MILÍCIAS DIGITAIS E CIBERCRIME: A ARQUITETURA DOS GOLPES E DAS ESTRATÉGIAS DE MANIPULAÇÃO ONLINE

Camili Medeiros[1]
Luiz Phelipe Ramos Cardoso[2]
Paulo Vinícius Gevarowsky de Morais[3]

RESUMO

O presente artigo propõe uma análise aprofundada da evolução e da profissionalização da criminalidade no ambiente virtual, focando na atuação e arquitetura das milícias digitais. O estudo estabelece que esse fenômeno é uma simbiose orquestrada entre o crime organizado (Primeiro Comando da Capital e Comando Vermelho) e a tecnologia, onde, atraídos pela lucratividade copiosa e o menor risco penal dos crimes e fraudes digitais em comparação aos crimes cometidos fisicamente. O *modus operandi* desses grupos é sofisticado e se fundamenta primeiramente na engenharia social, uma técnica de manipulação psicológica que, aliada à personalização e à qualidade das fraudes, consegue subverter a confiança das vítimas e induzi-las ao erro. A estrutura de apoio desses criminosos é global, com destaque para a *Dark Web*, que funciona como um verdadeiro mercado ilegal de ferramentas e manuais, operando sob o modelo *Crime as a Service (CaaS)*. Facilidade essa, que permite o acesso de indivíduos sem *expertise* técnica, transformando-os em verdadeiros agentes criminosos capazes de executar golpes complexos, como *phishing, ransomware* e sequestro de contas por *SIM Swap.* Essa rede é alimentada pelo recrutamento contínuo e ativo de jovens e laranjas, seduzidos por intermédios de falsos anúncios de emprego e promessas de lucro fácil e rápido, o que garante a expansão do negócio e reduz a vulnerabilidade do grupo criminoso. Em conclusão, o artigo aponta para a urgência de uma resposta multifacetada para proteger a sociedade digital. Tal qual, sugere-se o aprimoramento da legislação, como a aprovação do Projeto de Lei (PL) 1740/2025, que tipifica o aliciamento de jovens para o cibercrime, e o investimento contínuo em *expertise* policial para superar as barreiras de rastreabilidade postas por criptomoedas e VPN (Rede Virtual Privada). Bem como, a conscientização social e a educação da população, visando edificar um pilar mais eficaz, mitigando a vulnerabilidade das vítimas e contendo o avanço das milícias digitais.

Palavras-chave: milícias digitais; fraudes digitais; crime organizado.

1 INTRODUÇÃO

Com o avanço da tecnologia, a utilização do mundo virtual se torna algo recorrente no cotidiano das pessoas. Algo como transferências bancárias, compra de produtos, e até mesmo contato com outras pessoas, se tornam exemplos de afazeres que a alguns anos atrás comum seria, se feito de forma física. Atualmente, mais do que nunca, o inverso se torna verdade. Abrindo portas para a criminalidade que usa de forma criativa e muitas vezes inovadora meios lícitos para alcançar o ilícito, ou então, meios ilícitos visando atividades criminosas com

[1] Estudante do Curso de Direito da FAMEPLAHOÇA – UNIASSELVI. E-mail camili.medeiros0213@gmail.com
[2] Estudante do Curso de Direito da FAMEPLAHOÇA – UNIASSELVI. E-mail luizpheelipe@gmail.com
[3] Estudante do Curso de Direito da FAMEPLAHOÇA – UNIASSELVI. E-mail paulovinicius.pv36@gmail.com

grande potencial de impacto na sociedade. Majoritariamente conduzidas na internet, na *surface web*[4] (superfície da web).

Esses criminosos que promovem tais atividades, fazem parte de um grupo que a poucos anos era seleto, e hoje, se encontra em montes. Os criminosos digitais, ou cibercriminosos, que acabam por se transformar em uma espécie de milícia digital, um grupo que a cada dia que passa toma mais e mais forma, ajustando o seu *modus operandi* quando necessário e mais do que nunca, com a internet, enriquecendo ilicitamente com golpes e fraudes em desfavor da sociedade. (Diniz; Cardoso; Puglia, 2022, p.2).

Dentre todas às práticas criminosas atuais, as mais cotidianas, reiteradas e com grande impacto em nossas vidas, sem dúvidas são os golpes, as fraudes digitais e os famosos furos, que seriam os furtos digitais (Fórum Brasileiro de Segurança Pública, 2025, p.20). Porém, para entendermos tudo isso, precisamos voltar na origem, na estrutura, dissociando-as do modo e da forma.

Versaremos inicialmente sobre a gênese dessas milícias digitais, que podemos caracterizar como uma vertente criminosa. Surgindo em uma simbiose entre o crime organizado e o ambiente digital. Consoante supracitado, a origem não está em um evento isolado, mas sim, decorrente de um longo processo gradual. Sendo assim, o problema de pesquisa constitui-se em: Como é possível detectar as milícias digitais constituídas por cibercriminosos, compreender seu modo de operação e quais as medidas preventivas e repressivas para mitigar os riscos?

Constitui o objetivo geral identificar as milícias digitais juntamente com o modo criminoso de operação deste grupo, como agem, de que forma e, como prevenir.

Como objetivos específicos pretende-se: a) identificar a milícia digital e saber quem faz parte deste grupo criminoso, b) verificar o *modus operandi* da organização criminosa, c) expor os meios utilizados para a prática delituosa.

Faça vista, que a metodologia aplicada no presente estudo, foi realizada por meio de uma revisão bibliográfica de doutrinas, legislações pertinentes e buscas incessantes por informações de caráter oficial. Onde foram analisados artigos, anuários, cartilhas, projetos de lei, entre outros periódicos para a realização desta pesquisa. Visando detectar as milícias digitais constituídas por cibercriminosos, compreender seu modo de operação e adotar medidas de prevenção.

2 DESENVOLVIMENTO

a) DA IDENTIFICAÇÃO DA MILÍCIA DIGITAL E QUEM FAZ PARTE DESTE GRUPO CRIMINOSO.

A milícia digital, pode ser conceituada como: “uma associação de pessoas interligadas de forma mais ou menos flexível e sem um arranjo jurídico-legal, que agem de maneira coordenada ou orquestrada na web, em sua grande maioria pelas redes sociais, se utilizando de robôs, contas automatizadas e perfis falsos [...]” (Lobo; Morais; Nemer, 2021, p.359).

Essa etimologia, mesmo que ampla, pode e deve ser filtrada. Em 2025, presente ano, as principais manifestações de milícias digitais estão associadas à política, na qual, envolvem temas como extremismo, discurso

[4] Surface Web: Superfície da Internet, a web padrão conhecida e utilizada no dia-dia por todos, sendo que a navegação é monitorada e controlada o tempo todo.

de ódio e fake News. Atualmente em análise pelo Supremo Tribunal Federal na Ação Penal n° 2694/2025. Entretanto, neste caso, o cerne da questão é outro.

Nos primórdios da internet, entre 1990 - 2000 (Cendon, 2025), era possível verificar um ambiente sem regulação. Na qual, hackers e crackers utilizavam suas habilidades para fins criminosos, individualmente ou em pequenos grupos, explorando vulnerabilidades por desafio ou somente para roubar informações. As transações se davam em fóruns *undergrounds*[5], mas não havia uma estrutura de comando ou organização hierárquica.

Passados alguns anos, em meados de 2000, o sucesso dos golpes e a facilidade da comunicação online permitiu o avanço das práticas criminosas. Mas desta vez, com organização. Em vez de um único criminoso fazer todo o processo, a fraude e os golpes passaram a ser um trabalho em equipe, onde um grupo se especializa em roubo de dados, outro em criar páginas falsas, e em aplicar golpes de engenharia social, que seria a estratégia de manipulação psicológica comumente usada por criminosos, no contexto de segurança da informação, para induzir as pessoas ao erro e enganá-las através de narrativas convincentes (Abin, 2021).

Neste ínterim, ao decorrer do tempo, a prática de se reunir com pessoas especializadas em determinadas funções para práticas de crimes, foi ficando cada vez mais frequente. Se tornando um negócio lucrativo. As formas e ferramentas de ataque, juntamente com as bases de dados das vítimas começaram a ser comercializadas, tanto nas redes sociais, como na internet e atualmente sendo facilmente achadas na *dark web*[6] (Redação, 2022).

E foi dessa maneira que o cibercrime deixou de ser um mero hobby ou passatempo, passando a consolidar-se como profissão. Nesse estágio que vivemos, o grupo criminoso se profissionaliza hierarquicamente, denomina especialistas e cria setores de atuação. Podendo atuar nessa prática criminosa até mesmo aqueles que se encontram encarcerados. No relatório do Fórum Brasileiro de Segurança Pública de 2024 (FBSP, 2024, p.101) deixa bem evidente o exposto: “enquanto o espaço físico potencializa riscos e limita a quantidade de vítimas possíveis, o mundo virtual permite o escalonamento da ação delituosa e, consequentemente, o lucro do criminoso”.

Destarte a isso, é essencial identificar e combater as milícias digitais, assim como compreender a sua composição. Sua estrutura é simples, formada majoritariamente por criminosos comuns que utilizam a internet para a prática criminosa.

Os principais integrantes dessas milícias digitais criminosas são, sem dúvidas grupos com maior poder e capacidade de mobilização. Logo, atualmente esse posto é ocupado pelo crime organizado, como facções de roubo e tráfico, que observaram no ambiente digital um novo e lucrativo mercado. Antonio Nicaso *apud* (Alves, 2025, p.1), da Rádio Nacional, destaca que o crime organizado está se tornando cada vez mais híbrido e capaz de se adaptar e evoluir lado a lado com o desenvolvimento tecnológico, até aqueles com uso de inteligência artificial, ou mesmo, criptomoedas e metaverso. Onde, já estão sendo utilizadas em atividades ilícitas em diversos países, inclusive no Brasil.

Com o avanço constante da tecnologia acaba influenciando no mercado financeiro, sendo este atualmente, bastante explorado pelas organizações criminosas. Assim, corroborando para as práticas já exercidas, como o esquema de pirâmide, que está tomando diversas proporções distintas no âmbito da criminalidade penal econômica.

---

[5] Underground: Significa pertencer ou se relacionar com uma cultura alternativa que foge dos padrões comerciais, da grande mídia e do mainstream (a corrente principal da sociedade).

[6] *Dark Web*: A *dark web* é uma parte oculta da internet, não indexada por mecanismos de busca comuns, acessada por meio de navegadores especializados como o Tor. Ela hospeda atividades legais e ilegais, oferecendo anonimato, mas também apresentando riscos como golpes e conteúdo ilícito.

Em uma segunda análise, um pouco mais exemplificativa, podemos observar que o aumento da criminalidade digital, é mais negócio para o criminoso praticar ilícitos por meio da internet (via anonimato) do que ir para as ruas e cometer assaltos. Isto porque, se o objetivo principal de quem comete crimes contra o patrimônio é, na maioria esmagadora das vezes, a vantagem econômica, para o criminoso é mais seguro e lucrativo cometer o delito de estelionato do que o de roubo. Aquele, além de possuir pena mais branda, muitas vezes, pela dificuldade encontrada na identificação dos autores durante a fase investigatória, não é solucionado, enquanto que este, além de ter que sair para as ruas, portando uma arma de fogo ou arma branca, e correr o risco de ser interceptado pela polícia, possui uma pena muito mais severa, embora as consequências nem sempre sejam da mesma proporção do que de um desfalque patrimonial provocado por um estelionatário. (Diniz; Cardoso; Puglia, 2022, p.15).

Desta forma, a digitalização dos crimes patrimoniais tem impulsionado outros crimes, como o furto de celulares, que está diretamente ligado à aplicação de golpes bancários e fraudes financeiras, como transações indevidas via PIX e boletos falsificados.

Segundo o FBSP (2024), o crime organizado no Brasil movimentou de julho de 2023 a julho de 2024, R$ 186 bilhões (cento e oitenta e seis bilhões de reais), em práticas delitivas digitais, sendo objeto de renda para as facções. Essa cifra supera a receita estimada de outras atividades ilícitas, como o tráfico de drogas, que gerou cerca de R$15 bilhões (quinze bilhões de reais) no mesmo período. Seguindo os dados do FBSP, relatam ainda que, o prejuízo médio por vítima dessas fraudes gira em torno de R$1.702 (mil setecentos e dois reais) no caso de cartões de crédito e de R$1.470 (mil quatrocentos e setenta reais) para transações bancárias digitais.

No que tange a atuação do crime organizado no ambiente virtual, também entre julho de 2023 a julho de 2024, logo um ano, a cada uma hora 4.504 (quatro mil quinhentos e quatro) novas vítimas entram para a estatística de tentativas de golpes por aplicativos de mensagens ou por ligações no país, podendo ser, conforme já exposto, por transferências via pix ou boletos falsos. Acerca de golpes financeiros por falsas centrais de seguranças foram cerca de 4.678 (quatro mil seiscentos e setenta e oito) vítimas por hora. Ademais, 1.220 (mil duzentos e vinte) a cada 60 minutos sofreram golpes ou fraudes em algum investimento que realizou após publicidade em redes sociais ou internet. Dessa forma, a partir do levantamento feito pelo Fórum Brasileiro de Segurança Pública, é inquestionável a participação das facções criminosas no âmbito das milícias digitais. O Primeiro Comando da Capital (PCC) e o Comando Vermelho (CV) seguem sendo as organizações criminosas mais presentes e operantes na maioria dos estados da federação. (FBSP, 2024).

Entretanto não se pode polarizar somente as organizações criminosas, onde é notório que muitos criminosos também são cidadãos comuns. Sendo esses, muitas vezes, recrutados por intermédio de redes sociais ou anúncios falsos de emprego. Os co-infratores são frequentemente necessários para completar a série complexa de eventos. Alguns são recrutados para fornecer capacidades específicas que podem aumentar a capacidade e o escopo para perpetrar fraudes, enquanto outros são obrigados a realizar tarefas que exigem muito trabalho. Exemplos incluem o recrutamento de facilitadores profissionais legítimos, criminosos cibernéticos com acesso a conhecimento técnico e recursos e operadores de telefonia que realizam telemarketing. (UNODC, 2024).

Vale destacar, que o Branco do Brasil em seu site alerta sobre o tema, trazendo a figura dos laranjas. Na postagem sobre Prevenções e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo e a Corrupção. Em muitos casos esses laranjas, detentores de pouca educação e baixo poder aquisitivo. Assim, acabam por se iludir com propostas de lucro fácil, emprestando seu nome para abertura de contas, emitindo procurações para abrir empresas de fachada e outras práticas.

De forma semelhante, o Superior Tribunal de Justiça (STJ) segundo sua jurisprudência já consolidada, disserta sobre um tema análogo à matéria.

> De um lado, um grupo interessado em ganhar dinheiro por meio de uma estrutura montada apenas para beneficiar seus criadores, mediante a captação de recursos de indivíduos "recrutados"; do outro lado, uma grande quantidade de pessoas atraídas pela perspectiva de lucro fácil, mas normalmente alheia ao verdadeiro objetivo dos captadores; na terceira face, um discurso que mistura marketing, falsas promessas e a "venda" de sonhos; na última face, o verdadeiro propósito dessa suposta oportunidade: o pagamento para aderir ao sistema ou a exigência de compra dos produtos oferecidos pelos recrutadores, trazendo cada vez mais dinheiro para os idealizadores do negócio. Essas são as quatro faces das chamadas pirâmides financeiras (ou Esquema Ponzi), sistema fraudulento identificado pela primeira vez há mais de cem anos, nos Estados Unidos. [...] Esta notícia refere-se ao(s) processo(s): CC 146153 , RHC 132655, HC 293.052, HC 464608 , CC 170392 .

Não obstante que, no dia 16 de abril de 2025, a Deputada Federal Rogéria de Almeida Pereira dos Santos, por meio do Projeto de Lei 1740/2025 (Brasil, 2025a), reconheceu a gravidade da situação aqui exposta. Cuja redação do Projeto de Lei é:

> Recrutamento de jovens para a prática de crimes cibernéticos.
> Art. 288-B Induzir, aliciar, recrutar ou de qualquer modo instigar ou treinar jovem de até 21 (vinte e um) anos de idade à prática de crime cibernético, por meio de grupos organizados ou atuação coordenada em redes digitais:
> Pena: reclusão de 3 (três) a 6 (seis) anos, e multa.
> §1ºIncorre nas mesmas penas quem facilita ou promove o ingresso de jovens até 21 anos em comunidades, grupos ou redes voltadas à prática de crimes cibernéticos.
> §2º A pena é aumentada de 1/3 (um terço) até a metade se:
> I - a vítima for menor de 18 (dezoito) anos;
> II - houver promessa de recompensa financeira ou vantagem indevida;
> III - o agente integrar grupo criminoso estruturado, ainda que informalmente, para a prática reiterada desse tipo de crime.
> §3º Aplica-se as mesmas penas quem cria, divulga ou compartilha, por meio de plataformas digitais, conteúdos com finalidade de doutrinação, apologia ou instrução técnica para a prática de crimes cibernéticos por jovens.” (NR)

Observa-se que a Deputada Federal, analisou a necessidade de alteração legislativa ao Decreto-Lei n° 2.848 de 7 de dezembro de 1940 (Código Penal), para tipificar a conduta de induzir, instigar, recrutar, aliciar ou treinar, por meio de internet ou de qualquer meio digital, jovens até 21 (vinte e um) anos e praticar crime cibernético ou outro crime cuja execução envolva uso de tecnologia da informação. Na qual, deu-se a justificativa do Projeto de Lei 1740/2025, segundo a Deputado Federal, o preenchimento de uma lacuna legislativa que se tornou evidente com a crescente utilização de adolescentes e jovens por organizações criminosas digitais – como grupos de hackers – para execução de crimes tecnológicos. Em geral, os jovens são abordados, recrutados e até treinados por redes virtuais por meio de fóruns, aplicativos de mensagens e jogos online. Muitas vezes, são utilizados como “testas de ferro” ou para executar ações de alto risco, dado seu menor discernimento jurídico e maior vulnerabilidade psicológica.

Tal qual, embora o ordenamento jurídico brasileiro preveja dispositivos de proteção à criança e ao adolescente como o art. 244-B do Estatuto da Criança e do Adolescente (Brasil, 1990), não há atualmente um tipo penal específico que abrange o contexto tecnológico e a atuação insidiosa de criminosos digitais sobre jovens, especialmente entre 18 e 21 anos - faixa etária comumente utilizada em aliciamentos desse tipo.

Ante todo o exposto, no que confere à luz legislativa, judiciária, social, digital e demais vertentes, vislumbra-se com extrema clareza e discricionariedade todos os âmbitos introdutórios da milícia digital. No que toca às práticas delituosas de golpe e outros meios criminosos utilizados. Expondo assim, os membros destas milícias, juntamente com dados alarmantes na perspectiva jurídica do fato.

b) DA VERIFICAÇÃO DO *MODUS OPERANDI,* SIMULTANEAMENTE COM OS MEIOS UTILIZADOS PARA O SUCESSO DA AÇÃO CRIMINOSA.

Assim sendo, com o avanço das ferramentas tecnológicas e digitais, vem crescendo no mundo virtual uma camada mais profunda e especializada do meio à prática do crime de estelionato e outros crimes cibernéticos, onde uma gama muito alta e heterogênea de criminosos vem se formando e se estruturando em grupos para a prática desses crimes. Eles atuam em simbiose com as novas tecnologias e a evolução das redes de conhecimento virtual para o aperfeiçoamento do seu famigerado *modus operandi*. De acordo com o site Jurídicos (2024), *modus operandi*, é: "Nada mais do que uma espécie de passo a passo para a realização do crime, é um conjunto de atos necessários para concluir o objetivo daquele crime".

Para tal entendimento, classificamos o cibercrime em duas vertentes: o próprio, o qual seu ponto alvo são os componentes físicos do aparato computacional (*hardware*)[7], ele visa danificar também seu sistema operacional (*software*)[8], no meio judicial tem como objetivo lesar bens jurídicos informáticos, podendo citar as invasões de dados, interceptações de e-mail e a infiltração de softwares maliciosos (*Malware*)[9] para a captação de dados para fins não dignos e ou para dana-los. Em contrapartida, o cibercrime impróprio caracteriza-se pela utilização de ferramentas digitais como meio delituoso para a prática de crime comuns, de menor potencial ofensivo, sendo esses, em sua grande maioria já tipificados na norma penal.

Nas palavras de Crespo (2015), crimes digitais são tanto crimes tradicionais, já previstos na legislação, contra os valores que tradicionalmente conhecemos como merecedores de proteção, praticado com auxílio da mais moderna tecnologia, bem como as condutas ilícitas passíveis de penas que se voltem contra os sistemas informatizados e os dados. Assim, muitos indivíduos estão se utilizando dos dois meios para a prática do ato delituoso, havendo ainda jurisdições onde vislumbram uma terceira classificação, a qual a atuação se dá pelo uso de um computador como meio acessório, como a exemplo o uso deste para o armazenamento de dados roubados.

E nesse cenário que o *modus operandi* se encaixa, ele nos trará a receita para a prática do ato delituoso por grupos já pré-ordenados, comumente chamados de milícias digitais. Para tanto, precisamos conceituar e traçar um perfil de quem são essas pessoas e onde elas se encontram. Em um cenário onde a realidade está cada vez mais difícil de se determinar, o mundo das redes sociais está, cada vez mais, sendo invadido pelas novas ascensões do mercado tecnológico, as inteligências artificiais (IA). Rastrear esses indivíduos e seus grupos vem se tornando cada vez mais difícil de se executar, tendo em vista, que são verdadeiros dissimuladores em uma manada social, desvirtuada da habilidade de discernir o verdadeiro do falso, ou mesmo da pretensão de quem está atrás da tela.

[7] *Hardware*: Parte física de um computador ou dispositivo eletrônico formada pela placa-mãe, a CPU (Unidade Central de Processamento), a memória RAM (memoria de acesso aleatório), o disco rígido e a placa de vídeo. Estes componentes juntos têm a função executar as atividades definidas pelo Software.
[8] *Software*: Conjunto de instruções, dados ou programas em linguagem de programação executados por um computador ou outro dispositivo eletrônico semelhante. Sua função primordial é transmitir tarefas e comandos para o dispositivo hardware, o qual este executara fisicamente a atividade.
[9] *Malware*: Programa malicioso projetado para invadir, danificar ou desativar computadores, redes, tablets e outros dispositivos com a intenção final de roubar e criptografar dados, danificar arquivos e mesmo espionar as atividades exercidas pelo usuário no aparelho eletrônico.

Segundo Lima e Silva, (2000, p.1), o perfil do criminoso digital é baseado em pesquisa empírica, indica jovens, inteligentes, educados, com idade entre 16 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, uma brincadeira.

Ao adentrar na busca por estes criminosos, nos deparamos com uma barreira de entrada gigantesca, atualmente, de acordo com o Clear Sale (2022) em sua matéria sobre cibercriminosos, quem são, e a dificuldade em puni-los, somente a Polícia federal e polícia paulista se destaca na batalha contra essa rede tão emaranhada nas nossas camadas sociais digitais. Contudo, em razão de serem muitos, sua busca se torna ainda mais infindável. Estes infratores digitais veem armados com inúmeras ferramentas de ocultação e de dissimulação para garantir a prática do crime, ferramentas estas como VPN (Rede Virtual Privada), criptografia e principalmente as criptomoedas (moedas virtuais). Com o surgimento das criptomoedas os infratores aperfeiçoaram seu *modus operandi,* pois pela sua dificuldade de rastreabilidade e consequentemente sua identificação. As criptomoedas foram essenciais para a prática de tal ato, onde os criminosos utilizam-se desses meios para camuflar sua passagem pelo local do crime.

c) DA EXPOSIÇÃO DOS MEIOS UTILIZADOS PARA À PRÁTICA DELITUOSA.

A fim de iluminar o entendimento, os golpistas se utilizam da boa-fé das vítimas, como modelo. Evocamos o caso de múltiplas fraudes e estelionatos cometidos após o desastre natural das enchentes que assolaram o estado do Rio Grande do sul, os quais se estenderam entre, final de abril e o início de maio de 2024. (Brasil, 2025b).

A Polícia Civil do Estado do Rio Grande do Sul (PCRS), por meio da Delegacia de Repressão aos Crimes Informáticos e Defraudações (DRCI/DEIC), na Operação Dilúvio Moral, foram cumpridos mandados de prisão em desfavor dos fraudadores da arrecadação destinada para as vítimas atingidas da tragédia. Em conformidade com o site da PCRS, foram cumpridos três mandados de prisão preventiva e ainda, outros três de busca e apreensão, nos estados de Pernambuco, Minas Gerais e Bahia.

Além de tudo, de acordo com eles, contou com o apoio da Polícia Civil do Estado de Pernambuco (PCPE), através da Delegacia de Repressão ao Estelionato (DPRE/DEPATRI/DIRESP), da Polícia Civil do Estado de Minas Gerais, por meio da Coordenação de Apoio Policial (CAP/COE), e da Polícia Civil do Estado da Bahia, por meio da 2° Delegacia Territorial de Feira de Santana.

A operação teve conclusão com três prisões, uma para cada estado investigado. A fraude foi estruturada da seguinte maneira: 1. Uma falsa página oficial do governo era simulada para a vítima, onde ela era redirecionada para a página falsa de arrecadação, a qual nesta, hipoteticamente, seriam arrecadados valores destinados para as vítimas das enchentes. 2. Em sua página era encontrado um *qr code*[10], em que o usuário poderia por via pix, fazer sua doação, após a transferência, o valor era encaminhado para um *Gateway* de pagamento,[11] através do qual fazia o repasse das quantias para local de destino determinado pelos golpistas. 3. O site, supostamente verdadeiro, era divulgado nos meios midiáticos para que houvesse repercussão em massa das informações da operação de arrecadamento.

[10] *Qr code*: Código de barras bidimensional que armazena qualquer tipo de informação, desde arquivos a links de sites da internet. Seu acesso se faz por meio de uma câmera que irá encane-lo e lhe redirecionar ao seu conteúdo.
[11] *Gateway* de pagamento: Sistema em forma de serviço que viabiliza a conexão e transferência segura e rápida de dados entre um comercio eletrônico e processadores de pagamentos.

Em harmonia com o caso narrado, na explicação de Vinicius Albino *apud* (Pinotti, 2025) da CNN Brasil, especialista em tecnologia e sistemas com inteligência artificial, “os golpes deixaram de ter aquela aparência amadora, com erros de português e design malfeito”. Logo, os criminosos sofisticaram seus meios de manipulação em relação à vítima, baseando-se ilicitamente em três principais métodos (Quadro 1).

Quadro 1 – Métodos Utilizados pelos Criminosos.

Personalização	Implementação de informações relevantes da vítima ou se sua vida para a aplicação do golpe, na maioria das vezes obtidas em roubos e vazamentos de dados.
Qualidade	Qualificação dos meios técnicos e de contatos com a vítima em potencial para gerar mais confiança nesta, com o objetivo de causar uma ideia de confiabilidade da fonte utilizada. Exemplifica se casos em que se utilizam de cabeçalhos e rodapés simulando uma empresa verídica em e-mails, ou mesmo desenhando websites falsos com identidades visuais de empresas já conhecidas para persuadir a vítima.
Engenharia Social	Visam sugerir para a vítima propostas atraentes com supostos desejos ou ambições do indivíduo, formuladas com base em informações pessoais roubadas destas.

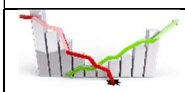
Fonte adaptada pelo autor de: Albino, (2025).

Ainda existe outros métodos e ferramentas que esses golpistas implementam na prática delituosa, mas o mundo informativo e virtual está em constante desenvolvimento e aprimoramento, assim se tornando quase impossível tratar de todos os existentes. Segundo o relatório do Ministério Público do Estado de Minas Gerais (MPMG), intitulado “Tendências em Fraudes para 2025 e o Futuro dos Golpes Digitais” (2025), constata-se um uso gradativo de ferramentas na aplicação de ataques cibernéticos e crimes de fraude. Deduz-se que, a partir de 2025, haverá um aumento de crimes de IA generativa, ataques a carteiras e sistemas de pagamento, *ransomware* mais avançado, fraudes no comércio eletrônico, exposição de APIs (Interface de Programação de Aplicações) e golpes em pagamentos pix ou transferências conta a conta.

Tendo em conta o exposto, existe um rol de crimes praticados na internet e na sua rede mundial de computadores, já que de acordo com uma pesquisa exposta pelo Senado Notícias em 2024, cerca de 24% da população brasileira foi atingida por esses golpes no ano de 2024, não identificando um perfil específico de vítimas, mas tendo uma proporção semelhante às características socioeconômicas da população brasileira.

Dando importância a isso, a Polícia Civil do Estado de Santa Catarina (PCSC), por intermédio de uma cartilha de prevenção contra golpes (2024), se aprofundou nos mais utilizados atualmente como meios de dissuadir, dissimular, enganar e fraudar pessoas, empresas, informações e quantias, tendo como objetivo tomar mais conhecimento aprofundado de como funciona esse caminho do crime e como seus criadores implementam suas estratégias em busca de uma recompensa financeira (Quadro 2).

Quadro 2 – Golpes Atuais Utilizados para a Execução Criminosa.

 *Phishing*[12] (*Pharming*[13] e *Spear phishing*[14])	O golpe opera por intermédio de e-mails na caixa de entrada ou direcionados ao *spam*, ou outras formas de comunicação fraudulentas, com o intuito de induzir a vítima ao erro, e obter informações confidenciais, como dados pessoais e financeiros. Essas mensagens, por sua vez, podem conter links que direcionam a sites maliciosos, visualmente idênticos aos originais, contendo URLs falsas. O redirecionamento de URLs falsas é conhecido como *pharming*, uma subdivisão do *phising*, que ocorre quando o DNS (sistema responsável por traduzir os endereços da web) é manipulado. No primeiro momento, a vítima nem se deu conta de que foi ludibriada, e suas informações apropriadas pelos criminosos. Ademais, o *spear phishing*, normalmente utilizado no meio corporativo com o intuito de comprometer a segurança de corporações e também a possível venda desses dados, já que seus alvos, em geral, são os funcionários das empresas. Muitos desses infratores utilizam IA's (Inteligências artificiais) para alcançar uma aparência mais verídica na aplicação desse golpe, visando manter o padrão gramatical e de comunicação da vítima.
 Pirâmides financeiras	As pirâmides financeiras são conhecidas como Pirâmide de Ponzi[15]. Onde, baseiam sua estrutura em uma falsa promessa de lucro fácil e rápido, a fim, de atrair o máximo de investidores. Exigindo um recrutamento em massa ferrenho, pois o retorno desses investidores é pago com capital dos novos. O esquema colapsa quando o fluxo de novos investidores cessa e, como resultado, a perda total dos valores investidos pelas últimas pessoas que aderiram ao esquema.
 Golpe do pix	Normalmente, nesse método, o golpista se passa por um conhecido ou parente da vítima solicitando uma transação monetária via pix, os criminosos optam por utilizar métodos como engenharia social e personalização para conseguir persuadir a vítima na entrega da quantia. Outra vertente do golpe, é quando o criminoso faz agendamentos de pagamentos e simula seu comprovante em troca de um serviço ou produto. Ao final, a vítima nunca recebe o pagamento e acaba ficando no prejuízo. Um caso semelhante que utilizou esse método, foi o caso já supracitado, da fraude de arrecadação monetária para as vítimas das enchentes do Rio Grande do Sul.
 Investimentos falsos	Essa prática se associa muito a um roubo típico, contudo, o criminoso utiliza técnicas de persuasão para ludibriar a vítima, criando um senso de urgência por meio de expressões como " investimento imperdível". Entretanto, o retorno financeiro prometido pouco volta aos investidores, e os supostos representantes das empresas desaparecem com a quantia e a vítima fica impossibilitada de recuperar o dinheiro.

[12] *Phishing*: Ataque cibernético normalmente realizado por e-mails enganosos que visam obter informações sigilosas, como números de identidade, senhas bancárias, números de cartões de crédito e outras informações confidenciais do usuário. Esses ataques costumam se valer de mensagens que se passam por instituições ou entidades confiáveis para induzir a pessoa ao erro.
[13] *Pharming*: Ataque cibernético que redireciona o usuário de um site legitimo para um falso totalmente idêntico ao original com a finalidade de roubar os dados destes sem que ele perceba.
[14] *Spear phishing*: Termo genérico utilizado para se referir a cibercrimes praticados por meio de e-mails, SMS, chamadas telefônicas, entre outros meios, contra pessoas e empresas específicas.
[15] Pirâmide de Ponzi: Esquema criminoso para captar dinheiro do público através de negócios aparentemente legítimos. Sustentando-se pela entrada de investimento que bancará os lucros dos investidores já inseridos no esquema.

 Sequestro de contas de whatsapp	O método para essa execução é mais aperfeiçoado e os criminosos velem-se muitas vezes de uma ferramenta chamada *SIM Snap*. O método acontece por meio do contato dos golpistas com a operadora, em primeiro momento passam-se pela vítima para poder transferir a linha telefônica do usuário para um chip sobre o controle destes. Com a linha telefônica roubada, aproveitam-se para acessar e captar informações privilegiadas da vítima, por exemplo, números de contas bancárias, redes sociais e podem também se passar pela vítima perante familiares e conhecidos, com o objetivo de obter quantia sem serem reconhecidos.
 Ataques de ransonware	Trata-se do crime de estelionato, em sua forma mais elementar. Contudo, os criminosos têm aperfeiçoado suas técnicas de extorsão. Ocorrida, na maioria das vezes, mediante grave ameaça a vítima, com o intuito de intimidá-la a entregar certa quantia para poder ter acesso novamente aos seus dados roubados ou criptografados. Esses criminosos impedem o acesso do dono as suas informações, através do uso de um malware (site malicioso) e muitas vezes também por meio da criptografia dos dados. Essa tática é usualmente deflagrada contra empresas, tendo em vista o mantimento de informações sensíveis destas para a obtenção de grandes quantias de retorno financeiro.

Fonte adaptada pelo autor de: Polícia Civil do Estado de Santa Catarina, (2024).

Exposto o que são as milícias digitais, quem são seus integrantes, como opera seu *modus operandi* e, quais são os meios e locais onde estes indivíduos praticam seus atos criminosos. É de suma importância agora, entender que muitos dos métodos e crimes citados usufruem-se das mesmas técnicas para a prática de diferentes crimes, ou mesmo o contrário, utilizando diferentes técnicas para um mesmo crime. Observa-se, considerando o que foi dito, que qualquer um, na atualidade, tem capacidade para se tornar um criminoso virtual.

Para tanto, é fundamental explicar e citar a já mencionada, *Dark web*, e seu papel nesse cenário. A *dark web*, é o principal ponto de encontro desses agentes criminais virtuais, sendo um ambiente em que o ilícito prospera. Nesse espaço encontramos plataformas como a *CaaS*[16] (*Crime as a service*[17] *kits de ransonware*[18], campanhas de *phishing*, *dumps* de credenciais, ou seja, nada mais que ferramentas e manuais que permitem a execução da atividade delituosa, podendo qualquer pessoa sem devida experiência técnica, se utilizar desses meios, para novas práticas criminosas. A revista Forbes (2019), comentou sobre o tema em sua publicação, onde qualquer pessoa pode ser um hacker hoje em dia, graças ao *RaaS* (*Ransom as a Service*). Só é preciso um pouco de pesquisa e bitcoins para comprar um serviço de invasão de e-mail na *dark web*.

Sendo assim, ferramentas que facilitam o acesso ao mundo do crime para leigos e aspirantes, servindo também como meio de recrutamento e treinamento de jovens por milicias digitas. Inclusive, cibercriminosos buscam novos talentos e funcionários para seus negócios através de anúncios e entrevistas de emprego.

Consequentemente, produzindo uma interconexão socioeconômica com os principais meios e estratégias de manipulação. A complexidade das milícias digitais é vasta, não reside apenas em sua arquitetura técnica, mas na sua capacidade de estruturar uma economia paralela que explora, simultaneamente, a fragilização da soberania

[16] *Caas (Crime as a service*): Modelo de venda de técnicas e ferramentas ilícitas para a prática de cibercrimes. O especialista cria essas ferramentas para que o usuário comprador não precise ter conhecimento ou mesmo experiencia para utilizar a ferramenta, para assim praticar o crime.
[15] *Kits de ransonware*: Kits de ferramentas e software maliciosos destinados a prática do cibercrime.
[18] *Dump de credenciais*: Técnica para extrair dados de autenticação, como nome de usuários e senhas. Método usado antes de ataques de ransonware ou outros softwares maliciosos.

digital, competente ao Estado e a baixa resiliência cognitiva da sociedade. Sendo assim, uma correlação entre o refinamento das estratégias de manipulação e o agigantamento dos impactos socioeconômicos. Revelando um cenário onde a fraude deixou de ser um delito de oportunidade para tornar-se uma indústria escalável.

Devido à facilidade de acesso a esses recursos, é urgente a implementação de medidas e precauções para evitar que este cenário se agrave nas próximas gerações.

3 CONSIDERAÇÕES FINAIS

Nota se, no presente artigo, analisar a complexa arquitetura das milícias digitais e do cibercrime, como objetivo geral foi instituído o ônus de identificar e compreender o modo de operação desse grupo criminoso, bem como de apontar medidas de prevenção. De modo semelhante, a questão que norteou este artigo foi: "Como é possível detectar as milícias digitas constituídas por cibercriminosos, compreender seu modo de operação e adotar medidas de prevenção?". Que foi respondida, assim como, sanada ao longo desta pesquisa, demonstrando e transparecendo a urgência de uma resposta judicial, legislativa e tecnológica para o presente cenário.

Destacou-se, desde do início, a transformação do ambiente virtual em um novo e lucrativo palco para a criminalidade. Essa transformação digital, resultou na profissionalização dos cibercriminosos, que se organizaram em milícias digitais. Por sua vez, foi revelado que o cerne do problema reside na relação perigosa entre o crime organizado e a tecnologia. Onde, facções como o Primeiro Comando da Capital (PCC) e o Comando Vermelho (CV) viram no meio digital um mercado mais lucrativo e de menor risco penal. Considerando a dicotomia entre o crime presencial, e o crime digital, concluímos que por vezes, o roubo, forma presencial do meio insidioso do tipo subtrair patrimônio alheio, muito se difere do estelionato, prática essa, comumente adotada pelos criminosos, visando a subtração patrimonial de maneira digital. Movimentando quantias monetárias alarmantes, como os R$186 bilhões em práticas delitivas digitais registrados entre julho de 2023 e julho de 2024.

Foi aludido ainda, a verificação do *modus operandi* que, diante da comutação tecnológica evoluiu suas ações individuais para um trabalho em equipe, especializado em roubo de dados, criação de páginas falsas e, principalmente, na aplicação da Engenharia Social. O uso de ferramentas avançadas, Personalização e Qualidade nas fraudes, muitas vezes potencializadas por Inteligência Artificial (IA), conferindo aos golpes uma aparência cada vez mais verídica. Ademais, a *Dark Web* se consolidou como o principal ponto de encontro e mercado para a comercialização de ferramentas criminosas (*Crime as a servisse – CaaS*), facilitando o acesso ao mundo do crime para os leigos e aspirantes. O recrutamento de jovens e de cidadãos comuns, vulgo laranjas, que por meio de anúncios falsos de emprego e promessas de lucro fácil, ingressam nessa expansão criminosa.

Diante da consolidação desse cenário, tem-se em vista a necessidade urgente de soluções que envolvam a prevenção e o combate eficiente dessa *lide*[19]. Sendo crucial a aprovação do Projeto de Lei (PL) 1740/2025, que visa tipificar o recrutamento e treinamento de jovens de até 21 anos para a prática de crimes cibernéticos. Sendo essa medida, indispensável para preencher a lacuna legal existente, conferindo assim, um tratamento penal específico e mais rigoroso à atuação insidiosa dos criminosos digitais.

No que concerne, à luz da prevenção e conscientização social, passa necessariamente pela educação da população e redução diante da Engenharia Social. Como a exposição das práticas delituosas, através de campanhas de conscientização sobre os métodos de golpe (*Phishing*, Pirâmides Financeiras, Golpe do Pix) devem ser disseminadas para mitigar o impacto monetário e social das milícias digitais. No Estado de Santa Catarina, já temos exemplos de órgãos que promovem essa prática, como o Detran/SC, prevenindo os usuários contra os

[19] Lide: Conflito de interesses entre partes que precisa ser resolvido.

Golpes de Pix no seu próprio site, alertando sobre o endereço digital falso. Bem como, a Polícia Civil do Estado de Santa Catarina, que divulgou uma cartilha de prevenção contra golpes, com o seguinte logo: “O golpe tá aí. Cai quem não se informa”

Em conclusão, a ameaça das milicias digitais transcende a esfera digital, configurando um problema de segurança pública e econômica de vastas proporções. A detecção, compreensão do *modus operandi* e a implementação célere de medidas, tanto na esfera legislativa/judicial quanto na conscientização social e repressão tecnológica, sem dúvidas, é o caminho crucial a ser seguido para proteger as próximas gerações e garantir a segurança na sociedade digital.

REFERÊNCIAS.

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN). **Engenharia Social: Guia para Proteção de Conhecimentos Sensíveis**. Brasília, DF: ABIN, 2021. Disponível em: https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/PNPC/boaspraticas/cartilha-engenharia-social-guia-para-protecao-de-conhecimentos-sensiveis. Acesso em: 17 out. 2025.

AGÊNCIA NACIONAL DE ÁGUAS E SANEAMENTO BÁSICO (ANA). **Estudo aponta que enchentes de 2024 foram maior desastre natural da história do RS e sugere caminhos para futuro com eventos extremos mais frequentes**. ANA Notícias, Brasília, DF: [s.n.], 30 abr. 2025. Disponível em: https://www.gov.br/ana/pt-br/assuntos/noticias-e-eventos/noticias/estudo-aponta-que-enchentes-de-2024-foram-maior-desastre-natural-da-historia-do-rs-e-sugere-caminhos-para-futuro-com-eventos-extremos-mais-frequentes. Acesso em: 21 out. 2025.

ALGAR, Blog. **10 golpes mais comuns na internet: saiba quais são!** Algar Blog, 2025. Disponível em: https://blog.algar.com.br/golpes-mais-comuns-na-internet/. Acesso em: 12 out. 2025.

ALVES, Tatiana. **Estudo aponta que crime organizado se adapta a novas tecnologias.** Radio Agência, 22 abr. 2025. Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/seguranca/audio/2025-04/estudo-aponta-que-crime-organizado-se-adapta-novas-tecnologias. Acesso em: 22 ago. 2025.

BANCO DO BRASIL. **Conheça as tipologias do crime lavagem de dinheiro**. BB Segurança, 2025. Disponível em: https://www.bb.com.br/pbb/pagina-inicial/bb-seguranca/prevencao-e-combate-a-lavagem-de-dinheiro-e-ao-financiamento-do-terrorismo-e-a-corrupcao/conheca-as-tipologias-do-crime-lavagem-de-dinheiro#/ . Acesso em: 04 set. 2025.

BRASIL, Câmara dos Deputados. **Projeto de Lei nº 1740, de 2025**. Autor: Rogéria Santos. Dispõe sobre a tipificação penal do aliciamento e recrutamento de menores para a prática de crimes cibernéticos. Brasília, DF, 24 de abril de 2025. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2498284. Acesso em: 26 ago. 2025.

BRASIL. Superior Tribunal de Justiça. **Os quatro lados de um projeto de ruína: as pirâmides financeiras segundo a jurisprudência do STJ**. Notícias STJ, Brasília, DF, 18 set. 2022. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2022/18092022-Os-quatro-lados-de-um-projeto-de-ruina-as-piramides-financeiras-segundo-a-jurisprudencia-do-STJ.aspx. Acesso em: 26 ago. 2025.

CAMPÊLO, Maria. **Engenharia social: como aspectos psicológicos podem se relacionar com golpes e fraudes**. 2024. Disponível em: https://www.gov.br/investidor/pt-br/penso-logo-invisto/engenharia-social-como-aspectos-psicologicos-podem-se-relacionar-com-golpes-e-fraudes-1. Acesso em: 22 ago. 2025.

CARDOSO; DINIZ; PUGLIA. **O crime de estelionato e suas implicações na era contemporânea: o constante crescimento dos golpes via internet.** Libertas Direito, Belo Horizonte, v.3, n.1, jul 2022. Disponível em: https://www.periodicos.famig.edu.br/index.php/direito/article/view/215/142. Acesso em: 21 set. 2025.

CENDON, Beatriz Valadares. **A internet.** Fontes de Informação para pesquisadores e profissionais. Belo Horizonte: Editora UFMG, p. 275-300, 2000.

CLEARSALE, blog. **Cibercriminosos: quem são e por que é tão difícil puni-los?** ClearSale, 2022. Disponível em: https://br.clear.sale/blog/cibercriminosos. Acesso em: 12 out. 2025.

CNN BRASIL. **Golpes digitais estão mais sofisticados e personalizados; como evitar cair?** CNN Brasil, 2025. Disponível em: https://www.cnnbrasil.com.br/tecnologia/golpes-digitais-estao-mais-sofisticados-e-personalizados-como-evitar-cair/. Acesso em: 12 out. 2025.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). **Pirâmides financeiras e esquemas Ponzi.** CVM, 2022. Disponível em: https://www.gov.br/investidor/pt-br/investir/cuidados-ao-investir/evitando-problemas/principais-fraudes-e-esquemas-irregulares/piramides-financeiras-e-esquemas-ponzi. Acesso em: 12 out. 2025.

DETRAN/SC. **Site Falso do Detran/sc**. Brasil, Santa Catarina, 31 mar. 2024. Disponível em: https://www.detran.sc.gov.br/site-falso-do-detran-sc-2/. Acesso em: 21 out. 2025.

ESCRITÓRIO DAS NAÇÕES UNIDAS SOBRE DROGAS E CRIME. **Fraude Organizada.** Viena: UNODC, 2024. Disponível em: https://brasil.un.org/sites/default/files/2025-04/PT_IssuePaperFraud.pdf. Acesso em: 25 out. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **19º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 16 out. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública**. São Paulo: FBSP, 2024. Disponível em: https://publicacoes.forumseguranca.org.br/items/f62c4196-561d-452d-a2a8-9d33d1163af0. Acesso em: 22 set. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA**. Rastreamento de Produtos e Enfrentamento ao Crime Organizado no Brasil**. São Paulo: FBSP, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/items/5c49e7c2-f01f-42c8-ae13-83d8fa9987c6. Acesso em: 22 set. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Segurança Pública e Crime Organizado no Brasil**. São Paulo: FBSP, 2024. Disponível em: https://publicacoes.forumseguranca.org.br/items/fcb7e2a1-8f36-487e-9190-8ecf4d294747. Acesso em: 22 set. 2025.

JURÍDICOS. **Qual o significado de Modus Operandi?** Jurídicos, 2024. Disponível em: https://www.juridicos.com.br/modus-operandi/. Acesso em: 12 out. 2025.

KASPERSKY. **O que é crime cibernético?** Kaspersky, 2017. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 12 out. 2025.

LÔBO; MORAIS; NEMER. **Democracia em perigo: compreendendo as ameaças das milícias digitais no Brasil.** Estudos Eleitorais, Brasília, DF, V.15, n.2, dezembro 2021. Disponível em: https://revistaeje.tse.jus.br/estudoseleitorais/article/view/233. Acesso em: 21 set. 2025.

MACHADO, Leia. **Cibercrime movimenta R$ 186 bilhões no Brasil**. Security Leaders, 14 fev. 2025. Disponível em: https://securityleaders.com.br/cibercrime-movimenta-r-186-bilhoes-no-brasil/. Acesso em: 21 set. 2025.

MINISTÉRIO PÚBLICO DO ESTADO DE MATO GROSSO. **Tendências em fraudes para 2025 e o futuro dos golpes digitais**. MPMT, 2025. Disponível em: https://www.mpmt.mp.br/portalcao/news/1217/153221/tendencias-em-fraudes-para-2025-e-o-futuro-dos-golpes-digitais/100. Acesso em: 12 out. 2025.

MONROE COLLEGE, Cybersecurity. **History, Hacking & Data Breaches.** Monroe College **News**, 2025. Disponível em: https://www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches. Acesso em: 25 ago. 2025.

OFICINA DA NET. **Golpes da internet: confira a lista dos principais e saiba como evitar de cair na armadilha**. Oficina da Net, 2021. Disponível em: https://www.oficinadanet.com.br/post/12727-golpes-da-internet-confira-a-lista-dos-principais-e-saiba-como-evitar-de-cair-na-armadilha. Acesso em: 12 out. 2025.

PORTO SEGURO, Blog. **6 principais golpes digitais de 2025: como se proteger das ameaças.** Blog Porto Seguro, 10 jul. 2025. Disponível em: https://blog.portoseguro.com.br/6-principais-golpes-digitais-de-2025-como-se-proteger-das-ameacas. Acesso em: 04 set. 2025

REDAÇÃO. **Venda de Dados de brasileiros na *dark web* soma R$88 milhões**, 2022. Disponível em: https://www.cisoadvisor.com.br/venda-de-dados-de-brasileiros-na-dark-web-soma-r-88-milhoes/. Acesso em: 16 out. 2025.

RIO GRANDE DO SUL (Estado). Polícia Civil. **Nova fase da Operação Dilúvio Moral é deflagrada no combate a fraudes praticadas durante o período de enchentes no RS.** PC/RS, 2024. Disponível em: https://www.pc.rs.gov.br/nova-fase-da-operacao-diluvio-moral-e-deflagrada-no-combate-a-fraudes-praticadas-durante-o-periodo-de-enchentes-no-rs. Acesso em: 12 out. 2025.

RODAS, Sérgio. **Avanço digital explica explosão de estelionatos, não exigência de representação.** Consultor Jurídico, 18 ago. 2025. Disponível em: https://www.conjur.com.br/2025-ago-18/avanco-digital-explica-explosao-de-estelionatos-nao-exigencia-de-representacao/. Acesso em: 22 ago. 2025.

SANTA CATARINA (Estado). Polícia Civil. **Cartilha: prevenção de golpes**. Florianópolis, 2024. Disponível em: https://pc.sc.gov.br/wp-content/uploads/2024/04/Cartilha-Prevencao-Golpes-1.pdf. Acesso em: 21 out. 2025.

SANTA CATARINA. Tribunal de Justiça. **Entenda como funcionam os ataques de hackers na internet**. TJSC, 2025. Disponível em: https://www.tjsc.jus.br/web/servidor/dicas-de-ti/-/asset_publisher/0rjJEBzj2Oes/content/entenda-como-funcionam-os-ataques-de-hackers-na-internet. Acesso em: 25 ago. 2025.

SANTOS, Carlos Henrique Aguiar dos; MARCHI, Késsia Rita da Costa. **O que a Deep Web pode oferecer além da Surface Web**. Trabalho de Conclusão de Curso (Tecnologia em Sistemas para Internet) – Universidade Paranaense, Paranavaí, 2013. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/38756570/Carlos_Henrique_Aguiar_dos_Santos-libre.pdf. Acesso em: 04 set. 2025.

SCHIAPPA, Daniel. **Entenda como funciona a *dark web*, onde acontecem grandes negócios de crimes virtuais.** Forbes, 2019. Disponível em: https://forbes.com.br/colunas/2019/09/entenda-como-funciona-a-dark-web-onde-acontecem-grandes-negocios-de-crimes-virtuais/. Acesso em: 12 out. 2025.

SENADO FEDERAL, Notícias. **Golpes digitais atingem 24% da população brasileira, revela DataSenado**. Senado, 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado. Acesso em: 12 out. 2025.

SILVA, Danielly. **Cibercriminalidade: uma releitura acerca do "modus operandi**". Jusbrasil, 2022. Disponível em: https://www.jusbrasil.com.br/artigos/cibercriminalidade-uma-releitura-acerca-do-modus-operandi/1542934635. Acesso em: 12 out. 2025.