UFSM

InterAção

ISSN 2357-7975
ACESSO ABERTO

IA., Santa Maria, v. 17, n. 3, e99414, p. 1-31, 2026 • https://dx.doi.org/10.5902/2357797599414
Submissão: 18/10/2026 • Aprovação: 16/11/2026 • Publicação: 23/11/2026

Artigos Dossiê

Redes de phishing e cibercrime: impactos e desafios sociais e políticos no contexto global

Phishing networks and cybercrime: social and political impacts and challenges globally

Bruno André Rodrigues Machado[I]

[I]Universidade Aberta, Lisboa, Portugal

Resumo

Este trabalho analisa as redes de phishing como um ator global relevante no cibercrime, com foco nos impactos e desafios sociais e políticos deste fenómeno transnacional no contexto global. Especializadas em fraudes eletrónicas para obtenção de dados sensíveis, estas redes transcendem fronteiras, aproveitando-se das desigualdades sociais e das lacunas institucionais para expandir as suas operações. A análise centra-se em compreender como as dinâmicas sociais e políticas da globalização, impulsionadas pelo modernismo, favorecem o surgimento e a proliferação destas práticas ilícitas. O estudo examina também os métodos operacionais destas redes, destacando as estratégias de manipulação baseadas em engenharia social, e os impactos multifacetados, que incluem consequências económicas significativas, destabilização social e desafios políticos para os Estados e organizações internacionais. Além disso, são abordadas as vulnerabilidades estruturais que tornam possíveis estas atividades, explorando a necessidade de respostas coordenadas e eficazes por parte da comunidade internacional. Baseado numa revisão da literatura, a investigação adota uma metodologia que permite uma análise sistemática e crítica sobre o tema, privilegiando fontes académicas e relatórios internacionais relevantes. Este trabalho procura contribuir para uma compreensão mais clara do fenómeno, proporcionando uma base sólida para estudos futuros que explorem soluções práticas e inovadoras no combate a este problema transnacional. A relação entre cibercrime e globalização será analisada como uma manifestação indireta do fenómeno estudado, ilustrando de que forma estas dinâmicas influenciam as sociedades contemporâneas e moldam as políticas de segurança global.

Palavras-chave: Phishing; Cibercrime transnacional; Redes criminosas; Criminalidade global; Política criminal

Artigo publicado por InterAção sob uma licença CC BY-NC-SA 4.0.

Abstract

This paper analyses phishing networks as a relevant global actor in cybercrime, focusing on the social and political impacts and challenges posed by this transnational phenomenon in a global context. Specialising in electronic fraud aimed at obtaining sensitive data, these networks cross borders and exploit social inequalities and institutional gaps to expand their operations. The analysis seeks to understand how the social and political dynamics of globalisation, driven by modernism, favour the emergence and spread of such unlawful practices. The study also examines the operational methods of these networks, particularly manipulation strategies based on social engineering, and their multifaceted impacts, including significant economic consequences, social destabilisation and political challenges for states and international organisations. Structural vulnerabilities that make these activities possible are also addressed, alongside the need for coordinated and effective responses from the international community. Based on a literature review, the research adopts an approach allowing a systematic and critical analysis of the topic, favouring relevant academic sources and international reports. The paper seeks to contribute to a clearer understanding of the phenomenon and provide a basis for future studies exploring practical and innovative responses to this transnational problem. The relationship between cybercrime and globalisation is considered as an indirect manifestation of the phenomenon under study, illustrating how these dynamics influence contemporary societies and shape global security policies.

Keywords: Phishing; Transnational cybercrime; Criminal networks; Global crime; Criminal policy

1 INTRODUÇÃO

As redes de phishing configuram-se como um objeto de estudo relevante e complexo no âmbito do cibercrime global, suscitando questões que ultrapassam fronteiras geográficas e desafiam a resiliência de instituições e mercados globais. Estas redes, focadas em fraudes eletrónicas para obtenção de dados sensíveis, estão intrinsecamente ligadas às dinâmicas de um mundo cada vez mais interconectado, onde a expansão digital parece trazer tanto oportunidades quanto riscos associados à criminalidade transnacional.

No contexto dos estudos globais, a análise destas redes revela-se imprescindível para compreender as interseções entre cibercrime, globalização e as transformações socioeconómicas e culturais contemporâneas, cuja relevância e atualidade do tema reside desde logo na sua dimensão tecnológica, mas também na forma como estas práticas ilícitas exploram as desigualdades sociais e as lacunas institucionais para operar num espaço digital sem fronteiras.

Esta investigação propõe-se a articular os conceitos e debates teóricos mais relevantes, estabelecendo um quadro analítico que permita compreender o fenómeno das redes de phishing, enquanto o situa no contexto mais amplo das dinâmicas da globalização.

2 OBJETIVOS GERAIS E ESPECÍFICOS

O objetivo geral é analisar as redes de phishing como atores globais no panorama do cibercrime. Procura-se compreender como as dinâmicas globais, especialmente as transformações económicas, culturais e tecnológicas da globalização, influenciam o surgimento, o funcionamento e a expansão destas redes ilícitas, bem como identificar as vulnerabilidades estruturais e institucionais que facilitam a sua operação.

Como objetivos específicos, o trabalho propõe: (1) identificar e caracterizar as estratégias de engenharia social utilizadas pelas redes de phishing para obter dados sensíveis, explorando o seu alcance transnacional e a sua relação com os fluxos globais de informação e capital; (2) analisar os impactos económicos do phishing, com foco na sua relevância para economias globalizadas e as suas potenciais implicações em cadeias financeiras e de consumo; (3) investigar as implicações sociais do phishing, incluindo o efeito na confiança digital e nas dinâmicas sociais num contexto global; (4) avaliar os desafios políticos enfrentados pelos Estados na criação de respostas eficazes contra este fenómeno; e (5) explorar o papel das organizações internacionais na coordenação de esforços globais de combate ao phishing e cibercrime.

3 METODOLOGIA

A metodologia deste trabalho baseia-se numa revisão da literatura sobre as redes de phishing, a sua relação com a globalização e os respetivos impactos sociais, económicos e políticos. Esta abordagem científica permite uma análise sistemática e crítica de estudos existentes, sendo especialmente adequada para investigações

teóricas e exploratórias (BOOTH et al., 2016), como esta que procura enquadrar o fenómeno das redes de phishing no contexto dos estudos globais, sem recorrer a dados primários.

A seleção das fontes privilegiará a relevância, qualidade e credibilidade dos dados, incluindo publicações académicas, como artigos indexados, capítulos de livros, dissertações e relatórios de organizações internacionais como Europol, Interpol e Nações Unidas. Dar-se-á preferência a estudos recentes, salvo casos em que obras clássicas sejam fundamentais para o enquadramento teórico.

Os dados recolhidos serão submetidos a uma análise crítica e a revisão será organizada de forma estruturada, iniciando-se com uma contextualização teórica e prosseguindo com uma avaliação das perspetivas apresentadas na literatura. Este processo permitirá compreender o papel das redes de phishing no contexto global, identificar lacunas existentes no conhecimento e contribuir para o desenvolvimento de soluções mais eficazes.

4 BASES TEÓRICAS CONCEPTUAIS

Para compreender as redes de phishing no contexto global, é essencial delinear os conceitos operatórios fundamentais que sustentam a análise.

4.1 Phishing

Segundo BEUTIN e BORAN (2023) no livro The Great Web 3.0 Glossary, phishing é uma prática ilícita no domínio do cibercrime que envolve a manipulação de indivíduos ou organizações para obter informações sensíveis, como credenciais de acesso, dados bancários ou informações pessoais. A característica central do phishing é o uso de embustes tecnológicos e psicológicos para enganar as vítimas, aproveitando-se da confiança depositada em marcas, instituições ou indivíduos. As estratégias de phishing incluem emails fraudulentos, websites falsificados e mensagens instantâneas que simulam comunicação legítima.

No contexto global, este fenómeno é potenciado pela interconexão digital, que permite a proliferação transnacional dessas práticas com baixo custo e elevado alcance (PHILLIPS et al., 2023). O phishing será explorado como uma manifestação do cibercrime facilitada pelas estruturas globais de informação e capital.

4.2 Cibercrime

Por sua vez, o cibercrime refere-se a qualquer atividade criminosa que utiliza redes informáticas ou dispositivos conectados como ferramenta, alvo ou local de prática ilícita, englobando desde crimes de acesso indevido (hacking) até fraudes eletrónicas, como o phishing (PAYNE, 2020). Este conceito é central para o estudo, pois situa o phishing dentro de um quadro mais amplo de práticas criminosas que dependem da tecnologia para operar.

O cibercrime destaca-se pela sua natureza transnacional, desafiando as capacidades reguladoras dos Estados e exigindo respostas coordenadas a nível global (HOLT, 2020). No contexto deste trabalho, o cibercrime será analisado como consequência e promotor das dinâmicas da globalização, revelando as vulnerabilidades estruturais criadas pela interdependência digital.

4.3 Engenharia Social

Segundo SONOWAL (2023) a engenharia social alude ao conjunto de técnicas psicológicas utilizadas para manipular indivíduos a fim de obter acesso a informações confidenciais ou recursos protegidos. No phishing, a engenharia social desempenha um papel central, aproveitando-se de vulnerabilidades humanas, como a confiança excessiva, o medo ou a urgência, para induzir ações como clicar em links maliciosos ou partilhar informações privadas.

Este conceito será explorado como uma estratégia fundamental nas redes de phishing, destacando as formas como estas redes utilizam conhecimentos de psicologia e comportamento humano para criar cenários convincentes e enganosos.

A interligação entre a engenharia social e as desigualdades digitais será também abordada, uma vez que as vítimas mais vulneráveis tendem a ser aquelas com menor literacia digital (GOEL et al., 2017).

4.4 Globalização

A globalização consiste no processo de integração económica, social, cultural e tecnológica que transcende fronteiras nacionais, criando uma rede interconectada de fluxos de informação, capital e pessoas (ROBERTSON, 1992). Este fenómeno é amplamente reconhecido como um fator facilitador para a expansão do cibercrime, incluindo o phishing, ao proporcionar um ambiente onde as barreiras geográficas e temporais são minimizadas (COOK-KWENDA, 2024; KSHETRI, 2010; MALLICK; NATH, 2024).

No âmbito deste trabalho, a globalização será analisada como um fator estrutural que intensifica o alcance e a sofisticação das redes de phishing. A compressão espaço-temporal promovida pela globalização, como discutido por BAUMAN (1998), intensifica a interconexão global, criando tanto oportunidades quanto vulnerabilidades; nesse contexto, as dinâmicas globais de comércio digital, migração de dados e interdependência económica favorecem a atuação eficaz de redes, incluindo as criminosas, num ambiente transnacional. A globalização será também central para compreender os desafios enfrentados pelos Estados e organizações internacionais na criação de respostas coordenadas.

4.5 Segurança Digital

A segurança digital, ou cibersegurança, abrange práticas, tecnologias e políticas destinadas a proteger redes, sistemas, dispositivos e dados contra acessos não autorizados, ataques ou destruição, incluindo, no contexto do phishing, medidas técnicas como firewalls e sistemas de autenticação (LINDEMULDER; KOSINSKI, 2024). A segurança digital é atualmente debatida também sob a forma de estratégias de educação e sensibilização destinadas a prevenir a manipulação psicológica e a vitimização (MOONSAMY et al., 2024).

Este conceito será explorado no contexto da globalização como uma resposta ao cibercrime, destacando as lacunas e limitações das práticas de segurança digital no combate às redes de phishing.

A inter-relação entre estes conceitos operatórios evidencia a complexidade do fenómeno das redes de phishing. O phishing, enquanto prática de cibercrime, utiliza estratégias de engenharia social para explorar as vulnerabilidades humanas num ambiente globalizado, onde as interconexões digitais ampliam o seu alcance. Simultaneamente, a segurança digital emerge como um mecanismo de defesa, frequentemente limitado pelas mesmas dinâmicas globais que facilitam a proliferação do phishing. Estes conceitos articulam-se para oferecer uma visão abrangente do fenómeno, que será desenvolvida nos capítulos subsequentes.

5 ESTADO DA ARTE

O estudo das redes de phishing tem ganho destaque na literatura científica nos últimos anos, acompanhando o crescimento do cibercrime e a intensificação das dinâmicas globais de interconexão digital. A análise do estado da arte permite identificar os contributos mais relevantes para a compreensão deste fenómeno, destacando as abordagens que examinam o phishing como um reflexo das transformações sociais, económicas e políticas associadas à globalização.

A investigação sobre phishing revela a clara evolução e sofisticação das técnicas utilizadas por redes criminosas para iludir indivíduos e organizações. Estudos recentes (e.g., COOK-KWENDA, 2024; MOONSAMY et al., 2024) demonstram que as redes de phishing se apoiam fortemente em estratégias de engenharia social, que vão desde a imitação de marcas conhecidas até à personalização de mensagens com base em informações recolhidas online. As investigações evidenciam ainda a utilização de tecnologias avançadas, nomeadamente inteligência artificial e machine learning, para aprimorar e automatizar os processos envolvidos nestas operações, aumentando significativamente a sua eficácia (GUEMBE et al., 2022; HEIDING et al., 2024).

No contexto global, estas estratégias retratam as desigualdades em termos de literacia digital, uma vez que populações em países com menor acesso à educação tecnológica são frequentemente alvos preferenciais (BUTAVICIUS et al., 2022; GOEL et al., 2017). A literatura sublinha ainda que a interconectividade proporcionada pela globalização digital facilita o acesso a um grande número de potenciais vítimas, reduzindo custos operacionais para os criminosos (EUROPOL, 2023; KSHETRI, 2010).

Muitos estudos (e.g., EMARA; ABDELGHFAR, 2024; KOVALCHUK et al., 2021; SHEVCHENKO et al., 2023) têm abordado o impacto económico do phishing, revelando que estas redes causam prejuízos financeiros significativos a empresas e indivíduos. Relatórios anuais de cibersegurança indicam que o phishing continua a ser uma das formas mais prevalentes e dispendiosas de cibercrime. Segundo dados da Cybersecurity Ventures (MORGAN, 2022) e da Statista (FLECK, 2024) estima-se que o custo global relacionado com o cibercrime[I], incluindo práticas como o phishing, alcance valores entre 9 e 13 mil milhões de dólares anuais até 2028.

Estas perdas evidenciam as vulnerabilidades das economias globalizadas, caracterizadas pela interdependência dos fluxos financeiros e das transações digitais. A literatura sublinha ainda que os setores mais vulneráveis incluem as indústrias financeiras, o comércio eletrónico e o setor público, que lidam com grandes volumes de dados sensíveis (DAS et al., 2022; NTT SECURITY HOLDINGS, 2024).

No plano social, investigações como as de JHONSON et al. (2023), KIESOW CORTEZ (2020) e THANKGOD (2024) analisam os impactos do phishing na confiança digital, evidenciando que, para além de causarem prejuízos significativos às vítimas em níveis individuais, estas práticas comprometem de forma ampla a confiança nas plataformas digitais e nos serviços online, afetando o ecossistema digital como um todo. O aumento da desinformação e a proliferação de campanhas de phishing durante a pandemia de COVID-19 são exemplos de como estas práticas afetam a sociedade em momentos de vulnerabilidade global (INTERPOL, 2020).

[I] Onde se inclui apropriação indevida de dados pessoais e financeiros, perda de produtividade, apropriação de propriedade intelectual, desvio de fundos, fraude, danos à reputação, interrupção das operações, bem como custos associados à investigação forense e à recuperação de sistemas.

A literatura explora igualmente os desafios políticos associados ao phishing, destacando as dificuldades enfrentadas pelos Estados em regulamentar um fenómeno que ultrapassa as fronteiras nacionais. Estudos como os de HOLT (2020), KIESOW CORTEZ (2020) e KLEIJSSEN e PERRI (2017) sugerem que o cibercrime está profundamente interligado com os processos de globalização, tirando partido das assimetrias legislativas e da falta de coordenação eficaz entre jurisdições.

Apesar dos esforços das organizações internacionais, como a Interpol e a Europol[II], a resposta global ao phishing revela-se muitas vezes dispersa, caracterizada por estratégias variadas que nem sempre estão alinhadas ou coordenadas[III]. Estas organizações, juntamente com outros atores de relevância global, como Ghada WALY (2024), destacam a importância de implementar políticas integradas e de fortalecer a colaboração internacional para enfrentar um fenómeno que transcende fronteiras.

A relação entre phishing e globalização é amplamente discutida na literatura como um exemplo paradigmático dos impactos das dinâmicas globais no cibercrime. Diversos estudos (e.g., BAUMAN, 1998; GILLESPIE, 2019; LUO, 2022; ROBERTSON, 1992) sugerem, direta ou indiretamente, que a economia digital globalizada favorece a proliferação de redes criminosas, ao mesmo tempo que expõe fragilidades estruturais nas instituições e nos mercados globais. Outras pesquisas também destacam como essas redes utilizam infraestruturas globais de comunicação, como redes sociais e serviços de email, para alcançar vítimas em todo o mundo (e.g., LEE; PAEK, 2020; MCMAHON et al., 2016). A utilização destas infraestruturas ilustra as assimetrias da globalização, onde os benefícios da interconectividade global são inevitavelmente acompanhados por novos riscos e ameaças.

Apesar da vasta literatura existente sobre phishing, persistem lacunas importantes que requerem uma análise mais aprofundada. Estudos como os de ALKHALIL et al. (2021), TROPINA (2016) e UNODC (2024) destacam a urgência de investigações mais detalhadas sobre a estrutura organizacional das redes de phishing

[II] A Europol coordena investigações transfronteiriças na União Europeia, enquanto a Interpol apoia a cooperação policial global (Europol... INTERPOL... What's the Difference?, 2019)
[III] Director-General/Executive Director of United Nations Office on Drugs and Crime (UNODC)

e os fluxos financeiros que asseguram a sua sustentabilidade operacional. Além disso, verifica-se uma carência de investigações sobre as interseções entre o phishing e as dinâmicas sociopolíticas, nomeadamente no que diz respeito aos efeitos das políticas de globalização nos esforços para combater o cibercrime.

Este estado da arte revela que o phishing não é apenas uma prática isolada de cibercrime, mas sim um fenómeno profundamente enraizado nas dinâmicas globais de interconexão e vulnerabilidades sistémicas. O estudo deste fenómeno requer, portanto, uma abordagem multidimensional que articule as suas implicações económicas, sociais e políticas no contexto de uma economia digital globalizada.

5.1 Estratégias de Engenharia Social e o Alcance Transnacional do Phishing

Segundo SONOWAL (2023), as redes de phishing baseiam as suas operações em estratégias de engenharia social, recorrendo à manipulação psicológica de indivíduos e organizações para obter informações sensíveis ou alcançar ganhos financeiros de forma ilícita. O mesmo autor desenvolve, afirmando que estas redes recorrem a técnicas sofisticadas que exploram vulnerabilidades humanas, como a confiança, a curiosidade, o medo ou a sensação de urgência, para induzir comportamentos que facilitam os ataques. Entre as principais estratégias, destacam-se o envio de emails fraudulentos, a criação de websites falsificados, o uso de mensagens instantâneas e chamadas telefónicas que simulam comunicações legítimas, bem como a personalização de mensagens para se adequar ao perfil das vítimas.

Os e-mails fraudulentos, por exemplo, constituem uma técnica amplamente utilizada, em que os atacantes se fazem passar por instituições de confiança, como bancos, plataformas digitais ou autoridades públicas, para convencer os destinatários a clicar em links maliciosos ou fornecer informações pessoais (WILLIAMS; POLAGE, 2019). A sofisticação destas estratégias é tal que, muitas vezes, as mensagens são personalizadas com base em dados recolhidos previamente, aumentando a credibilidade do ataque (DRAKE et al., 2004). Outro exemplo relevante é o uso de

websites falsificados que replicam de forma quase idêntica as páginas legítimas das organizações, enganando os utilizadores e captando informações como credenciais de acesso ou detalhes financeiros (ABBASI et al., 2010).

No plano transnacional, estas estratégias evidenciam um alcance notável, funcionando de forma coordenada em várias regiões do mundo. Os exemplos que se seguem ilustram a diversidade e a sofisticação das estratégias utilizadas pelas redes de phishing, destacando a sua capacidade de operar em múltiplos contextos geográficos e culturais.

O grupo APT28, também conhecido como Fancy Bear, constitui um caso emblemático, sendo associado a campanhas de phishing patrocinadas pela Rússia. Estas operações utilizam documentos falsificados que simulam entidades governamentais e não governamentais, tendo como alvos setores essenciais como finanças, infraestruturas críticas e defesa, em regiões que incluem a Europa, a Ásia Central e a América do Norte (SLICK, 2022).

Neste contexto, destaca-se o grupo Dark Pink, responsável por sete ataques bem-sucedidos entre 2021 e 2022, dirigidos a organizações governamentais e militares na Ásia e na Europa, afetando países como a Bósnia e Herzegovina, Camboja, Indonésia, Malásia, Filipinas e Vietname, o que evidencia a capacidade destas redes se adaptarem a diferentes contextos regionais e económicos e ajustarem as suas abordagens às especificidades locais (POLOVINKIN, 2023).

Um dos exemplos mais emblemáticos de phishing é a fraude do “Nigerian prince”, na qual os atacantes se fazem passar por membros da realeza alegando dificuldades financeiras. Este esquema, que vitimou milhões de pessoas em todo o mundo, assenta na manipulação psicológica para obter transferências monetárias ou a cedência de informações pessoais (OKOSUN; ILO, 2023).

Outro incidente relevante ocorreu em 2013, quando o Yahoo sofreu um ataque que comprometeu as contas de mais de 3 mil milhões de utilizadores. Os hackers obtiveram acesso a informações sensíveis, como nomes, endereços de e-mail e

palavras-passe, demonstrando a escala global que estas operações podem alcançar e o impacto direto nos indivíduos (PERLROTH, 2017).

Por fim, durante a pandemia de COVID-19, observou-se um aumento expressivo nos ataques de phishing, evidenciando a forma como estas redes exploraram o interesse global por informações relacionadas com o vírus. Cibercriminosos recorreram a mensagens, e-mails e websites falsificados que imitavam organizações de saúde de renome, induzindo os indivíduos a partilharem dados pessoais sensíveis ou a descarregarem software malicioso (EITCA ACADEMY, 2024). Este acontecimento demonstra a sofisticação destas operações e capacidade destas redes capitalizarem sobre momentos de crise global, maximizando o impacto das suas ações ao tirar partido da ansiedade e da procura de informação por parte do público.

As estratégias de engenharia social e o alcance transnacional das redes de phishing, evidenciam a relevância dos fluxos globais de informação e capital para compreender o funcionamento destas práticas. Num ambiente digital interconectado, estas redes tiram partido da rapidez com que dados e valores financeiros circulam globalmente, explorando as oportunidades criadas pela interdependência económica e pela digitalização das transações para expandir as suas operações sem restrições geográficas.

5.2 Impactos Financeiros nas Economias Globalizadas

Na sequência da análise do alcance transnacional e das estratégias de engenharia social utilizadas pelas redes de phishing, importa agora examinar os impactos económicos significativos que estas práticas ilícitas geram, tanto a nível individual como organizacional, no contexto de economias globalizadas. O phishing afeta diretamente as suas vítimas, mas também gera repercussões que impactam setores económicos, expondo fragilidades estruturais e evidenciando os riscos da interconexão económica global (LEVI et al., 2015).

Os prejuízos económicos associados ao phishing são expressivos e multifacetados. Para os indivíduos, estes incluem o roubo de identidades, o acesso

indevido a contas bancárias e perdas financeiras diretas, muitas vezes agravadas pela dificuldade em recuperar os valores subtraídos (ALKHALIL et al., 2021). No caso das organizações, os custos vão além das perdas financeiras diretas, abrangendo danos à reputação, interrupções operacionais, custos de restauro de sistemas e investimento em medidas de cibersegurança para prevenir futuros ataques (VERGARA COBOS; CAKIR, 2024). Por exemplo, segundo dados da Cybersecurity Ventures (MORGAN, 2022) e da Statista (FLECK, 2024), estima-se que o cibercrime, incluindo o phishing, poderá custar à economia global entre 9 a 13 mil milhões de dólares anuais até 2028, evidenciando a dimensão económica do problema.

De acordo com o Global Financial Stability Report do Fundo Monetário Internacional (FMI) (2024), o phishing representa uma ameaça significativa para as cadeias financeiras globais, introduzindo perturbações que comprometem a confiança nos mercados digitais e nas transações eletrónicas. O relatório sublinha que estas cadeias, sustentadas numa infraestrutura digital altamente interdependente, tornam-se especialmente vulneráveis a falhas ou interrupções sempre que dados sensíveis são expostos ou indevidamente utilizados. Os ataques dirigidos a sistemas de pagamento digital e plataformas de comércio eletrónico, além de afetarem diretamente empresas e consumidores, criam uma sensação de insegurança generalizada, reduzindo o volume de transações digitais e, consequentemente, desacelerando o crescimento económico em setores estratégicos. Ainda segundo o FMI, o setor financeiro global enfrentou, nas últimas décadas, mais de 20 mil ataques cibernéticos dirigidos a bancos, seguradoras e gestoras de ativos, resultando em perdas de 12 mil milhões de dólares. Estas ações, frequentemente direcionadas a instituições financeiras em países em desenvolvimento, prejudicam transações internacionais e fragilizam a confiança no sistema financeiro global, demonstrando os riscos sistémicos associados ao cibercrime.

A interdependência das economias globais intensifica, assim, as consequências do phishing, criando um efeito dominó que ultrapassa as fronteiras nacionais.

As vulnerabilidades económicas tornam-se mais visíveis em países com menor capacidade de resposta a ataques cibernéticos (cf. WORLD ECONOMIC FORUM, 2025). Nestes contextos, os prejuízos gerados por redes de phishing não afetam apenas as economias locais, pois assumem repercussões globais, dada a ligação entre cadeias produtivas, fluxos financeiros e redes comerciais internacionais. Por exemplo, a exploração de vulnerabilidades em bancos de países em desenvolvimento pode comprometer transações internacionais e abalar a confiança no sistema financeiro global (STIGLITZ; BHATTACHARYA, 1999). Além disso, a crescente digitalização dos setores financeiros em mercados emergentes, sem a devida proteção contra ataques cibernéticos, aumenta a vulnerabilidade destas economias (NATALUCCI et al., 2024). Desta forma, os impactos económicos do phishing ilustram como as práticas ilícitas exploram, de forma estratégica, as fragilidades dos sistemas económicos globalizados.

5.3 Implicações Sociais num Mundo Interconectado

Seguindo a análise dos impactos económicos das redes de phishing, torna-se igualmente relevante examinar as implicações sociais deste fenómeno, que afeta tanto as estruturas económicas globais, como a confiança, as interações e a dinâmica social no espaço digital. Num mundo cada vez mais interconectado, onde a vida quotidiana depende fortemente da tecnologia, o phishing ameaça a estabilidade social ao minar a confiança digital e intensificar desigualdades preexistentes (ANDERSON; RAINIE, 2023).

A confiança digital é um pilar essencial das interações online, desde a utilização de plataformas de redes sociais até às transações financeiras e ao acesso a serviços públicos. O phishing, ao explorar a boa-fé dos utilizadores e comprometer informações sensíveis, enfraquece essa confiança, gerando um clima de insegurança no uso das tecnologias digitais (HOOPER et al., 2024). Este efeito repercute-se em comportamentos sociais, levando à relutância em partilhar informações, realizar transações eletrónicas ou confiar em novas tecnologias (ANDERSON et al., 2024). A título de exemplo, as vítimas de ataques de phishing frequentemente relatam uma perda prolongada de confiança

em serviços online, afetando tanto a sua experiência digital como o comportamento em ambientes virtuais (GOLDBERG, 2016).

De igual modo, as redes de phishing contribuem para a exacerbação de desigualdades sociais e a criação de dinâmicas de exclusão digital. Indivíduos e comunidades com menor literacia digital, ou com acesso limitado a recursos tecnológicos e educativos, tornam-se alvos mais fáceis destas redes criminosas (GOTTSCHALK; WEISE, 2023). Esta desigualdade aumenta o risco de vitimização, enquanto aprofunda as barreiras que já dificultam a inclusão plena no mundo digital. Isto é visível em regiões com infraestruturas tecnológicas menos desenvolvidas, onde as consequências do phishing podem ser mais graves, uma vez que a recuperação de dados ou de recursos financeiros é limitada por sistemas de segurança mais frágeis e pela ausência de políticas públicas robustas (CALLEJAS et al., 2021).

Para além do impacto estrutural, o phishing provoca um efeito psicológico significativo nas suas vítimas, afetando profundamente a sua identidade e privacidade (ALKHALIL et al., 2021). A apropriação de dados pessoais ou financeiros gera um sentimento de invasão e vulnerabilidade, que muitas vezes se traduz em ansiedade, stress ou até desconfiança generalizada no uso de tecnologias digitais. Este efeito psicológico não se limita ao indivíduo, mas estende-se ao círculo social e profissional das vítimas, criando um impacto social mais amplo (BARKER, 2022; SHLOMAN, 2024; UNITED NATIONS DEVELOPMENT PROGRAMME, 2022). Por conseguinte, a necessidade de restabelecer a privacidade, nomeadamente a complexidade associada à recuperação de uma identidade digital comprometida, evidencia a persistência e a profundidade das consequências deste fenómeno.

5.4 Desafios Políticos na Resposta ao Phishing

Na sequência da análise das implicações sociais do phishing, torna-se essencial examinar os desafios políticos que este fenómeno coloca aos Estados e às instituições internacionais. Num cenário global onde o cibercrime opera de forma transnacional

e sem barreiras geográficas, os governos deparam com dificuldades significativas na conceção e implementação de políticas eficazes para mitigar os efeitos do phishing (BUCKLAND et al., 2015). Estas dificuldades decorrem não só da sofisticação técnica das redes criminosas, mas também das limitações estruturais e institucionais que comprometem a coordenação entre jurisdições (BUCKLAND et al., 2015; SHENG et al., 2009).

Os Estados, ao procurar responder ao phishing, enfrentam desde logo desafios associados à constante evolução das técnicas utilizadas por estas redes. A rápida adaptação dos criminosos às novas tecnologias, aliada à falta de recursos especializados em cibersegurança em muitos países, torna a criação de mecanismos de combate eficazes um esforço complexo (AMOO et al., 2024). Além disso, a ausência de regulamentações globais uniformes dificulta a implementação de respostas coerentes, limitando a eficácia das estratégias nacionais, sendo que, enquanto algumas nações dispõem de avançados sistemas de monitorização e prevenção, outras carecem de infraestruturas básicas para detetar e reagir a este tipo de ataques (PAWLAK; GÉRY, 2024).

Outro obstáculo reside nos limites das jurisdições nacionais na resposta a crimes transnacionais. Segundo Jeff KOSSEFF (2018), o phishing e outros cibercrimes, ao explorar a interconectividade do ciberespaço, atravessam facilmente fronteiras jurisdicionais, dificultando a aplicação de legislações nacionais. A ausência de uma harmonização jurídica global permite que estas redes criminosas tirem partido de lacunas legais, operando em países com regulamentações mais brandas ou inexistentes. O mesmo autor aponta que enquanto algumas jurisdições possuem leis específicas para punir este tipo de ataques, outras carecem de enquadramentos adequados, criando assim ambientes mais permissivos para estas atividades prosperarem.

Para além das diferenças legais, a investigação de crimes transnacionais enfrenta obstáculos de natureza prática. As redes de phishing utilizam frequentemente infraestruturas dispersas por várias jurisdições, como servidores num país e vítimas noutros, exigindo mecanismos de cooperação internacional complexos (HOLT, 2020).

No entanto, tratados como os de assistência jurídica mútua são muitas vezes morosos e burocráticos, dificultando uma resposta célere (OECD, 2012). A desconfiança mútua entre Estados, aliada a interesses geopolíticos divergentes, intensifica as limitações na cooperação internacional, dificultando a implementação de respostas conjuntas eficazes. Este cenário cria um ambiente favorável para que redes criminosas transnacionais explorem lacunas nos sistemas jurídicos e institucionais, perpetuando as suas atividades ao tirar partido das desigualdades legais e da falta de mecanismos globais eficientes para as combater (CEPIK; BORBA, 2011; SECURITYMAGAZINE, 2024).

Na luta contra o phishing, diferentes países têm adotado políticas e estratégias que, embora representem avanços significativos, continuam a revelar limitações inerentes à sua implementação e alcance. Na União Europeia (UE), a adoção do Cybersecurity ACT (2019) e das diretivas Network and Information Security (EUROPEAN COMMISSION, 2025) têm constituído um passo importante no reforço da resiliência das infraestruturas digitais e na promoção da partilha de informações entre os Estados-membros. Conforme destacado pelo World Economic Forum, a mais recente diretiva NIS2, cuja implementação plena ocorreu em outubro de 2024, introduziu requisitos mais rigorosos para a proteção de infraestruturas críticas e estabeleceu prazos para a notificação de violações, visando fortalecer a resposta coordenada a ciberataques de grande escala. No entanto, a eficácia destas iniciativas continua a ser limitada pelas desigualdades nas capacidades nacionais de implementação e fiscalização, que refletem disparidades económicas e tecnológicas entre os países da UE, como inferem o documento de revisão da diretiva NIS da Comissão EUROPEIA (2020) e o relatório intitulado “Assessing the Economic Impact of EU Initiatives on Cybersecurity”, publicado pela Frontier ECONOMICS (2023).

Nos Estados Unidos da América, o Anti-Phishing Working Group (APWG) destaca-se como um esforço colaborativo que reúne entidades governamentais e privadas para combater o phishing (ANTI-PHISHING WORKING GROUP, s.d.). Apesar de desempenhar um papel importante na identificação de ameaças e na partilha de informações, o

APWG, tal como outros mecanismos internacionais, confrontam-se com dificuldades substanciais na neutralização de redes operativas fora da sua jurisdição, sublinhando a necessidade de uma maior harmonização legal e de uma cooperação internacional mais robusta (PERES, 2019).

Estes esforços, embora indispensáveis, demonstram os obstáculos subjacentes à abordagem de um fenómeno de escala global, em que a interconexão digital promove avanços tecnológicos enquanto exacerba os riscos inerentes à criminalidade transnacional. Por outro lado, países em desenvolvimento, onde os recursos são escassos, continuam a ser mais vulneráveis, destacando a disparidade global na capacidade de resposta.

5.5 O Papel das Organizações Internacionais na Coordenação Global

Após a análise dos desafios políticos que os Estados enfrentam na resposta ao phishing, torna-se essencial examinar o papel das organizações internacionais na coordenação de esforços globais para mitigar este fenómeno transnacional. Num cenário onde as redes de phishing operam além das fronteiras nacionais, explorando lacunas jurídicas e desigualdades institucionais, o envolvimento de entidades como a Interpol, Europol e as Nações Unidas surge como essencial para promover uma resposta conjunta e eficaz.

O combate ao phishing, enquanto fenómeno transnacional, exige esforços coordenados que transcendem as capacidades individuais dos Estados (BUÇAJ; IDRIZAJ, 2025). Neste contexto, as organizações internacionais desempenham um papel determinante na promoção da cooperação global, na partilha de informações e na implementação de iniciativas conjuntas que fortalecem as respostas ao cibercrime (PETERS; HINDOCHA, 2020; RADANLIEV, 2024). Entidades como a Interpol, a Europol e as Nações Unidas têm assumido a liderança na criação de quadros normativos, capacitação técnica e operações transfronteiriças destinadas a desmantelar redes criminosas (INTERPOL, 2021; KHAN et al., 2024).

A Interpol tem liderado diversas iniciativas para combater o phishing em múltiplas jurisdições. A operação HAECHI V (v. TEK / LUSA, 2024), realizada em 2024 com a participação de 40 países, resultou em mais de 5.500 detenções, na apreensão de 380 milhões de euros e na identificação de 1.900 vítimas de fraudes como phishing por voz[IV], burlas sentimentais e chantagens sexuais. Complementando, a operação Synergia II (v. INTERPOL, 2024), conduzida entre abril e agosto do mesmo ano, envolveu 95 países e levou à desativação de mais de 22.000 endereços IP maliciosos e à apreensão de servidores e dispositivos utilizados em cibercrimes. Estas ações evidenciam o papel da Interpol na partilha informações estratégicas e na capacitação técnica dos Estados-membros. As suas iniciativas, como os programas de capacitação em cibersegurança para países membros, procuram nivelar as capacidades de resposta entre Estados, enquanto os seus sistemas de alertas internacionais, como os red notices, são fundamentais para a identificação e captura de suspeitos operando em múltiplas jurisdições (INTERPOL, s.d.).

No contexto europeu, a Europol, através do seu Centro Europeu de Cibercriminalidade (EC3), tem desempenhado um papel fundamental no combate ao phishing e outras ameaças cibernéticas. Anualmente, a Europol publica o relatório Internet Organised Crime Threat Assessment (IOCTA), que fornece uma análise abrangente das ameaças cibernéticas emergentes, incluindo o phishing. O relatório mais recente, IOCTA 2024 (v. EUROPOL, 2024), destaca que o phishing permanece o vetor de ataque mais comum entre os esquemas de fraude online, com o smishing (phishing via SMS) a ser a variante mais prevalente, seguida pelo vishing (phishing por voz). Em 2023, emergiu também o quishing, que utiliza códigos QR para direcionar as vítimas a sites maliciosos. Em maio de 2024, a Europol coordenou a Operação Endgame, considerada a maior ação global contra redes de malware. A operação resultou na detenção de quatro indivíduos, na desativação de 100 servidores na Europa e América do Norte e na neutralização de mais de 2.000 domínios utilizados para atividades ilícitas (v. DESMARAIS, 2024).

[IV] O phishing por voz, também conhecido como vishing (uma combinação das palavras “voice” e “phishing”), é um tipo de ataque cibernético baseado em engenharia social que utiliza chamadas telefónicas para enganar as vítimas e levá-las a divulgar informações sensíveis, como credenciais bancárias, dados pessoais ou acessos a contas (Hooper et al., 2024).

As Nações Unidas, através do seu departamento sobre Drogas e Crime (UNODC), têm desenvolvido iniciativas normativas e operacionais. Uma das mais importantes foi a criação do Comitê Ad Hoc para uma Convenção Internacional sobre o Cibercrime (v. EXAME, 2024), que apresentou em 2024 um tratado internacional para harmonizar legislações nacionais e fortalecer a cooperação entre Estados.

A articulação entre Estados, organizações internacionais e setores privados tem sido fundamental, e iniciativas como as promovidas pela Interpol, Europol e UNODC constituem exemplos concretos de como a cooperação internacional tem contribuído para o combate ao cibercrime e para o fortalecimento da resiliência global no domínio digital.

Apesar da eficácia demonstrada por muitas destas iniciativas, persistem desafios significativos. A ausência de um consenso global em torno de normas jurídicas para o ciberespaço, a escassez de recursos em países em desenvolvimento e as complexidades associadas à soberania nacional dificultam a implementação de medidas uniformes (MALAGUTTI, 2022; RADANLIEV, 2024). Os avanços nestes contextos têm sido limitados pela disparidade entre os interesses e prioridades dos países membros, o que dificulta a implementação de uma abordagem uniforme e global (ANEEL et al., 2024). Esta divergência reflete-se na ausência de um consenso internacional acerca de normas jurídicas e operacionais que regulem o ciberespaço de forma abrangente (PAWLAK; GÉRY, 2024). Contudo, estas limitações não obstam a continuidade de esforços conjuntos, que se revelam imprescindíveis para enfrentar as ameaças colocadas pelo phishing – um fenómeno global que transcende fronteiras e explora a interdependência digital de forma sistemática e preocupante.

6 CONCLUSÃO

O presente trabalho apresentou avanços relevantes no cumprimento do objetivo geral, ao analisar as redes de phishing enquanto atores globais no panorama do cibercrime, situando-as no contexto das dinâmicas da globalização. Foi possível

compreender como transformações económicas, culturais e tecnológicas moldam o funcionamento e a expansão destas redes ilícitas, bem como identificar vulnerabilidades estruturais e institucionais que favorecem a sua operação, reforçando a pertinência do estudo no campo dos estudos globais.

A revisão da literatura permitiu identificar as estratégias de engenharia social que sustentam as práticas ilícitas associadas ao phishing, evidenciando a sua sofisticação e capacidade de adaptação num ambiente digital interconectado. Estas redes demonstram um alcance transnacional, aproveitando-se da rapidez dos fluxos globais de informação e capital, bem como de vulnerabilidades estruturais como a falta de literacia digital e a fragmentação das regulamentações internacionais. Este objetivo foi plenamente alcançado, destacando-se as principais técnicas empregues, como o envio de emails fraudulentos e a criação de websites falsificados, que exploram a interconectividade digital para ampliar o impacto das operações. Além disso, o trabalho analisou a relação destas práticas com os fluxos internacionais, reforçando a natureza transnacional das redes de phishing e a sua capacidade de explorar as fragilidades dos sistemas económicos e digitais à escala global.

No plano económico, concluiu-se que o phishing gera prejuízos diretos a empresas e indivíduos, mas também compromete a estabilidade dos mercados financeiros e das transações digitais, aumentando as fragilidades inerentes às economias globalizadas. Este fenómeno afeta a confiança no ecossistema digital, expondo vulnerabilidades sistémicas resultantes da interdependência económica e da insuficiência de respostas coordenadas. A análise realizada permitiu identificar impactos económicos significativos, evidenciando como o phishing prejudica cadeias financeiras e de consumo, fragilizando a confiança nas transações digitais e revelando as debilidades estruturais dos contextos globalizados. Apesar do cumprimento deste objetivo, estudos futuros podem considerar uma abordagem quantitativa que complemente e aprofunde as conclusões qualitativas, proporcionando um quadro mais detalhado sobre a dimensão económica do phishing.

Do ponto de vista social, a análise dos impactos do phishing revelou efeitos significativos na confiança digital e nas dinâmicas sociais, destacando o seu papel na expansão das desigualdades digitais e na criação de climas de insegurança que dificultam a adoção plena de tecnologias digitais. Este objetivo foi cumprido de forma satisfatória, com uma abordagem que incluiu o exame da exclusão digital e do impacto psicológico sentido pelas vítimas, demonstrando como o phishing contribui para reforçar barreiras existentes no acesso ao espaço digital. Contudo, a relação entre desigualdades sociais e vulnerabilidades digitais, embora abordada, beneficiaria de maior profundidade através de estudos empíricos complementares, que poderiam proporcionar uma compreensão mais detalhada e sustentada do fenómeno. Esta dimensão social é essencial para compreender as consequências imediatas do phishing e as suas implicações mais amplas para a coesão social e a inclusão digital global.

Do ponto de vista político, os desafios enfrentados pelos Estados na resposta ao phishing provam a necessidade urgente de uma cooperação internacional mais robusta e estruturada. A ausência de harmonização jurídica global, combinada com as limitações impostas pela soberania nacional e as disparidades entre países, compromete a eficácia e a coordenação de medidas destinadas a combater este fenómeno transnacional. Este objetivo foi abordado de forma abrangente, com a identificação de fatores críticos que limitam as respostas ao phishing, nomeadamente a fragmentação legislativa e as dificuldades na articulação internacional. A complexidade destas dinâmicas sublinha a importância de soluções globais e integradas que possam transcender fronteiras jurídicas e desigualdades institucionais, reforçando o combate eficaz ao phishing.

O trabalho destacou o papel essencial das organizações internacionais, como a Interpol, Europol e UNODC, na promoção de iniciativas conjuntas que têm desempenhado um papel determinante no combate ao fenómeno transnacional do phishing. Este objetivo foi plenamente atingido, evidenciando as contribuições destas entidades na facilitação da cooperação global e no fortalecimento das capacidades

técnicas necessárias para enfrentar o cibercrime. As iniciativas destas organizações incluem desde operações transnacionais para desmantelar redes criminosas até à criação de plataformas para a partilha de informações entre Estados e à capacitação de profissionais na área da cibersegurança.

Conclui-se que o phishing, enquanto prática de cibercrime profundamente enraizada nas dinâmicas da globalização, exige abordagens multidimensionais capazes de integrar esforços económicos, sociais e políticos. Os avanços registados em áreas como a regulamentação, a capacitação técnica e a cooperação internacional representam passos importantes na mitigação deste fenómeno transnacional. Porém, é essencial aprofundar as investigações sobre a estrutura organizacional das redes de phishing e os fluxos financeiros que as sustentam, bem como desenvolver políticas mais inclusivas e harmonizadas que abordem as vulnerabilidades destacadas ao longo desta análise.

Este trabalho proporcionou uma visão abrangente e fundamentada sobre as redes de phishing e os seus impactos globais, cumprindo os objetivos definidos. No entanto, a necessidade de dados empíricos mais robustos e de uma análise mais detalhada de contextos regionais específicos aponta para oportunidades de investigação futura. Ainda assim, o estudo contribui para a compreensão do fenómeno, reforçando a importância de iniciativas contínuas e inovadoras no combate ao phishing e na promoção de um ambiente digital mais seguro e resiliente face aos desafios da interconectividade global.

REFERÊNCIAS

ABBASI, A.; ZHANG, Z.; ZIMBRA, D.; CHEN, H.; NUNAMAKER, J. F., Jr. Detecting Fake Websites: The Contribution of Statistical Learning Theory. **MIS Quarterly**, 34(3), 435–461, 2010. Disponível em: https://doi.org/10.2307/25750686. Acesso em: 15 out. 2026.

ALKHALIL, Z.; HEWAGE, C.; NAWAF, L.; KHAN, I. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. **Frontiers in Computer Science**, 3, 563060, 2021. Disponível em: https://doi.org/10.3389/fcomp.2021.563060. Acesso em: 15 out. 2026.

AMOO, O. O.; ATADOGA, A.; ABRAHAMS, T. O.; FARAYOLA, O. A.; OSASONA, F.; AYINLA, B. S. The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. **World Journal of Advanced Research and Reviews**, 21(2), 205–217, 2024. Disponível em: https://doi.org/10.30574/wjarr.2024.21.2.0438. Acesso em: 15 out. 2026.

ANDERSON, J.; RAINIE, L. T**he most harmful or menacing changes in digital life that are likely by 2035**. Pew Research Center, 21 jun. 2023. Disponível em: https://www.pewresearch.org/internet/2023/06/21/themes-the-most-harmful-or-menacing-changes-in-digital-life-that-are-likely-by-2035/. Acesso em: 15 out. 2026.

ANDERSON, M.; MARCH, E.; LAND, L.; BOSHUIJZEN-VAN BURKEN, C. Exploring the roles played by trust and technology in the online investment fraud victimisation process. **Journal of Criminology**, 57(4), 488–514, 2024. Disponível em: https://doi.org/10.1177/26338076241248176. Acesso em: 15 out. 2026.

ANEEL, S. S.; RAFAY, S. M.; HIJAZI, A.; MUHAMMAD, S.; BILAL, M.; KHAN, U.; AHMAD, S.; QASIM, M.; MUMTAZ, H. Cyberspace as a Global Common: **Formulation and Applicability of International Law** (p. 30). Centre for Aerospace & Security Studies, 2024. Disponível em: https://casstt.com/wp-content/uploads/2024/08/PER-RT-Cyber-GlobalCommon-Rev2-ZM-30-July-2024-HM1-ED-SSA-APP.pdf. Acesso em: 15 out. 2026.

ANTI-PHISHING WORKING GROUP. **About the APWG**. [s.d.]. Disponível em: https://apwg.org/about-us/. Acesso em: 18 out. 2026.

BARKER, J. **The Psychological Impact of Phishing**. Cygenta, 13 jul. 2022. Disponível em: https://www.cygenta.co.uk/post/psychological-impact-phishing. Acesso em: 15 out. 2026.

BAUMAN, Z. **Globalization**: The Human Consequences. Columbia University Press, 1998.

BEUTIN, N.; BORAN, D. **The Great Web 3.0 Glossary**: All you need to know about Blockchain, Crypto, NFT, Metaverse, Service Robots & Artifical Intelligence. Fachmedien Recht und Wirtschaft, 2023.

BOOTH, A.; SUTTON, A.; PAPAIOANNOU, D. **Systematic Approaches to a Successful Literature Review**. SAGE, 2016.

BUÇAJ, E.; IDRIZAJ, K. The need for cybercrime regulation on a global scale by the international law and cyber convention. **Multidisciplinary Reviews**, 8(1), e2025024, 2025. Disponível em: https://doi.org/10.31893/multirev.2025024. Acesso em: 15 out. 2026.

BUCKLAND, B. S.; SCHREIER, F.; WINKLER, T. H. **Democratic Governance Challenges of Cyber Security**. DCAF Horizon, 1, 2015. Disponível em: https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf. Acesso em: 15 out. 2026.

BUTAVICIUS, M.; TAIB, R.; HAN, S. J. Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. **Computers & Security**, 123, 102937, 2022. Disponível em: https://doi.org/10.1016/j.cose.2022.102937. Acesso em: 15 out. 2026.

CALLEJAS, P. J. F.; AFIFI, A.; LOZINSKIY, N. C**ybersecurity in the United Nations system organizations (Report of the Joint Inspection Unit No. JIU/REP/2021/3)**. United Nations, 2021. Disponível em: https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf. Acesso em: 15 out. 2026.

CEPIK, M.; BORBA, P. Crime organizado, estado e segurança internacional. **Contexto Internacional**, 33, 375–405, 2011. Disponível em: https://doi.org/10.1590/S0102-85292011000200005. Acesso em: 15 out. 2026.

COOK-KWENDA, M. Tech-Enabled Global Cybercrime: Exploitation by Transnational Criminal Organizations (TCOS). **IRE Journals**, 8(3), 55–100, 2024.

DAS, S.; NIPPERT-ENG, C.; CAMP, L. Evaluating user susceptibility to phishing attacks. **Inf. Comput. Secur.**, 30, 1–18, 2022. Disponível em: https://doi.org/10.1108/ics-12-2020-0204. Acesso em: 15 out. 2026.

DESMARAIS, A. **Quatro detidos na maior operação de rede de malware do mundo**. euronews, 30 maio 2024. Disponível em: https://pt.euronews.com/next/2024/05/30/quatro-detidos-na-maior-operacao-de-combate-ao-malware-do-mundo-segundo-a-europol. Acesso em: 15 out. 2026.

DRAKE, C. E.; OLIVER, J. J.; KOONTZ, E. **Anatomy of a Phishing Email, 2004**. Disponível em: https://consensus.app/papers/anatomy-of-a-phishing-email-drake-oliver/1bb4c4002e9750e9bd0262148619ee3f/. Acesso em: 15 out. 2026.

EITCA ACADEMY. **Como evoluíram os ataques de phishing durante a pandemia da COVID-19 e que estratégias utilizaram os agentes mal-intencionados para explorar o desejo do público por informação?** 2024. Disponível em: https://l1nq.com/cLNzW. Acesso em: 15 out. 2026.

EMARA, A.; ABDELGHFAR, M. The impact of commercial fraud on e-commerce. Benha **Journal of Humanities Sciences**, 3(3), 177–196, 2024. Disponível em: https://doi.org/10.21608/bjhs.2024.316803.1268. Acesso em: 15 out. 2026.

EUROPEAN COMMISSION. **Combined Evaluation Roadmap/Inception Impact Assessment**: Revision of the NIS Directive, 2020.

EUROPEAN COMMISSION. **NIS2 Directive**: New rules on cybersecurity of network and information systems. 15 jan. 2025. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive. Acesso em: 15 out. 2026.

EUROPOL. **Europol... INTERPOL... what's the difference?** 10 set. 2019. Disponível em: https://www.europol.europa.eu/faq/europol...-interpol...-what's-difference. Acesso em: 15 out. 2026.

EUROPOL. **Internet Organised Crime Threat Assessment (IOCTA) 2024 (Publications Office of the European Union)**. Publications Office of the European Union, 2024. Disponível em: https://data.europa.eu/doi/10.2813/442713. Acesso em: 15 out. 2026.

EUROPOL. **The other side of the coin**: An analysis of financial and economic crime. Publications Office, 2023. Disponível em: https://data.europa.eu/doi/10.2813/105613. Acesso em: 15 out. 2026.

EXAME. **Comitê da ONU finaliza tratado internacional histórico sobre cibercrime** | Exame. exame, 15 ago. 2024. Disponível em: https://exame.com/tecnologia/comite-da-onu-finaliza-tratado-internacional-historico-sobre-cibercrime/. Acesso em: 15 out. 2026.

FLECK, A. **Infographic**: Cybercrime Expected To Skyrocket in Coming Years. Statista Daily Data, 22 fev. 2024. Disponível em: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027. Acesso em: 15 out. 2026.

FRONTIER ECONOMICS. **Assessing the Economic Impact of EU Initiatives on Cybersecurity**, 12 jul. 2023. Disponível em: https://www.frontier-economics.com/media/izyk5rgz/assessing-the-economic-cost-of-eu-initiatives-on-cybersecurity.pdf. Acesso em: 15 out. 2026.

GILLESPIE, A. Cybercrime: Key Issues and Debates. Routledge, 2019.

GOEL, S.; WILLIAMS, K.; DINCELLI, E. Got Phished? Internet Security and Human Vulnerability. **Journal of the Association for Information Systems**, 18(1), 2017. Disponível em: https://doi.org/10.17705/1jais.00447. Acesso em: 15 out. 2026.

GOLDBERG, R. L**ack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities**. National Telecommunications and Information Administration, 13 maio 2016. Disponível em: https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities. Acesso em: 15 out. 2026.

GOTTSCHALK, F.; WEISE, C. **Digital equity and inclusion in education**: An overview of practice and policy in OECD countries. OECD Education Working Paper, 299, 2023. Disponível em: https://one.oecd.org/document/EDU/WKP(2023)14/en/pdf. Acesso em: 15 out. 2026.

GUEMBE, B.; AZETA, A.; MISRA, S.; OSAMOR, V. C.; FERNANDEZ-SANZ, L.; POSPELOVA, V. The Emerging Threat of Ai-driven Cyber Attacks: A Review. **Applied Artificial Intelligence**, 36(1), 2037254, 2022. Disponível em: https://doi.org/10.1080/08839514.2022.2037254. Acesso em: 15 out. 2026.

HEIDING, F.; SCHNEIER, B.; VISHWANATH, A. **AI Will Increase the Quantity—and Quality—of Phishing Scams**. Harvard Business Review, 30 maio 2024. Disponível em: https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams. Acesso em: 15 out. 2026.

HOLT, T. J. Police and Extralegal Structures to Combat Cybercrime. *In*: T. J. Holt & A. M. Bossler (org.), **The Palgrave Handbook of International Cybercrime and Cyberdeviance** (pp. 385–402). Springer International Publishing, 2020. Disponível em: https://doi.org/10.1007/978-3-319-78440-3_12. Acesso em: 15 out. 2026.

HOLT, T. J.; BOSSLER, A. M. (org.). **The Palgrave Handbook of International Cybercrime and Cyberdeviance** (1st ed. 2020 edition). Palgrave Macmillan, 2020.

HOOPER, J.; BANNEAR, B.; CHEW, G. **Anti-Scam Handbook v1.0**: Collective Response and Tools to Safeguard Development i (p. 102). UNDP Policy Centre, 2024. Disponível em: https://www.undp.org/sites/g/files/zskgke326/files/2024-10/undp_anti-scam_handbook_v1.0.pdf. Acesso em: 15 out. 2026.

INTERNATIONAL MONETARY FUND, Monetary and Capital Markets Department. Global Financial Stability Report, April 2024: The Last Mile: Financial Vulnerabilities and Risks. **International Monetary Fund**, 2024. Disponível em: https://doi.org/10.5089/9798400257704.082. Acesso em: 15 out. 2026.

INTERPOL. (sem data). **Cybercrime. Interpol**. Disponível em: https://www.interpol.int/Crimes/Cybercrime. Acesso em: 15 out. 2026.

INTERPOL. **Cybercrime: Covid-19 Impact, 2020**. Disponível em: https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf. Acesso em: 15 out. 2026.

INTERPOL. **INTERPOL cyber operation takes down 22,000 malicious IP addresses**. Interpol, 5 nov. 2024. Disponível em: https://www.interpol.int/News-and-Events/News/2024/INTERPOL-cyber-operation-takes-down-22-000-malicious-IP-addresses. Acesso em: 15 out. 2026.

INTERPOL. **National Cybercrime Strategy Guidebook, 2021**. Disponível em: https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf. Acesso em: 15 out. 2026.

JHONSON, D.; SMITH, J.; SHEHZADI, T. **Digital Trust and Financial Transactions**: Building Confidence in Internet Banking Systems, 2023. Disponível em: https://www.researchgate.net/publication/376485477_Digital_Trust_and_Financial_Transactions_Building_Confidence_in_Internet_Banking_Systems. Acesso em: 15 out. 2026.

KHAN, S. H.; ZAKIR, M. H.; TAYYAB, A.; IBRAHIM, S. The Role of International Law in Addressing Transnational Organized Crime. **Journal of Asian Development Studies**, 13(1), Artigo 1, 2024. Disponível em: https://doi.org/10.62345/jads.2024.13.1.24. Acesso em: 15 out. 2026.

KIESOW CORTEZ, E. Data Breaches and GDPR. *In*: T. J. Holt & A. M. Bossler (org.), **The Palgrave Handbook of International Cybercrime and Cyberdeviance** (pp. 239– 256). Springer International Publishing, 2020. Disponível em: https://doi.org/10.1007/978-3-319-78440-3_39. Acesso em: 15 out. 2026.

KLEIJSSEN, J.; PERRI, P. Cybercrime, Evidence and Territoriality: Issues and Options. In: M. Kuijer & W. Werner (org.), **Netherlands Yearbook of International Law 2016** (Vol. 47, pp. 147–173). T.M.C. Asser Press, 2017. Disponível em: https://doi.org/10.1007/978-94-6265-207-1_7. Acesso em: 15 out. 2026.

KOSSEFF, J. **Developing collaborative and cohesive cybersecurity legal principles**. 2018 10th International Conference on Cyber Conflict (CyCon), 283–298, 2018. Disponível em: https://doi.org/10.23919/CYCON.2018.8405022. Acesso em: 15 out. 2026.

KOVALCHUK, O.; SHYNKARYK, M.; MASONKOVA, M. **Econometric Models for Estimating the Financial Effect of Cybercrimes**. 2021 11th International Conference on Advanced Computer Information Technologies (ACIT), 381–384, 2021. Disponível em: https://doi.org/10.1109/ACIT52158.2021.9548490. Acesso em: 15 out. 2026.

KSHETRI, N. **The Global Cybercrime Industry**: Economic, Institutional and Strategic Perspectives. Springer Science & Business Media, 2010.

LEE, B.; PAEK, S. Y. Phishing and Financial Manipulation. *In*: T. J. Holt & A. M. Bossler (org.), **The Palgrave Handbook of International Cybercrime and Cyberdeviance** (pp. 899–916). Springer International Publishing, 2020. Disponível em: https://doi.org/10.1007/978-3-319-78440-3_43. Acesso em: 15 out. 2026.

LEUKFELDT, R.; HOLT, T. J. (org.). **The Human Factor of Cybercrime**. Routledge, 2020.

LEVI, M.; DOIG, A.; GUNDUR, R.; WALL, D.; WILLIAMS, M. **The Implications of Economic Cybercrime for Policing**: Research report, City of London Corporation. City of London Corporation, 2015. Disponível em: https://orca.cf.ac.uk/88156/1/Economic-Cybercrime-FullReport.pdf. Acesso em: 15 out. 2026.

LINDEMULDER, G.; KOSINSKI, M. **What Is Cybersecurity?** IBM, 12 ago. 2024. Disponível em: https://www.ibm.com/topics/cybersecurity. Acesso em: 15 out. 2026.

LUO, Y. A general framework of digitization risks in international business. **Journal of International Business Studies**, 53(2), 344–361, 2022. Disponível em: https://doi.org/10.1057/s41267-021-00448-9. Acesso em: 15 out. 2026.

MALAGUTTI, M. Regulating States Cyber-Behaviour: Obstacles for a consensus. **Nação e Defesa**, 163, Artigo 163, 2022. Disponível em: https://revistas.rcaap.pt/nacao/article/view/29925. Acesso em: 15 out. 2026.

MALLICK, A. I.; NATH, R. **Navigating the Cyber security Landscape**: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. World Scientific News, 190(1), 1–69, 2024.

MCMAHON, R. A.; BRESSLER, M.; BRESSLER, L. **New Global Cybercrime Calls for High Tech Cyber-Cops**. Journal of Legal, Ethical and Regulatory Issues, 2016. Disponível em: https://www.semanticscholar.org/paper/New-Global-Cybercrime-Calls-for-High-Tech-McMahon-Bressler/c20c349aedcd99fdf6c6921517915e2ca3c666eb. Acesso em: 15 out. 2026.

MOONSAMY, A.; AHMED, M.; GUIDETTI, O.; RASHID, B. The Human Firewall: Mitigating Ransomware Risks in Critical Infrastructures through Human-Centric Approaches. *In*: **Ransomware Evolution** (pp. 192–207). CRC Press, 2024. Disponível em: https://doi.org/10.1201/9781003469506-14. Acesso em: 15 out. 2026.

MORGAN, S. Cybercrime To Cost The World 8 Trillion Annually In 2023. **Cybercrime Magazine**, 13 out. 2022. Disponível em: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/. Acesso em: 15 out. 2026.

NATALUCCI, F.; QURESHI, M.; SUNTHEIM, F. **Rising Cyber Threats Pose Serious Concerns for Financial Stability**. IMF, 9 abr. 2024. Disponível em: https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability. Acesso em: 15 out. 2026.

NTT SECURITY HOLDINGS. **Global Threat Intelligence Report 2023, 19 jun. 2024**. Disponível em: https://www.security.ntt/global-threat-intelligence-report-2023. Acesso em: 15 out. 2026.

OECD. **Typology on Mutual Legal Assistance in Foreign Bribery Cases**. OECD, 2012. Disponível em: https://doi.org/10.1787/a61063e4-en. Acesso em: 15 out. 2026.

OKOSUN, O.; ILO, U. The evolution of the Nigerian prince scam. **Journal of Financial Crime**, 30(6), 1653–1663, 2023. Disponível em: https://doi.org/10.1108/JFC-08-2022-0185. Acesso em: 15 out. 2026.

PAWLAK, P.; GÉRY, A. **Why the World Needs a New Cyber Treaty for Critical Infrastructure**. Carnegie Endowment for International Peace, 28 mar. 2024. Disponível em: https://carnegieendowment.org/research/2024/03/why-the-world-needs-a-new-cyber-treaty-for-critical-infrastructure?lang=en. Acesso em: 15 out. 2026.

PAYNE, B. K. Defining Cybercrime. *In*: T. J. Holt & A. M. Bossler (org.), **The Palgrave Handbook of International Cybercrime and Cyberdeviance** (pp. 3–25). Springer International Publishing, 2020. Disponível em: https://doi.org/10.1007/978-3-319-78440-3_1. Acesso em: 15 out. 2026.

PERES, M. **A cooperação judiciária internacional numa perspetiva prática**. Julgar, 39, 37–55, 2019.

PERLROTH, N. **All 3 Billion Yahoo Accounts Were Affected by 2013 Attack**. The New York Times, 3 out. 2017. Disponível em: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html. Acesso em: 15 out. 2026.

PETERS, A.; HINDOCHA, A. **US Global Cybercrime Cooperation**: A Brief Explainer. Third Way, 26 jun. 2020. Disponível em: https://www.thirdway.org/memo/us-global-cybercrime-cooperation-a-brief-explainer. Acesso em: 15 out. 2026.

PHILLIPS, A.; OJELADE, I.; TAIWO, E.; OBUNADIKE, C. Cyber-security Tactics In Mitigating Cyber-Crimes: A Review And Proposal. **International Journal on Cryptography and Information Security**, 13(2/3), 2023. Disponível em: https://doi.org/10.5121/ijcis.2023.13201. Acesso em: 15 out. 2026.

POLOVINKIN, A. **Dark Pink**: New APT group targets governmental, military organizations in APAC, Europe. Group-IB, 11 jan. 2023. Disponível em: https://www.group-ib.com/media-center/press-releases/dark-pink-apt/. Acesso em: 15 out. 2026.

RADANLIEV, P. Cyber diplomacy: Defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. **Journal of Cyber Security Technology**, 1–51, 2024. Disponível em: https://doi.org/10.1080/23742917.2024.2312671. Acesso em: 15 out. 2026.

ROBERTSON, R. **Globalization**: Social Theory and Global Culture. SAGE, 1992.

SECURITYMAGAZINE. Criminalidade organizada e incerteza geopolítica são ameaças em 2024. **Security Magazine**, 21 fev. 2024. Disponível em: https://www.securitymagazine.pt/2024/02/21/criminalidade-organizada-e-incerteza-geopolitica-sao-ameacas-em-2024/. Acesso em: 15 out. 2026.

SHENG, S.; KUMARAGURU, P.; ACQUISTI, A.; CRANOR, L.; HONG, J. **Improving phishing countermeasures**: An analysis of expert interviews. 2009 eCrime Researchers Summit, 1–15, 2009. Disponível em: https://doi.org/10.1109/ECRIME.2009.5342608. Acesso em: 15 out. 2026.

SHEVCHENKO, P. V.; JANG, J.; MALAVASI, M.; PETERS, G. W.; SOFRONOV, G.; TRÜCK, S. The nature of losses from cyber-related events: Risk categories and business sectors. **Journal of Cybersecurity**, 9(1), tyac016, 2023. Disponível em: https://doi.org/10.1093/cybsec/tyac016. Acesso em: 15 out. 2026.

SHLOMAN, T. **The Psychology of Phishing**: Unraveling the Success Behind Phishing Attacks and Effective Countermeasures. Trellix, 1 fev. 2024. Disponível em: https://www.trellix.com/blogs/research/understanding-phishing-psychology-effective-strategies-and-tips/. Acesso em: 15 out. 2026.

SLICK, S. B. I**ntelligence in Defense of Democracy, PRP 221. LBJ School of Public Affairs, 2022**. Disponível em: https://hdl.handle.net/2152/114667. Acesso em: 15 out. 2026.

SONOWAL, G. **Social Engineering Attack**: Rethinking Responsibilities and Solutions. Nova Science Publishers, Incorporated, 2023.

STIGLITZ, J. E.; BHATTACHARYA, A. **Underpinnings for a stable and equitable global financial system from old debates to a new paradigm**. World Bank Group, 30 abr. 1999. Disponível em: https://documents1.worldbank.org/curated/zh/414721468331876693/pdf/731600WP0under00Box371940B00PUBLIC0.pdf. Acesso em: 15 out. 2026.

TEK / LUSA. **Interpol regista em 2024 recorde na luta contra fraude informática**: Mais de 5.500 detenções e 380 milhões de euros apreendidos. SAPO Tek, 12 dez. 2024. Disponível em: https://tek.sapo.pt/noticias/internet/artigos/interpol-regista-em-2024-recorde-na-luta-contra-fraude-informatica-mais-de-5-500-detencoes-e-380-milhoes-de-euros-apreendidos. Acesso em: 15 out. 2026.

THANKGOD, J. **Cybersecurity in the Age of E-Commerce**: Defending Digital Trade Platforms from Emerging Threats (SSRN Scholarly Paper No. 4858731). Social Science Research Network, 2024. Disponível em: https://doi.org/10.2139/ssrn.4858731. Acesso em: 15 out. 2026.

TROPINA, T. **Do Digital Technologies Facilitate Illicit Financial Flows?** World Bank, Washington, DC, 2016. Disponível em: https://doi.org/10.1596/23803. Acesso em: 15 out. 2026.

UNIÃO EUROPEIA. R**egulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (Cybersecurity Act)**. Official Journal of the European Union, L 151, 2019. Disponível em: http://data.europa.eu/eli/reg/2019/881/oj/eng. Acesso em: 15 out. 2026.

UNITED NATIONS DEVELOPMENT PROGRAMME. **New Threats to Human Security in the Anthropocene**: Demanding Greater Solidarity. United Nations, 2022. Disponível em: https://doi.org/10.18356/9789210028332. Acesso em: 15 out. 2026.

UNODC. **Transnational Organized Crime and the Convergence of Cyber- Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia**: A Shifting Threat Landscape. United Nations Office on Drugs and Crime, 2024. Disponível em: https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf. Acesso em: 15 out. 2026.

VERGARA COBOS, E.; CAKIR, S. **A Review of the Economic Costs of Cyber Incidents**. World Bank, 2024. Disponível em: https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P178769-9ffee49b-b8d5-4779-80e8-701969ad0a18.pdf. Acesso em: 15 out. 2026.

WALY, G. **Speech of Ms. Ghada Waly, Executive Director of UNODC - Opening of the 67th Session of the Commission on Narcotic Drugs**. United Nations: UNODC ROMENA, 14 mar. 2024. Disponível em: https://www.unodc.org/romena/en/press/2024/March/speech-of-ms--ghada-waly--executive-director-of-unodc---opening-of-the-67th-session-of-the-commission-on-narcotic-drugs.html. Acesso em: 15 out. 2026.

WILLIAMS, E. J.; POLAGE, D. How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. **Behaviour & Information Technology**, 38(2), 184–197, 2019. Disponível em: https://doi.org/10.1080/0144929X.2018.1519599. Acesso em: 15 out. 2026.

WORLD ECONOMIC FORUM. **Global Cybersecurity Outlook 2025 (p. 49)**, 2025. Disponível em: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf. Acesso em: 15 out. 2026.

Autoria

1 Bruno André Rodrigues Machado

Licenciado em Solicitadoria pelo Instituto Politécnico de Bragança; Mestre em Ciências Policiais pelo Instituto Superior de Ciências Policiais e Segurança Interna; Pós-graduado em Transição e Transformação Digital nas Organizações; Doutorando em Estudos Globais

https://orcid.org/0009-0003-5585-4433 • bruno.machado.jds@gmail.com

Como citar este artigo

MACHADO, B. A. R. Redes de phishing e cibercrime: impactos e desafios sociais e políticos no contexto global. **InterAção**, Santa Maria, v. 17, n. 3, e99414, p. 1-31, 2026. DOI 10.5902/2357797599414. Disponível em: https://dx.doi.org/10.5902/2357797599414. Acesso em: dia mês abreviado. ano.

Declaração de utilização de inteligência artificial

Na preparação editorial desta versão do manuscrito original foi utilizado o ChatGPT (OpenAI) para apoiar a formatação exigida pela revista. A autoria intelectual e a responsabilidade pelo conteúdo permanecem exclusivamente no autor.