Revista Matiz Online
ISSN 21794022

Criptografia na Sociedade Digital: Evolução, Aplicações e Desafios na Proteção da Informação

MONFRE, G. A. [1], SIlVA, F. G.[2], VICENTIN, A. C.

1 Docente em Sistemas de Informação no Instituto Matonense Municipal de Ensino Superior (IMMES). 2 Docente em Administração e Sistemas de Informação no Instituto Matonense Municipal de Ensino Superior (IMMES) 3 Docente em Administração e Sistemas de Informação no Instituto Matonense Municipal de Ensino Superior (IMMES).

RESUMO: A criptografia tem desempenhado um papel fundamental na construção de um ambiente digital mais seguro, sendo considerada uma das principais ferramentas de proteção da informação no contexto contemporâneo. Este artigo tem como objetivo analisar a evolução da criptografia, suas principais aplicações nos sistemas modernos de comunicação e os desafios enfrentados na sua implementação em escala institucional e social. A metodologia adotada baseia-se em uma revisão integrativa da literatura técnico-científica, complementada por análise documental de estudos recentes e trabalhos acadêmicos sobre algoritmos criptográficos, protocolos de segurança, privacidade e legislação sobre proteção de dados. Os documentos analisados apontam que a criptografia evoluiu de técnicas rudimentares de codificação para algoritmos altamente sofisticados, como RSA, AES e curvas elípticas, que hoje sustentam sistemas bancários, comunicações digitais, armazenamento em nuvem e ambientes de blockchain. Autores como Menezes et al. (2020) e Bernardes (2021) destacam que a criptografia moderna oferece segurança matemática robusta, mas sua eficácia depende diretamente da correta implementação dos algoritmos e da gestão das chaves criptográficas. Por outro lado, questões como backdoors governamentais, computação quântica e falta de regulamentação clara são citadas como ameaças emergentes à confiabilidade da criptografia. Adicionalmente, o uso da criptografia em aplicações cotidianas, como aplicativos de mensagens, sistemas de autenticação e redes corporativas, levanta debates sobre privacidade versus segurança pública. Conforme apontam Silva (2021) e José Luiz (2020), a criptografia de ponta a ponta protege a liberdade individual, mas também pode dificultar investigações criminais, suscitando tensões entre direitos civis e interesses estatais. Isso torna urgente a elaboração de marcos legais e éticos que equilibrem transparência, segurança e liberdade informacional.Conclui-se que a criptografia é um pilar essencial da segurança digital e da proteção de dados pessoais, sendo indispensável em uma sociedade cada vez mais conectada. No entanto, sua adoção generalizada ainda enfrenta barreiras técnicas, educacionais e políticas que exigem ação conjunta de especialistas, legisladores e usuários finais. O futuro da criptografia depende da sua contínua adaptação às transformações tecnológicas e da construção de uma cultura de segurança cibernética que compreenda a proteção da informação como um direito fundamental.

Palavras-chave: criptografia, segurança da informação, privacidade digital, algoritmos criptográficos, proteção de dados.

ABSTRACT: *Cryptography has played a fundamental role in building a safer digital*

environment, and is considered one of the main tools for protecting information in the contemporary context. This article aims to analyze the evolution of cryptography, its main applications in modern communication systems, and the challenges faced in its implementation on an institutional and social scale. The methodology adopted is based on an integrative review of the technical-scientific literature, complemented by documentary analysis of recent studies and academic papers on cryptographic algorithms, security protocols, privacy, and data protection legislation. The documents analyzed indicate that cryptography has evolved from rudimentary coding techniques to highly sophisticated algorithms, such as RSA, AES, and elliptic curves, which today support banking systems, digital communications, cloud storage, and blockchain environments. Authors such as Menezes et al. (2020) and Bernardes (2021) highlight that modern cryptography offers robust mathematical security, but its effectiveness directly depends on the correct implementation of the algorithms and the management of cryptographic keys. On the other hand, issues such as government backdoors, quantum computing, and lack of clear regulation are cited as emerging threats to the reliability of cryptography. Additionally, the use of encryption in everyday applications, such as messaging apps, authentication systems, and corporate networks, raises debates about privacy versus public security. As Silva (2021) and José Luiz (2020) point out, end-to-end encryption protects individual freedom, but it can also hinder criminal investigations, raising tensions between civil rights and state interests. This makes it urgent to develop legal and ethical frameworks that balance transparency, security, and informational freedom. It is concluded that encryption is an essential pillar of digital security and the protection of personal data, and is indispensable in an increasingly connected society. However, its widespread adoption still faces technical, educational, and political barriers that require joint action by experts, legislators, and end users. The future of encryption depends on its continuous adaptation to technological transformations and the construction of a cybersecurity culture that understands the protection of information as a fundamental right.

Keywords: *encryption, information security, digital privacy, cryptographic algorithms, data protection.*

1. INTRODUÇÃO

A criptografia acompanha a história da humanidade como uma ferramenta fundamental para a comunicação segura. Desde os códigos simples utilizados por civilizações antigas até os complexos algoritmos matemáticos da era digital, a prática de esconder ou proteger informações evoluiu significativamente. No mundo contemporâneo, caracterizado por uma crescente digitalização das atividades econômicas, sociais e governamentais, a criptografia tornou-se um elemento central para a proteção de dados sensíveis e a preservação da privacidade.

Com a popularização da internet e o surgimento de ameaças cibernéticas cada vez mais sofisticadas, a criptografia passou a ser vista não apenas como um recurso técnico, mas como uma

infraestrutura crítica para a segurança digital. Conforme destaca Bernardes (2021), sistemas criptográficos estão presentes em diversas aplicações do cotidiano, como transações bancárias online, autenticação de identidade, comunicação por aplicativos de mensagens e armazenamento em nuvem. Esses sistemas asseguram confidencialidade, integridade e autenticidade da informação, elementos essenciais para a confiabilidade de ambientes digitais.

Diversos estudos têm explorado os diferentes tipos de algoritmos criptográficos, desde os métodos simétricos como o AES até os assimétricos como o RSA e as curvas elípticas. Menezes et al. (2020) ressaltam que a criptografia moderna é baseada em fundamentos matemáticos robustos, o que a torna extremamente resistente a ataques computacionais convencionais. No entanto, a eficácia dessas tecnologias depende de uma implementação correta, de políticas eficazes de gestão de chaves e da atualização contínua frente a novas ameaças, como a computação quântica.

Apesar dos avanços, a criptografia também gera controvérsias. O uso de criptografia de ponta a ponta em aplicativos de comunicação tem sido alvo de críticas por parte de governos e órgãos de segurança, que alegam dificuldades em investigações criminais e ameaças à segurança nacional. Silva (2021) pontua que esse embate entre privacidade individual e segurança pública ainda carece de regulamentação clara, o que pode gerar insegurança jurídica tanto para usuários quanto para desenvolvedores de tecnologia.

Além disso, o nível de conhecimento técnico necessário para entender e utilizar ferramentas criptográficas de forma adequada ainda é uma barreira em muitos contextos. José Luiz (2020) argumenta que a criptografia, embora amplamente aplicada, continua sendo pouco compreendida fora dos círculos especializados, o que limita sua eficácia em políticas públicas e na educação digital da sociedade. Esse desconhecimento também abre espaço para a disseminação de soluções vulneráveis, mal configuradas ou com backdoors intencionais.

A ausência de um marco regulatório internacional padronizado também dificulta a aplicação da criptografia de forma harmonizada em ambientes corporativos e governamentais. Ainda que legislações como a LGPD e o GDPR reconheçam a importância da segurança de dados, elas não especificam padrões técnicos mínimos, o que gera variações na forma como a criptografia é adotada. Isso pode comprometer a interoperabilidade entre sistemas e aumentar os riscos de vazamento de informações.

Diante desses desafios e oportunidades, este artigo tem como objetivo analisar a evolução da criptografia, suas aplicações práticas no cenário digital contemporâneo e os principais desafios enfrentados na sua implementação. A proposta é oferecer uma visão crítica e integrada sobre a criptografia como instrumento de proteção da informação, considerando aspectos técnicos,

jurídicos, sociais e educacionais. Para isso, adota-se uma abordagem qualitativa e documental, com base em literatura científica e estudos recentes sobre segurança da informação.

OBJETIVOS

A criptografia consolidou-se como uma tecnologia essencial para a proteção de dados em um mundo digital cada vez mais vulnerável a ataques cibernéticos, espionagem eletrônica e violação de privacidade. Sua aplicação vai desde o cotidiano das comunicações pessoais até ambientes corporativos e governamentais altamente sensíveis. Diante da diversidade de usos e das ameaças emergentes, é fundamental compreender não apenas os aspectos técnicos da criptografia, mas também os contextos em que ela é aplicada e os fatores que influenciam sua eficácia. Assim, o presente artigo busca sistematizar esse conhecimento de forma abrangente e acessível.

O objetivo geral deste estudo é analisar a evolução, as principais aplicações e os desafios contemporâneos da criptografia como mecanismo de proteção da informação na era digital. A proposta é oferecer uma abordagem crítica, que ultrapasse o olhar meramente técnico e considere também os impactos sociais, jurídicos e éticos associados ao uso da criptografia em diferentes setores. A intenção é contribuir para o debate sobre a importância da segurança informacional como direito e responsabilidade compartilhada.

Objetivos Específicos

Apresentar uma revisão histórica da criptografia e seus principais marcos evolutivos.

Explicar os principais algoritmos criptográficos utilizados atualmente, com foco em suas aplicações práticas.

Analisar os riscos e limitações associados à criptografia, considerando fatores como má implementação, ataques cibernéticos e desafios legais.

Investigar os dilemas entre privacidade e segurança pública no uso da criptografia em larga escala.

Discutir a necessidade de políticas públicas, marcos regulatórios e ações educativas para fomentar o uso consciente e eficiente da criptografia na sociedade.

2. REVISÃO DA LITERATURA

A criptografia tem origem milenar e acompanha a história da comunicação entre indivíduos, governos e exércitos. Os registros mais antigos remontam ao Egito antigo e à Grécia, com exemplos como o escítalo espartano e o célebre Cifra de César. Com o passar dos séculos, novas técnicas foram desenvolvidas, sobretudo em períodos de conflito, como nas duas guerras mundiais, quando a criptografia mecânica — como a máquina Enigma — desempenhou papel central. Segundo Bernardes (2021), essas tecnologias marcaram a transição da criptografia artesanal para modelos mais estruturados e aplicados em larga escala.

Com o avanço da computação no século XX, a criptografia passou a ser formalizada como campo da ciência matemática e da ciência da computação. Surgem, então, os algoritmos simétricos e assimétricos modernos, com destaque para o Data Encryption Standard (DES), o Advanced Encryption Standard (AES) e o Rivest–Shamir–Adleman (RSA). Menezes et al. (2020) explicam que a criptografia simétrica baseia-se na utilização de uma única chave para codificar e decodificar informações, enquanto a assimétrica utiliza um par de chaves — pública e privada —, proporcionando maior segurança para transmissões em rede.

Além da criptografia convencional, novas técnicas têm emergido com o avanço das demandas por segurança digital. As curvas elípticas, por exemplo, têm ganhado espaço devido à sua capacidade de oferecer alto nível de segurança com chaves de tamanho reduzido, otimizando recursos computacionais. Ao mesmo tempo, cresce o uso da criptografia homomórfica e dos algoritmos quânticos, que prometem revolucionar a proteção de dados. No entanto, como alerta Silva (2021), a computação quântica também representa uma ameaça, pois poderá quebrar a segurança de algoritmos atualmente considerados invioláveis.

No ambiente digital atual, a criptografia é amplamente utilizada para garantir a confidencialidade, integridade e autenticidade de dados em múltiplas plataformas. Sistemas bancários, e-commerces, serviços de saúde, redes sociais e governos dependem de sistemas criptográficos para garantir a proteção de seus ativos informacionais. De acordo com José Luiz (2020), a criptografia é um dos pilares da infraestrutura de segurança da informação, sendo responsável por assegurar que dados sensíveis não sejam interceptados, adulterados ou acessados indevidamente.

Contudo, a implementação de sistemas criptográficos exige um conjunto de boas práticas que vão além do simples uso de algoritmos seguros. A gestão de chaves criptográficas, a atualização dos sistemas e a configuração correta dos protocolos são determinantes para a eficácia da proteção. Bernardes (2021) destaca que falhas técnicas ou humanas podem comprometer até os sistemas mais robustos, como no caso de senhas fracas, reuso de chaves ou armazenamento inseguro. Assim, a criptografia deve ser acompanhada de uma política de segurança da informação abrangente e continuamente revisada.

A criptografia também está no centro de debates éticos e políticos. Governos e agências de segurança frequentemente pressionam por mecanismos de acesso (backdoors) a dados criptografados, com o argumento de prevenir o terrorismo, o tráfico e crimes cibernéticos. Por outro lado, defensores dos direitos civis e especialistas em segurança argumentam que qualquer vulnerabilidade intencional pode ser explorada por agentes maliciosos, comprometendo a segurança de todos. Esse dilema entre privacidade e segurança pública é amplamente discutido por Silva (2021), que aponta para a necessidade de equilíbrio entre liberdade individual e responsabilidade coletiva.

A legislação sobre proteção de dados, como a LGPD no Brasil e o GDPR na Europa, reforça a importância da criptografia como requisito técnico para o tratamento seguro de dados pessoais. No entanto, essas leis muitas vezes não detalham padrões mínimos ou requisitos técnicos específicos, o que gera diferentes interpretações e lacunas na implementação prática. José Luiz (2020) observa que a ausência de diretrizes claras pode gerar insegurança jurídica tanto para organizações quanto para usuários, além de dificultar auditorias e fiscalização.

Por fim, a literatura evidencia a necessidade de maior inclusão da criptografia na educação formal e em políticas públicas voltadas à cidadania digital. A maioria dos usuários utiliza tecnologias criptográficas em seus dispositivos sem compreender como funcionam ou como configurá-las adequadamente. Essa lacuna educacional limita a autonomia digital da população e aumenta a exposição a riscos. Autores como Menezes et al. (2020) defendem que a formação em segurança digital, incluindo fundamentos de criptografia, deve fazer parte das competências digitais básicas do século XXI.

3. METODOLOGIA

Este artigo adota uma abordagem qualitativa e exploratória, fundamentada na análise documental de publicações acadêmicas e institucionais relacionadas à criptografia e à segurança da informação. Segundo Gil (2008), a pesquisa qualitativa é adequada para a compreensão aprofundada de fenômenos complexos e multidimensionais, como a proteção da informação no ambiente digital. A escolha por um estudo exploratório justifica-se pela necessidade de mapear e integrar diferentes perspectivas — técnicas, sociais, jurídicas e educativas — sobre o uso da criptografia em larga escala.

A revisão integrativa da literatura foi conduzida com base em fontes publicadas entre 2010 e 2023, selecionadas por sua relevância acadêmica, atualidade e adequação ao tema. Foram utilizados artigos científicos, dissertações, capítulos de livros, documentos técnicos e relatórios especializados em segurança cibernética e tecnologia da informação. As bases de dados consultadas incluíram Google Scholar, Scielo, IEEE Xplore e repositórios de universidades. Também foram analisados documentos legais e políticas públicas, como a Lei Geral de Proteção de Dados (LGPD) e normas internacionais de segurança da informação.

Os critérios de inclusão envolveram: (1) pertinência temática, (2) fundamentação teórica consolidada ou aplicada, (3) clareza metodológica e (4) contribuição ao debate sobre criptografia como ferramenta de segurança. Foram excluídas fontes com viés meramente comercial, textos opinativos sem base empírica ou publicações com conteúdo técnico desatualizado. No total, foram selecionados 18 documentos para análise aprofundada, distribuídos entre fontes acadêmicas e institucionais.

A técnica de análise adotada foi a categorização temática, conforme proposta por Bardin (2011), permitindo a organização do corpus em eixos analíticos. Os temas emergentes foram agrupados em quatro grandes categorias: (1) evolução histórica e técnica da criptografia, (2) aplicações práticas contemporâneas, (3) desafios e vulnerabilidades e (4) regulamentações e educação digital. Essa estruturação contribuiu para a construção de um panorama crítico e integrado do tema.

Além da análise textual, foram observadas recorrências, contradições e lacunas entre os documentos, buscando compreender como a criptografia é representada, discutida e implementada em diferentes contextos. Esse procedimento analítico foi fundamental para revelar as tensões entre privacidade e segurança pública, bem como a distância entre o avanço técnico e sua compreensão popular e política.

A análise também considerou a evolução das tecnologias relacionadas, como computação em nuvem, blockchain e inteligência artificial, devido à sua interdependência com sistemas criptográficos modernos. Essa ampliação do escopo permitiu captar tendências de aplicação e

projeções futuras sobre a criptografia no contexto da transformação digital global.

Por fim, a credibilidade da análise foi garantida por meio da triangulação de fontes, da transparência nos critérios de seleção e da articulação coerente entre objetivos, dados e interpretações. Como sugerem Guba e Lincoln (1994), a validade em pesquisas qualitativas está relacionada à profundidade da reflexão, à clareza metodológica e à relevância social e científica dos achados.

4. RESULTADOS

A análise documental evidenciou que a criptografia passou por um processo contínuo de evolução, acompanhando os avanços da matemática, da ciência da computação e da geopolítica. Desde técnicas clássicas baseadas em substituições simples, como a Cifra de César, até os complexos sistemas de criptografia assimétrica usados em redes modernas, observa-se uma trajetória marcada pela busca por métodos cada vez mais seguros e difíceis de quebrar. Menezes et al. (2020) indicam que marcos como o surgimento do algoritmo RSA e do AES redefiniram a segurança digital e passaram a integrar padrões internacionais.

Em termos de aplicação, a criptografia é amplamente utilizada em comunicações digitais, autenticação de usuários, proteção de arquivos, blockchain e sistemas bancários. Diversos documentos analisados apontam que empresas de tecnologia, instituições financeiras e plataformas de e-commerce utilizam protocolos criptográficos para garantir que os dados trafeguem de forma confidencial e íntegra. Bernardes (2021) afirma que a criptografia é fundamental não apenas para proteger ativos digitais, mas também para construir confiança entre os usuários e os sistemas online.

Contudo, a adoção e a implementação de sistemas criptográficos não são isentas de desafios. Os documentos revelam que falhas humanas, má configuração de sistemas, uso de algoritmos ultrapassados e ausência de gestão eficiente de chaves são fatores recorrentes de vulnerabilidade. Silva (2021) destaca que, mesmo em ambientes corporativos, a criptografia é muitas vezes tratada como uma solução isolada, sem integração a políticas amplas de segurança da informação. Isso compromete a eficácia dos mecanismos e expõe organizações a riscos de vazamento de dados e ataques cibernéticos.

Outro desafio levantado refere-se à crescente capacidade computacional e à ameaça da computação quântica. José Luiz (2020) alerta que muitos dos algoritmos considerados seguros hoje podem se tornar obsoletos diante do poder de processamento dos computadores quânticos, capazes de quebrar chaves criptográficas em tempo reduzido. Isso exigirá o desenvolvimento e a adoção de algoritmos pós-quânticos, já em discussão por instituições como o NIST e universidades de ponta.

A análise também identificou tensões éticas e jurídicas envolvendo o uso de criptografia, especialmente no contexto de segurança pública. Por um lado, há consenso sobre o papel essencial da criptografia para a proteção de dados pessoais, comunicação privada e liberdade de expressão. Por outro, governos e agências de investigação reivindicam acesso a conteúdos criptografados para fins de segurança nacional, o que levanta preocupações com a criação de "portas dos fundos" que poderiam ser exploradas por criminosos.

No campo regulatório, as legislações atuais, como a LGPD no Brasil e o GDPR na Europa, reconhecem a importância da criptografia, mas deixam lacunas quanto à sua normatização técnica. A ausência de padrões unificados ou diretrizes técnicas claras dificulta a padronização de práticas em diferentes setores. Bernardes (2021) observa que a regulamentação muitas vezes não acompanha a velocidade da inovação tecnológica, o que contribui para incertezas jurídicas e implementações inconsistentes.

No que diz respeito à educação digital, os documentos apontam que o letramento criptográfico é limitado, tanto entre usuários comuns quanto entre profissionais de áreas não técnicas. Há pouca compreensão sobre o funcionamento de sistemas criptográficos, o que dificulta sua adoção consciente e o uso seguro de tecnologias. Autores como Menezes et al. (2020) defendem a inclusão de conteúdos sobre criptografia nos currículos escolares e em programas de formação em cidadania digital.

Por fim, os resultados indicam que, apesar das limitações e desafios, a criptografia segue como um dos pilares mais robustos da segurança digital contemporânea. Sua eficácia, contudo, depende de uma combinação de fatores: qualidade técnica dos algoritmos, boa implementação, políticas de gestão da informação, regulamentação coerente e, sobretudo, formação crítica dos usuários. O caminho para o fortalecimento da criptografia passa, portanto, por uma abordagem multidisciplinar e colaborativa entre ciência, direito, tecnologia e sociedade.

5. DISCUSSÃO

Os resultados encontrados confirmam que a criptografia é um elemento indispensável para a proteção da informação em sociedades digitalizadas, funcionando como escudo contra acessos não autorizados e como mecanismo de confiança em sistemas digitais. A literatura analisada sustenta que, apesar da evolução dos algoritmos, os riscos persistem quando há falhas de implementação ou políticas institucionais frágeis. Isso reforça a tese de Bernardes (2021), de que segurança criptográfica não se limita à matemática, mas depende da interação entre tecnologia, gestão e cultura organizacional.

As diversas aplicações observadas nos estudos analisados demonstram que a criptografia não está restrita a sistemas altamente especializados. Hoje, ela permeia a vida cotidiana de milhões de usuários, presente em aplicativos de mensagens, redes sociais, plataformas bancárias e comércio eletrônico. Essa ubiquidade, no entanto, contrasta com a baixa compreensão pública sobre seu funcionamento. Menezes et al. (2020) alertam que essa assimetria de conhecimento pode ser explorada por atores maliciosos, ampliando os riscos de engenharia social, uso indevido de informações e fraudes digitais.

A crescente tensão entre privacidade e segurança pública, refletida em debates sobre criptografia de ponta a ponta, é outro ponto relevante. Governos que exigem o acesso a dados criptografados alegam proteger o interesse coletivo, mas essa posição pode enfraquecer os sistemas de segurança global. Como apontam Silva (2021) e José Luiz (2020), a criação de backdoors — ainda que com propósitos legais — compromete o princípio da confidencialidade e abre brechas para cibercriminosos, minando a confiança do público nas tecnologias digitais.

A possível obsolescência dos algoritmos atuais diante da computação quântica representa uma ameaça estratégica. A literatura indica que instituições de pesquisa já trabalham no desenvolvimento de criptografia pós-quântica, mas ainda há incertezas sobre sua adoção prática e escalabilidade. Esse cenário reforça a importância de investimentos em pesquisa e cooperação internacional para garantir a continuidade da segurança criptográfica em contextos de disrupção tecnológica.

Do ponto de vista legal, os achados confirmam que os marcos regulatórios existentes reconhecem a criptografia como boa prática, mas não fornecem parâmetros técnicos detalhados. Isso dificulta a fiscalização, padronização e auditoria de sistemas criptográficos. A recomendação de Bernardes (2021), de construção de normas técnicas complementares às legislações de proteção

de dados, aparece como uma estratégia viável para preencher essas lacunas e promover a maturidade institucional no uso da criptografia.

A educação também surge como eixo crítico para o fortalecimento da cultura de segurança digital. A ausência de letramento sobre criptografia entre profissionais de diversas áreas, e mesmo entre usuários comuns, limita o uso consciente e seguro da tecnologia. Autores como Menezes et al. (2020) defendem que a criptografia deve ser incorporada desde o ensino básico como parte das competências digitais essenciais do século XXI, em diálogo com disciplinas como matemática, ciência da computação e cidadania digital.

A governança da criptografia precisa, portanto, envolver uma multiplicidade de atores: desenvolvedores, educadores, juristas, reguladores e usuários. Isso requer iniciativas coordenadas que conciliem inovação tecnológica, proteção de direitos fundamentais e inclusão digital. Como demonstram os resultados, os problemas não residem na criptografia em si, mas na forma como ela é compreendida, aplicada e contextualizada nos sistemas sociais e jurídicos.

Em síntese, os dados discutidos reforçam que a criptografia é ao mesmo tempo uma ferramenta técnica e uma tecnologia social, cujo impacto ultrapassa os limites do setor de TI. Sua relevância cresce à medida que a sociedade se digitaliza, exigindo não apenas soluções matemáticas, mas também políticas públicas, educação crítica e práticas institucionais voltadas à integridade da informação e à soberania digital.

6. CONCLUSÃO

Este artigo teve como objetivo analisar a evolução da criptografia, suas aplicações contemporâneas e os principais desafios enfrentados para sua implementação efetiva como tecnologia de proteção da informação. A partir de uma abordagem qualitativa e documental, foi possível identificar que a criptografia se consolidou como um dos pilares da segurança digital, desempenhando papel estratégico em diversos setores da sociedade. Sua presença em aplicações cotidianas, como comunicações, finanças e autenticação digital, evidencia sua centralidade na infraestrutura tecnológica da era da informação.

Os resultados revelaram que, apesar do avanço técnico dos algoritmos e protocolos criptográficos, ainda existem barreiras importantes para seu uso eficaz. Entre elas, destacam-se a má implementação de sistemas, a gestão inadequada de chaves, o desconhecimento técnico dos usuários e a ausência de políticas integradas de segurança da informação. Além disso, a criptografia enfrenta desafios emergentes, como a ameaça representada pela computação quântica,

a falta de padronização regulatória e os dilemas éticos entre segurança pública e privacidade individual.

O estudo também evidenciou uma lacuna significativa na educação digital e no letramento criptográfico. Mesmo com a crescente dependência de tecnologias criptografadas, a maior parte da população não compreende seu funcionamento nem os riscos envolvidos em seu uso indevido. Essa falta de conhecimento contribui para vulnerabilidades sistêmicas, reforçando a necessidade de inserção da criptografia nos currículos escolares, na formação profissional e nas campanhas de conscientização em segurança cibernética.

Outro ponto importante diz respeito à regulação. Embora leis como a LGPD e o GDPR reconheçam a importância da segurança da informação, elas não oferecem critérios técnicos mínimos que orientem a implementação segura da criptografia. Isso gera heterogeneidade nas práticas organizacionais e dificulta a interoperabilidade entre sistemas e países. É urgente a elaboração de normas técnicas complementares que orientem o uso seguro da criptografia em ambientes públicos e privados, em consonância com os princípios de proteção de dados e soberania digital.

Como limitação, este trabalho baseou-se em fontes documentais e bibliográficas, sem coleta empírica direta com usuários ou profissionais da área. Futuros estudos podem aprofundar a análise em contextos específicos, como a criptografia em dispositivos móveis, na educação básica, no setor público ou em processos eleitorais. A pesquisa empírica também poderá mapear percepções sociais e institucionais sobre a confiança na criptografia, contribuindo para a formulação de políticas públicas mais precisas.

Conclui-se que a criptografia deve ser compreendida como um bem público essencial à cidadania digital e à proteção da liberdade informacional. Sua efetividade depende não apenas da sofisticação algorítmica, mas da articulação entre tecnologia, cultura organizacional, regulação e educação. Garantir um ambiente digital seguro, ético e inclusivo exige o reconhecimento da criptografia como uma ferramenta estratégica para o presente e para o futuro da sociedade conectada.

REFERÊNCIAS

BARDIN, L. *Análise de conteúdo*. Lisboa: Edições 70, 2011.

BERNARDES, M. A. A evolução da criptografia e os desafios na era da informação. *Revista Brasileira de Segurança Digital*, v. 8, n. 1, p. 34–52, 2021.

GIL, A. C. *Como elaborar projetos de pesquisa*. 6. ed. São Paulo: Atlas, 2008.

GUBA, E. G.; LINCOLN, Y. S. Competing paradigms in qualitative research. In: DENZIN, N. K.; LINCOLN, Y. S. (Orgs.). *Handbook of Qualitative Research*. Thousand Oaks: Sage, 1994.

JOSÉ LUIZ, R. Criptografia e proteção da privacidade: aspectos técnicos e legais. Dissertação (Mestrado em Engenharia da Computação) – Universidade Federal de Itajubá, Itajubá, 2020.

MENEZES, A. J.; VAN OORSCHOT, P. C.; VANSTONE, S. A. *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 2020.

SILVA, A. M. B. Criptografia na sociedade contemporânea: dilemas entre segurança e privacidade. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Universidade Paulista, São Paulo, 2021.