REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

A ERA DO CANGAÇO DIGITAL: TRANSIÇÃO, ENGENHARIA SOCIAL E OS DESAFIOS DO ESTELIONATO NA SOCIEDADE DA INFORMAÇÃO

THE ERA OF DIGITAL BANDITRY: TRANSITION, SOCIAL ENGINEERING, AND THE CHALLENGES OF FRAUD IN THE INFORMATION SOCIETY

Ciências Exatas e da Terra • 21/07/2026

REGISTRO DOI: 10.70773/revistatopicos/784401343

Fábio Júnior Gomes de Lima[1]

Paulo Ricardo Claro[2]

Douglas Moro Piffer[3]

RESUMO

O presente artigo apresenta uma revisão sistemática da literatura sobre a evolução dos crimes cibernéticos, com ênfase na transição do estelionato tradicional para o denominado "Cangaço Digital", caracterizado pelo emprego intensivo de engenharia social, inteligência artificial e exploração das vulnerabilidades humanas na sociedade da informação. A pesquisa teve como objetivo analisar as principais evidências científicas nacionais e internacionais acerca das estratégias utilizadas pelos cibercriminosos, dos impactos provocados sobre as vítimas e dos desafios enfrentados pelos sistemas de segurança pública e justiça criminal. A revisão foi conduzida conforme as diretrizes do protocolo PRISMA 2020, abrangendo artigos científicos publicados entre 2016 e 2026, selecionados em bases de dados nacionais e internacionais. Os resultados demonstraram que a engenharia social consolidou-se como o principal mecanismo de execução das fraudes digitais, enquanto tecnologias como inteligência artificial, aprendizado de máquina e deepfakes ampliaram significativamente a sofisticação dos ataques. Também foram identificados impactos financeiros, psicológicos e sociais decorrentes da vitimização, bem como limitações relacionadas à investigação criminal, à cooperação internacional e à atualização dos instrumentos jurídicos frente à rápida evolução tecnológica. Constatou-se ainda que a prevenção dos crimes cibernéticos depende da integração entre inovação tecnológica, educação digital, fortalecimento institucional e proteção de dados pessoais. Conclui-se que o "Cangaço Digital" representa um novo paradigma da criminalidade contemporânea, exigindo estratégias multidisciplinares que articulem tecnologia, segurança pública, governança digital e conscientização da sociedade para reduzir a vulnerabilidade dos usuários e fortalecer a resiliência diante das ameaças presentes no ambiente virtual.

Palavras-chave: Cangaço Digital; Crimes cibernéticos; Engenharia social; Estelionato digital.

ABSTRACT

This article presents a systematic literature review on the evolution of cybercrime, emphasizing the transition from traditional fraud to the phenomenon referred to as "Digital Cangaço", characterized by the intensive use of social engineering, artificial intelligence, and the exploitation of human vulnerabilities in the information society. The study aimed to analyze national and international scientific evidence regarding cybercriminal strategies, the impacts on victims, and the challenges faced by public security and criminal justice systems. The review followed the PRISMA 2020 guidelines and included scientific articles published between 2016 and 2026 from national and international databases. The findings indicate that social engineering has become the primary mechanism for carrying out digital fraud, while technologies such as artificial intelligence, machine learning, and deepfakes have significantly increased the sophistication of cyberattacks. Financial, psychological, and social impacts on victims were also identified, in addition to limitations involving criminal investigations, international cooperation, and the adaptation of legal frameworks to rapid technological change. The review further highlights that effective cybercrime prevention depends on the integration of technological innovation, digital literacy, institutional strengthening, and personal data protection. It is concluded that "Digital Cangaço" represents a new paradigm of contemporary crime, requiring multidisciplinary strategies that combine technology, public security, digital governance, and public awareness to enhance resilience against cyber threats.

Keywords: Digital Cangaço; Cybercrime; Social engineering; Digital fraud.

1. INTRODUÇÃO

A intensificação da transformação digital alterou profundamente a dinâmica das relações sociais, econômicas e institucionais, proporcionando avanços tecnológicos sem precedentes, mas também ampliando o campo de atuação da criminalidade. Nesse contexto, os crimes cibernéticos deixaram de representar eventos isolados para constituírem uma modalidade estruturada de atuação criminosa, marcada pela utilização de técnicas de engenharia social, inteligência artificial, vazamentos massivos de dados e manipulação psicológica das vítimas. Esse novo cenário, denominado neste estudo como "Cangaço Digital", simboliza a transição da criminalidade patrimonial tradicional para um modelo altamente tecnológico, descentralizado e escalável, no qual o principal alvo deixa de ser a infraestrutura computacional e passa a ser o comportamento humano (Ferreira; Cotta, 2024; Birthriya; Ahlawat; Jain, 2025).

Embora o crescimento dos crimes cibernéticos tenha estimulado avanços na produção científica internacional, observa-se que ainda existem lacunas relevantes na compreensão integrada dos fatores tecnológicos, jurídicos, sociais e psicológicos que favorecem a expansão do estelionato digital. Diante desse contexto, emerge a seguinte questão norteadora desta revisão sistemática: como a literatura científica nacional e internacional tem abordado a transição para o denominado "Cangaço Digital", especialmente quanto ao papel da engenharia social, da evolução tecnológica e dos desafios impostos ao enfrentamento do estelionato na sociedade da informação?

O presente estudo tem como objetivo geral analisar, por meio de uma revisão sistemática da literatura, a produção científica acerca da transição da criminalidade patrimonial para o chamado "Cangaço Digital", enfatizando a engenharia social e os desafios contemporâneos do estelionato na sociedade da informação. Como objetivos específicos, busca-se: a) identificar as principais estratégias utilizadas por organizações criminosas na prática de fraudes digitais e ataques baseados em engenharia social; b) examinar as contribuições da literatura sobre os impactos da inteligência artificial, do phishing e dos deepfakes na evolução dos crimes cibernéticos; e c) discutir os desafios enfrentados pelos sistemas de segurança pública, pelo Direito e pelas políticas de prevenção.

A realização desta revisão sistemática justifica-se pela crescente relevância científica, jurídica e social do fenômeno dos crimes cibernéticos, cuja evolução tem superado a capacidade de resposta dos modelos tradicionais de investigação e prevenção. A ampliação do uso de tecnologias digitais, associada à circulação massiva de dados pessoais, ao emprego de inteligência artificial e à sofisticação das técnicas de manipulação psicológica, exige uma compreensão interdisciplinar capaz de integrar conhecimentos provenientes da segurança pública, da criminologia, do Direito Digital, da ciência da computação e das ciências comportamentais (Wendt, 2024; Barros Filho, 2024; Lourenço; Santos, 2023).

2. FUNDAMENTAÇÃO TEÓRICA

A transformação digital modificou significativamente a forma como indivíduos, empresas e instituições públicas se relacionam, promovendo benefícios em termos de comunicação, acesso à informação e desenvolvimento econômico. Entretanto, esse

processo também ampliou o espaço de atuação das organizações criminosas, que passaram a explorar as tecnologias da informação para a prática de delitos cada vez mais sofisticados. Nesse contexto, os crimes cibernéticos consolidaram-se como uma das principais ameaças à segurança pública contemporânea, exigindo respostas integradas entre Direito, tecnologia e políticas de prevenção (Barros Filho, 2024; Wendt, 2024).

Entre as modalidades criminosas que mais cresceram nos últimos anos destaca-se o estelionato digital, caracterizado pela utilização de recursos tecnológicos para induzir vítimas ao erro e obter vantagens econômicas ilícitas. Diferentemente dos ataques tradicionais baseados na exploração de vulnerabilidades técnicas, grande parte das fraudes atuais concentra-se na manipulação do comportamento humano por meio da engenharia social. Essa estratégia utiliza confiança, urgência, medo e curiosidade para persuadir as vítimas a fornecer informações sigilosas ou realizar transações financeiras, tornando o fator humano o principal alvo dos cibercriminosos (Mashtalyar et al., 2021; Birthriya; Ahlawat; Jain, 2025).

A evolução das tecnologias baseadas em inteligência artificial representa outro elemento determinante para a expansão do denominado "Cangaço Digital". Ferramentas capazes de produzir conteúdo altamente realistas, como mensagens automatizadas, clonagem de voz e deepfakes, aumentam a capacidade de convencimento dos criminosos e dificultam a identificação das fraudes pelas vítimas. Em contrapartida, a própria inteligência artificial vem sendo utilizada como mecanismo de defesa, permitindo o desenvolvimento de sistemas inteligentes para detecção de phishing, identificação de padrões suspeitos e

monitoramento preventivo de ataques cibernéticos (Alghenaim; Alkawsi; Barnhart, 2025; Popescul; Radu, 2025).

Outro aspecto amplamente discutido pela literatura refere-se aos impactos produzidos pelos crimes cibernéticos sobre as vítimas. Além dos prejuízos financeiros, as fraudes eletrônicas provocam consequências emocionais, sociais e psicológicas que frequentemente permanecem invisíveis nas estatísticas oficiais. Sentimento de insegurança, perda de confiança, ansiedade e sofrimento psicológico são recorrentes entre pessoas vitimadas por golpes virtuais, especialmente quando envolvem exposição de dados pessoais ou utilização indevida da identidade digital (Gautam; Yadav, 2026).

No âmbito jurídico e institucional, observa-se que a crescente sofisticação das organizações criminosas impõe desafios relevantes aos sistemas de investigação e persecução penal. A atuação transnacional das redes criminosas, a utilização de criptografia, moedas virtuais e serviços digitais descentralizados dificultam a identificação dos autores e a obtenção de provas eletrônicas. O fortalecimento da investigação criminal especializada, aliado ao aperfeiçoamento da legislação e da cooperação entre instituições públicas e privadas, constitui elemento indispensável para ampliar a eficiência no combate aos crimes cibernéticos (Ferreira; Cotta, 2024; Pereira, 2025).

O enfrentamento do estelionato digital exige uma abordagem multidisciplinar que combine inovação tecnológica, educação digital, inteligência artificial, fortalecimento institucional e conscientização da população. A prevenção depende não apenas do desenvolvimento de ferramentas computacionais mais eficientes,

mas também da construção de uma cultura de segurança digital capaz de reduzir a vulnerabilidade dos usuários diante das estratégias de manipulação empregadas pelos criminosos. Assim, o conceito de "Cangaço Digital" representa uma importante categoria analítica para compreender a industrialização das fraudes eletrônicas e os novos desafios impostos à segurança pública na sociedade da informação (Caneppele, 2025; James et al., 2026).

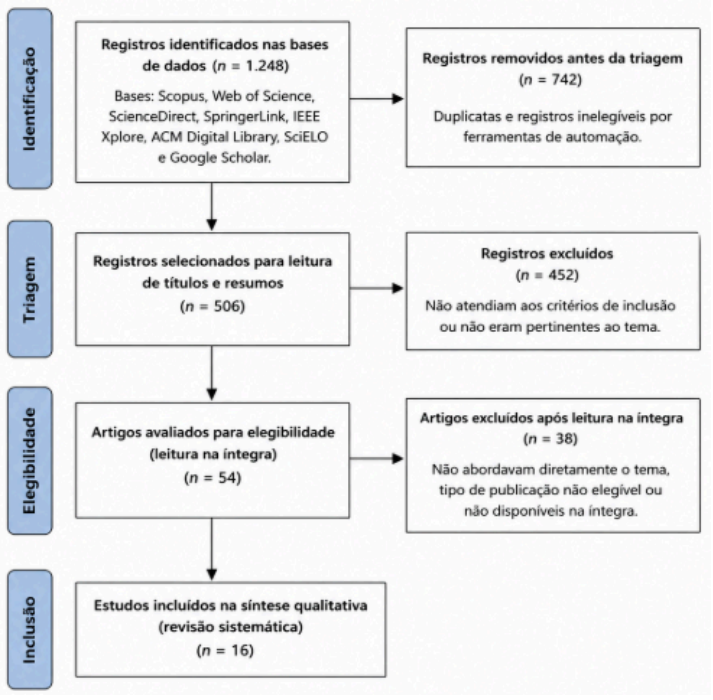
3. METODOLOGIA

A presente pesquisa caracteriza-se como uma revisão sistemática da literatura, desenvolvida conforme as recomendações do *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (Prisma, 2020), por se tratar de um método capaz de identificar, selecionar, avaliar criticamente e sintetizar evidências científicas de maneira transparente, rigorosa e reprodutível. A adoção desse protocolo possibilitou a organização sistemática da produção científica acerca da evolução dos crimes cibernéticos, da engenharia social, do estelionato digital e da utilização de tecnologias emergentes na prática e no enfrentamento das fraudes eletrônicas.

As buscas bibliográficas foram realizadas entre os meses de junho e julho de 2026 nas bases de dados Scopus, Web of Science, ScienceDirect, SpringerLink, ACM Digital Library, IEEE Xplore, Scopus Preview, SciELO e Google Scholar, utilizando descritores em português e inglês combinados por operadores booleanos (AND e OR). Foram empregados os seguintes termos de busca: "cybercrime", "digital fraud", "online fraud", "social engineering", "phishing", "deepfake", "artificial intelligence", "financial crimes", "crimes cibernéticos", "engenharia social", "estelionato digital" e "sociedade da informação".

Os critérios de elegibilidade foram definidos previamente. Foram incluídos exclusivamente artigos científicos publicados entre janeiro de 2016 e julho de 2026, disponíveis na íntegra, publicados em português ou inglês, indexados em bases científicas reconhecidas e relacionados diretamente aos temas crimes cibernéticos, engenharia social, phishing, estelionato eletrônico, inteligência artificial aplicada à segurança digital, deepfakes, investigação criminal cibernética ou impactos sociais e jurídicos do cibercrime. Foram excluídos livros, capítulos de livros, dissertações, teses, anais de eventos, relatórios técnicos, documentos institucionais, estudos duplicados e publicações cujo conteúdo não apresentasse relação direta com os objetivos desta revisão sistemática.

Figura 1. Fluxograma PRISMA



Fonte: elaborado pelo autor (2026).

O processo de seleção ocorreu em duas etapas. Inicialmente, realizou-se a leitura dos títulos, resumos e palavras-chave de todos os registros recuperados para verificar sua compatibilidade com os critérios de inclusão. Após a aplicação dos critérios de elegibilidade,

foram incluídos 16 artigos científicos na síntese qualitativa da revisão (figura 1), contemplando pesquisas nacionais e internacionais que abordam diferentes dimensões do fenômeno investigado, incluindo engenharia social, inteligência artificial, phishing, deepfakes, investigação criminal, impactos psicológicos das vítimas, segurança pública e evolução dos crimes cibernéticos.

4. RESULTADOS E DISCUSSÕES OU ANÁLISE DOS DADOS

A análise dos estudos selecionados permitiu identificar que a produção científica recente converge para o entendimento de que os crimes cibernéticos passaram por um processo de transformação impulsionado pela evolução tecnológica, pela ampliação do acesso à internet e pela crescente circulação de dados pessoais em ambientes digitais. As evidências demonstram que o estelionato eletrônico deixou de depender exclusivamente de conhecimentos técnicos em informática para incorporar estratégias sofisticadas de manipulação psicológica, inteligência artificial e exploração do comportamento humano. Nesse cenário, o conceito de "Cangaço Digital" representa uma interpretação contemporânea da criminalidade patrimonial, marcada pela industrialização das fraudes eletrônicas e pela utilização da engenharia social como principal mecanismo de obtenção de vantagens ilícitas.

Diferentemente dos ataques tradicionais voltados à exploração de vulnerabilidades em sistemas computacionais, as pesquisas demonstram que os criminosos passaram a direcionar seus esforços para a manipulação das decisões humanas. Estratégias baseadas em senso de urgência, autoridade, confiança e medo são amplamente utilizadas para convencer as vítimas a compartilhar informações pessoais ou realizar transferências financeiras. Esse

deslocamento do foco tecnológico para a vulnerabilidade comportamental evidencia uma mudança significativa na dinâmica do cibercrime contemporâneo (Mashtalyar et al., 2021; Birthriya; Ahlawat; Jain, 2025).

Essa modalidade permanece entre as principais portas de entrada para ataques financeiros e furtos de identidade digital, sendo continuamente aperfeiçoada pelo emprego de ferramentas baseadas em inteligência artificial. A utilização de mensagens altamente personalizadas, páginas falsas praticamente idênticas às oficiais e sistemas automatizados de envio em larga escala aumenta significativamente a taxa de sucesso das fraudes. Em resposta a esse cenário, diversos pesquisadores defendem o desenvolvimento de algoritmos inteligentes capazes de identificar padrões suspeitos e bloquear tentativas de ataque antes que alcancem os usuários (Alghenaim; Alkawsi; Barnhart, 2025; Popescul; Radu, 2025).

Enquanto ferramentas de aprendizado de máquina vêm sendo utilizadas para fortalecer sistemas de detecção de ameaças, monitoramento de redes e identificação automática de fraudes, os próprios grupos criminosos passaram a incorporar essas tecnologias em suas operações ilícitas. Estudos recentes destacam o uso crescente de modelos generativos para produção de conteúdo falsificados, clonagem de voz, criação de imagens sintéticas e automatização de ataques direcionados. Esse cenário amplia a complexidade das investigações e exige constante atualização das estratégias de defesa empregadas pelos órgãos responsáveis pela segurança pública (Tiwari et al., 2026; James et al., 2026).

A literatura demonstra que os prejuízos não se restringem às perdas financeiras, alcançando também dimensões emocionais,

psicológicas e sociais frequentemente negligenciadas pelos estudos tradicionais sobre criminalidade. Após sofrerem golpes virtuais, muitas vítimas desenvolvem sentimento de culpa, ansiedade, insegurança e desconfiança em relação às tecnologias digitais. Esses efeitos tendem a comprometer relações sociais, atividades profissionais e a própria percepção de segurança no ambiente virtual, indicando que o enfrentamento do problema exige ações que ultrapassem a repressão penal e contemplem estratégias de acolhimento e prevenção (Gautam; Yadav, 2026).

O aumento das fraudes eletrônicas observado nos últimos anos tem sido acompanhado por dificuldades estruturais na investigação criminal, especialmente em razão da velocidade de evolução das tecnologias utilizadas pelas organizações criminosas e da atuação transnacional desses grupos. Além disso, estudos brasileiros apontam limitações relacionadas à produção de provas digitais, à cooperação entre instituições e à necessidade de constante capacitação dos profissionais responsáveis pela persecução penal. Tais fatores contribuem para a sensação de impunidade e dificultam a resposta estatal diante da rápida expansão da criminalidade digital (Ferreira; Cotta, 2024; Wendt, 2024).

A intensificação das atividades remotas, do comércio eletrônico, dos serviços bancários digitais e das comunicações virtuais ampliou significativamente a superfície de ataque disponível para os criminosos. A revisão demonstra que esse processo favoreceu o aumento de golpes envolvendo falsas campanhas de saúde, aplicativos fraudulentos, links maliciosos e tentativas de obtenção de dados pessoais por meio de mensagens eletrônicas. Mesmo após o período mais crítico da pandemia, muitos desses padrões permaneceram ativos, evidenciando que a transformação digital

consolidou novas oportunidades para o desenvolvimento do estelionato eletrônico em larga escala (Lourenço; Santos, 2023; Barros Filho, 2024).

Nota-se crescente sofisticação das técnicas de engenharia social, que passaram a combinar informações obtidas em redes sociais, bancos de dados vazados e recursos de inteligência artificial para construir ataques altamente personalizados. Os estudos indicam que a personalização das mensagens aumenta significativamente a credibilidade das fraudes, reduzindo a capacidade de percepção das vítimas e ampliando a eficiência dos golpes. Essa mudança demonstra que o êxito das ações criminosas depende cada vez menos da invasão de sistemas computacionais e mais da exploração dos processos cognitivos e emocionais dos usuários (Birthriya; Ahlawat; Jain, 2025).

O desenvolvimento dos chamados deepfakes representa uma nova etapa na evolução do estelionato digital. A utilização de vídeos, imagens e áudios sintéticos produzidos por inteligência artificial permite criar comunicações praticamente indistinguíveis de conteúdos autênticos, favorecendo fraudes financeiras, falsificação de identidade e disseminação de desinformação. Esse cenário amplia os desafios para a investigação criminal, pois dificulta a verificação da autenticidade das provas digitais e exige a adoção de novas ferramentas tecnológicas para identificação de conteúdos manipulados (James et al., 2026).

Os estudos demonstram que algoritmos baseados em aprendizado de máquina apresentam elevada capacidade para identificar padrões anômalos em mensagens eletrônicas, reconhecer tentativas de phishing e bloquear automaticamente atividades

suspeitas antes que produzam prejuízos aos usuários. Entretanto, a revisão indica que a evolução constante das estratégias criminosas exige atualização permanente desses sistemas, tornando a inovação tecnológica um processo contínuo e indispensável para a proteção do ambiente digital (Alghenaim; Alkawsi; Barnhart, 2025; Popescul; Radu, 2025).

Os processos decisórios das vítimas constituem elemento central para a compreensão dos crimes cibernéticos contemporâneos. Diversos estudos apontam que fatores como excesso de confiança, sobrecarga informacional, pressão temporal e familiaridade com plataformas digitais influenciam diretamente a suscetibilidade às fraudes eletrônicas. Essa constatação reforça a necessidade de ampliar as pesquisas sobre comportamento humano no contexto da segurança digital, superando modelos de prevenção baseados exclusivamente em soluções tecnológicas (Rajan et al., 2026).

No contexto brasileiro, os estudos apontam que o fortalecimento das instituições responsáveis pela investigação dos crimes cibernéticos permanece como um dos principais desafios para o enfrentamento do estelionato eletrônico. A natureza transnacional dessas organizações criminosas, aliada à velocidade das transações financeiras e à utilização de tecnologias de anonimização, dificulta a identificação dos responsáveis e reduz a efetividade das investigações. Dessa forma, torna-se indispensável ampliar investimentos em inteligência policial, capacitação técnica e cooperação entre órgãos nacionais e internacionais (Wendt, 2024; Ferreira; Cotta, 2024).

Crianças e adolescentes passaram a ocupar posição de maior vulnerabilidade em razão da intensa utilização de plataformas

digitais para educação, entretenimento e interação social. Os estudos demonstram que esses usuários estão sujeitos não apenas a fraudes financeiras, mas também a crimes relacionados à exploração sexual, aliciamento, extorsão e divulgação ilícita de dados pessoais. Essa realidade evidencia a necessidade de políticas públicas voltadas à educação digital e ao fortalecimento dos mecanismos de proteção desse público (Andrade; Pataro et al., 2026).

O enfrentamento da criminalidade digital exige aperfeiçoamento constante do sistema jurídico. A rápida evolução tecnológica impõe desafios à produção de provas eletrônicas, à responsabilização penal dos autores e à adaptação da legislação às novas modalidades criminosas. As pesquisas ressaltam que a efetividade das normas depende não apenas da atualização legislativa, mas também da integração entre Poder Judiciário, órgãos de investigação, instituições financeiras e empresas de tecnologia, favorecendo respostas mais rápidas e eficientes às práticas criminosas (Marinho; Teles, 2024; Pereira, 2025).

A crescente digitalização dos serviços públicos e privados ampliou significativamente a superfície de exposição aos crimes cibernéticos. Processos bancários, serviços governamentais, plataformas de comércio eletrônico e sistemas de autenticação digital passaram a concentrar grande volume de informações pessoais e financeiras, tornando-se alvos estratégicos das organizações criminosas. Embora essas tecnologias tenham proporcionado maior eficiência e acessibilidade, os estudos analisados demonstram que a velocidade da transformação digital nem sempre foi acompanhada por investimentos equivalentes em segurança da informação e educação dos usuários. Esse desequilíbrio favorece o surgimento de novas modalidades de fraude e amplia os riscos associados ao

compartilhamento contínuo de dados pessoais em ambientes virtuais (Barros Filho, 2024; Caneppele, 2025).

A literatura demonstra que medidas exclusivamente repressivas apresentam eficácia limitada diante da rápida capacidade de adaptação das organizações criminosas. Em contrapartida, estratégias fundamentadas na educação digital, na conscientização da população, na cooperação entre instituições públicas e privadas e na utilização de tecnologias inteligentes de monitoramento mostram-se mais promissoras para reduzir a incidência das fraudes eletrônicas. Essa perspectiva amplia o papel da segurança pública, que passa a incorporar ações preventivas e educativas como componentes essenciais para a construção de uma cultura de proteção digital (Ferreira; Cotta, 2024; Wendt, 2024).

A evolução contínua da inteligência artificial, da engenharia social e das plataformas digitais exigirá respostas igualmente inovadoras por parte da comunidade científica, dos órgãos de segurança e dos formuladores de políticas públicas. Assim, compreender as múltiplas dimensões desse fenômeno constitui etapa indispensável para o desenvolvimento de mecanismos capazes de fortalecer a resiliência digital da sociedade e reduzir os impactos sociais, econômicos e jurídicos provocados pelos crimes cibernéticos contemporâneos (Tiwari et al., 2026; James et al., 2026).

De forma geral, a análise integrada da literatura demonstra que o denominado "Cangaço Digital" representa uma nova configuração da criminalidade organizada, caracterizada pela convergência entre tecnologia, engenharia social, inteligência artificial e exploração sistemática das vulnerabilidades humanas. A produção científica evidencia que a prevenção desses delitos depende da combinação

entre inovação tecnológica, fortalecimento institucional, educação digital, cooperação internacional e desenvolvimento de políticas públicas orientadas para a proteção dos dados pessoais e da cidadania digital. Esses elementos indicam que o combate ao estelionato eletrônico deve ser compreendido como desafio permanente da sociedade da informação, exigindo respostas igualmente dinâmicas diante da constante evolução das ameaças cibernéticas (Caneppele, 2025; Barros Filho, 2024).

5. CONCLUSÃO

A presente revisão sistemática permitiu compreender que a evolução dos crimes cibernéticos representa uma das mais significativas transformações da criminalidade contemporânea, evidenciando a transição de modelos tradicionais de fraude para estruturas altamente organizadas, tecnologicamente sofisticadas e fortemente apoiadas na exploração do comportamento humano. O estudo demonstrou que o denominado "Cangaço Digital" constitui uma expressão adequada para representar esse novo cenário, caracterizado pela utilização de engenharia social, inteligência artificial, vazamentos de dados e mecanismos de manipulação psicológica como instrumentos para a prática do estelionato eletrônico.

Verificou-se ainda que o avanço dessas modalidades criminosas impõe desafios crescentes às instituições responsáveis pela segurança pública, ao sistema de justiça e às políticas de proteção de dados, exigindo respostas cada vez mais integradas entre tecnologia, legislação e prevenção social. O enfrentamento efetivo do estelionato na sociedade da informação depende da adoção de

estratégias multidisciplinares que articulem inovação tecnológica, fortalecimento institucional e educação digital da população.

Embora ferramentas baseadas em inteligência artificial ampliem a capacidade de identificação de ameaças e prevenção de fraudes, a vulnerabilidade humana permanece como o principal vetor explorado pelas organizações criminosas, tornando indispensável o investimento em letramento digital, conscientização e desenvolvimento de uma cultura permanente de segurança da informação.

REFERÊNCIAS BIBLIOGRÁFICAS

ALGHENAIM, M.; ALKAWSI, G.; BARNHART, C. R. The State of the Art in AI-Based Phishing Detection: A Systematic Literature Review. *Springer,* 2025. Disponível em: https://link.springer.com/chapter/10.1007/978-3-031-75091-5_23. Acesso em: 06 jan. 2026.

ANDRADE, G. P.; PATARO, L. D. E. S.; et al. Crimes cibernéticos contra crianças e adolescentes: os desafios do primeiro grau de jurisdição. *Revista Jurídica Gralha Azul*, 2026. Disponível em: https://revista.tjpr.jus.br/gralhaazul/article/view/412. Acesso em: 09 jul. 2026.

BARROS FILHO, J. Crimes cibernéticos: consequências jurídicas e sociais. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, 2024. Disponível em: https://periodicorease.pro.br/rease/article/view/16881. Acesso em: 06 jan. 2026.

BIRTHRIYA, S. K.; AHLAWAT, P.; JAIN, A. K. A comprehensive survey of social engineering attacks: taxonomy of attacks, prevention, and mitigation strategies. *Journal of Applied Security Research*, 2025. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/19361610.2024.2372986. Acesso em: 06 jan. 2026.

CANEPPELE, S. Observing, Measuring, and Researching Cybercrime: A Scoping Review of Systematic Reviews Since 2010s. *Springer,* 2025. Disponível em: https://link.springer.com/chapter/10.1007/978-3-031-72387-2_5. Acesso em: 06 jan. 2026.

FERREIRA, M. F. G.; COTTA, F. A. Ciências policiais e crimes cibernéticos: reflexões iniciais sobre o estelionato em ambiente digital em Minas Gerais. *O Alferes*, 2024. Disponível em: https://revista.policiamilitar.mg.gov.br/index.php/alferes/article/view/878. Acesso em: 06 jan. 2026.

GAUTAM, R.; YADAV, S. Psychological impact of cyber-crime on victims. *Current Psychology*, 2026. Disponível em: https://link.springer.com/article/10.1007/s12144-025-08873-x. Acesso em: 06 jan. 2026.

JAMES, E. C. et al. A systematic literature review on how cybercriminals are utilizing deepfakes to conduct cyberattacks. *Digital Threats: Research and Practice*, 2026. Disponível em: https://dl.acm.org/doi/10.1145/3801545. Acesso em: 06 jan. 2026.

LOURENÇO, A. C. G.; SANTOS, C. E. P. dos. O aumento dos crimes cibernéticos durante a pandemia da Covid-19 e as dificuldades para combatê-los. *Libertas Direito*, 2023. Disponível em:

https://periodicos.famig.edu.br/index.php/direito/article/view/387. Acesso em: 06 jan. 2026.

MARINHO, M. G.; TELES, D. R. de S. Os ataques cibernéticos e suas implicações penais. *Revista JRG de Estudos Acadêmicos*, 2024. Disponível em: https://www.revistaft.com/ft/article/view/840. Acesso em: 09 jul. 2026.

MASHTALYAR, N. et al. Social Engineering Attacks: Recent Advances and Challenges. *Springer, 2*021. Disponível em: https://link.springer.com/chapter/10.1007/978-3-030-77392-2_27. Acesso em: 06 jan. 2026.

PEREIRA, V. R. Trinta anos da Lei 9.099/1995: entre a promessa de democratização e a realidade da crise cibernética: uma análise crítica do ciberespaço judicial e das ameaças ransomware/DDoS ao acesso à justiça no Brasil. *Revista Jurídica Gralha Azul*, 2025. Disponível em: https://revista.tjpr.jus.br/gralhaazul/article/view/313. Acesso em: 09 jul. 2026.

POPESCUL, D.; RADU, L. D. AI in phishing detection: a bibliometric review. *Frontiers in Artificial Intelligence*, 2025. Disponível em: https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1496580/full. Acesso em: 06 jan. 2026.

RAJAN, S. K. et al. Behavioral influences on cybersecurity decisions in phishing scenarios: a systematic review. *Information & Computer Security*, 2026. Disponível em: https://www.emerald.com/ics/article/doi/10.1108/ICS-10-2025-0439/1385259. Acesso em: 06 jan. 2026.

TIWARI, M. et al. Generative AI and financial crimes: a quantitative systematic literature review. *Crime Science*, 2026. Disponível em: https://link.springer.com/article/10.1186/s40163-026-00268-y. Acesso em: 06 jan. 2026.

WENDT, E. Sísifo e a investigação criminal cibernética: por que não avançamos? *Revista do Sistema Único de Segurança Pública*, 2024. Disponível em: https://revistasusp.mj.gov.br/susp/index.php/revistasusp/article/view/631. Acesso em: 06 jan. 2026.

---

[1] Tecnólogo em Redes de Computadores. Campus Porto Velho Zona Norte do Instituto Federal de Rondônia (IFRO). Porto Velho - Rondônia, Brasil. E-mail: acesse o artigo original para visualizar o e-mail.

[2] Tecnólogo em Redes de Computadores. Campus Porto Velho Zona Norte do Instituto Federal de Rondônia (IFRO). Porto Velho - Rondônia, Brasil. E-mail: acesse o artigo original para visualizar o e-mail.

[3] Mestre em Administração. Campus Porto Velho Zona Norte do Instituto Federal de Rondônia (IFRO). Porto Velho - Rondônia, Brasil. E-mail: acesse o artigo original para visualizar o e-mail.