Sales da. In: ADRIANA SCHULER CAVALLI; ANNA QUIALHEIRO ABREU DA SILVA; MANOEL FREIRE DE OLIVEIRA NETO; et al (org.). Novas diretrizes frente ao envelhecimento: diversidades, cuidados, inclusão e visibilidade. 1. ed. [s.l.]: Realize, 2022.

NÄSI, Matti; KOIVUSILTA, Leena. Internet and everyday life: the perceived implications of internet use on memory and ability to concentrate. **Cyberpsychology, Behavior, and Social Networking**, v. 16, n. 2, p. 88–93, 2013. Disponível em: <http://www.liebertpub.com/doi/10.1089/cyber.2012.0058>. Acesso em: 17 out. 2023.

PACHERREZ, Y. Luliana. **Competencia digital y autoeficacia en el uso de TIC en una institución educativa pública de una provincia de Cajamarca**. Repositorio Institucional - UCV, 2022. Disponível em: <https://repositorio.ucv.edu.pe/handle/20.500.12692/95563>. Acesso em: 15 nov. 2023.

PATRÍCIO, Maria Raquel; OSÓRIO, António. Lifelong learning, intergenerational relationships and ICT: perceptions of children and older adults. **Elderly, Education, Intergenerational Relationships and Social Development. Proceedings of 2nd Conference of ELOA**, n. 1st ed. October 2011, p. 224–232, 2011. Disponível em: <https://bibliotecadigital.ipb.pt/handle/10198/7061>. Acesso em: 15 nov. 2023.

RANA, Md Shohel; NOBI, Mohammad Nur; MURALI, Beddhu; et al. **Deepfake Detection: A Systematic Literature Review**. IEEE Access, v. 10, p.

ISBN: 978-85-61702-73-1

25494–25513, 2022. Disponível em: <https://ieeexplore.ieee.org/abstract/document/9721302>. Acesso em: 10 out. 2023.

SCHEMER, Christian; MASUR, Philipp K; GEISS, Stefan; et al. The Impact of Internet and Social Media Use on Well-Being: A Longitudinal Analysis of Adolescents Across Nine Years. **Journal of Computer-Mediated Communication**, v. 26, n. 1, p. 1–21, 2021. Disponível em: <https://academic.oup.com/jcmc/article/26/1/1/6032209>. Acesso em: 15 out. 2023.

SCHUARTZ, Antonio Sandro; SARMENTO, Helder Boska De Moraes. Tecnologias digitais de informação e comunicação (TDIC) e processo de ensino. **Revista Katálysis**, v. 23, n. 3, p. 429–438, 2020. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1414-49802020000300429&tlng=pt>. Acesso em: 15 out. 2023.

SUDHAKAR, K. N; SHANTHI, M.B. Deepfake: An Endanger to Cyber Security. In: 2023 **International Conference on Sustainable Computing and Smart Systems (ICSCSS)**. [s.l.: s.n.], 2023, p. 1542–1548. Disponível em: <https://ieeexplore.ieee.org/abstract/document/10169246?casa_token=cQF6Z-JkkRU0AAAAA:BSSDjD7UNa3NG8vexOcYk081fWvEGENGridBNsu_qm7rFR-bfwrz_pey3SPnFFsnVmm3mjD00eUCK>. Acesso em: 15 nov. 2023.

WANG, Xueyu; HUANG, Jiajun; MA, Siqi; et al. **DeepFake Disrupter: The Detector of DeepFake Is My Friend**, 2022, p. 14920–14929. Disponível em: <https://openaccess.thecvf.com/content/CVPR2022/html/Wang_DeepFake_Disrupter_The_D etector_of_DeepFake_Is_My_Friend_CVPR_2022_paper.html>. Acesso em: 15 nov. 2023.

WANG, Zuoguang; ZHU, Hongsong; SUN, Limin. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. **IEEE Access**, v. 9, p. 11895–11910, 2021. Disponível em: <https://ieeexplore.ieee.org/abstract/document/9323026>. Acesso em: 11 nov. 2023.