

A ENGENHARIA SOCIAL COMO FERRAMENTA DE INTELIGÊNCIA POLICIAL: APLICAÇÕES E LIMITES NA ATUAÇÃO DA POLÍCIA MILITAR DO PARÁ

SOCIAL ENGINEERING AS A TOOL FOR POLICE INTELLIGENCE: APPLICATIONS AND
LIMITATIONS IN THE OPERATIONS OF THE PARÁ MILITARY POLICE

INGENIERÍA SOCIAL COMO HERRAMIENTA PARA LA INTELIGENCIA POLICIAL:
APLICACIONES Y LIMITACIONES EN EL DESEMPEÑO DE LA POLICÍA MILITAR DE
PARÁ

Jailson Otávio Ribeiro Lopes¹

Danival da Silva Almeida²

Kelen Fernanda Ferezini³

Nayara Alves de Jesus⁴

RESUMO: A crescente digitalização das relações sociais e institucionais ampliou significativamente a incidência de fraudes cibernéticas baseadas em engenharia social, tornando o fator humano um dos principais vetores de vulnerabilidade em organizações públicas e privadas. Nesse contexto, o presente artigo analisa a engenharia social como ferramenta de inteligência policial, investigando suas aplicações e limites na atuação da Polícia Militar do Pará (PMPA). O problema de pesquisa consiste em compreender de que maneira técnicas de engenharia social podem contribuir para a produção de conhecimento de inteligência sem violar direitos fundamentais, princípios éticos e limites legais impostos à atividade policial militar. O objetivo geral é avaliar o potencial da engenharia social como instrumento de inteligência policial preventiva e repressiva, identificando riscos, oportunidades e mecanismos de controle institucional. A metodologia adotada é qualitativa, de natureza exploratória e descritiva, baseada em pesquisa bibliográfica e documental, com análise de normas constitucionais, publicações acadêmicas, cartilhas institucionais e dados recentes sobre fraudes digitais no Brasil. Os resultados indicam que a engenharia social pode ser empregada legitimamente em ações de conscientização, prevenção de golpes, análise de comportamento criminoso e proteção de ativos informacionais da PMPA, contribuindo para a preservação da ordem pública e da segurança institucional. Contudo, seu uso operacional encontra limites constitucionais relacionados à legalidade, proporcionalidade, privacidade e dignidade da pessoa humana. Conclui-se que a PMPA deve priorizar o emprego defensivo da engenharia social, mediante protocolos normativos, capacitação continuada e integração com órgãos de inteligência e segurança cibernética, fortalecendo sua missão constitucional de polícia ostensiva e preservação da ordem pública.

I

Palavras-chave: Engenharia social. Inteligência policial. Segurança pública. Polícia Militar do Pará. Fraudes digitais. Segurança da informação.

¹ Mestrando no Programa de Pós-graduação em Computação, UFOPA. Bacharel em Sistemas de Informação, Universidade Federal do Oeste do Pará (UFOPA), Santarém-PA, Brasil. Pós-graduação Lato Sensu em Informática na Educação e Tutoria em Educação a Distância, FAVENI.

² Pós-graduação Lato Sensu em Segurança Pública, FAVENI. Curso Superior em Gestão em Organização de Saúde, FIT - Faculdades Integradas do Tapajós, Santarém-PA, Brasil.

³ Pós-graduação Lato Sensu em Segurança Pública, EAD - FAVENI. Bacharel em Engenharia Civil, Centro Universitário Luterano de Santarém (ULBRA), Santarém-PA, Brasil.

⁴ Pós-graduação Lato Sensu em Direito Penal e Processo Penal, Faculdade Única. Curso Superior em Direito, Universidade Luterana do Brasil, Santarém-PA, Brasil.

ABSTRACT: The increasing digitalization of social and institutional relations has significantly expanded the incidence of cyber fraud based on social engineering, making the human factor one of the main vectors of vulnerability in public and private organizations. In this context, this article analyzes social engineering as a police intelligence tool, investigating its applications and limits within the activities of the Military Police of Pará (PMPA). The research problem seeks to understand how social engineering techniques may contribute to intelligence production without violating fundamental rights, ethical principles, and legal limits imposed on military police activity. The general objective is to assess the potential of social engineering as a preventive and repressive police intelligence instrument, identifying risks, opportunities, and institutional control mechanisms. The methodology is qualitative, exploratory, and descriptive, based on bibliographic and documentary research, including constitutional norms, academic publications, institutional prevention booklets, and recent data on digital fraud in Brazil. The results indicate that social engineering may be legitimately employed in awareness campaigns, fraud prevention actions, criminal behavior analysis, and protection of PMPA informational assets, contributing to public order preservation and institutional security. However, its operational use is limited by constitutional principles related to legality, proportionality, privacy, and human dignity. It is concluded that PMPA should prioritize the defensive use of social engineering through normative protocols, continuous training, and integration with intelligence and cybersecurity agencies, thereby strengthening its constitutional mission of preventive policing and public order preservation.

Keywords: Social engineering. Police intelligence. Public security. Military Police of Pará. Digital fraud. Information security.

I INTRODUÇÃO

A transformação digital da sociedade brasileira alterou profundamente as formas de comunicação, interação econômica e circulação de informações. O crescimento do uso de aplicativos bancários, redes sociais, plataformas de comércio eletrônico e sistemas governamentais digitais ampliou não apenas as facilidades de acesso aos serviços, mas também as oportunidades para práticas criminosas baseadas na manipulação psicológica das vítimas. Entre essas práticas, destaca-se a engenharia social, entendida como o conjunto de técnicas utilizadas para obter informações, acesso ou vantagens mediante exploração de emoções, confiança, autoridade, urgência ou desconhecimento das pessoas.

Segundo Santos (2013), a engenharia social representa o aproveitamento do fator humano como ponto vulnerável dos sistemas de segurança da informação, sendo frequentemente mais eficaz do que ataques puramente tecnológicos. A criminalidade contemporânea passou a combinar recursos digitais e estratégias psicológicas, produzindo fraudes cada vez mais sofisticadas, especialmente em operações financeiras eletrônicas e golpes envolvendo o sistema Pix.

A relevância do tema para a Polícia Militar do Pará decorre de sua missão constitucional de polícia ostensiva e preservação da ordem pública, prevista no artigo 144 da Constituição Federal de 1988. A atuação policial moderna exige capacidade de produzir conhecimento

estratégico, prevenir riscos, proteger ativos institucionais e orientar a população quanto às novas modalidades criminosas. Nesse cenário, a engenharia social apresenta dupla dimensão: de um lado, constitui ameaça concreta à segurança institucional; de outro, pode fornecer elementos para atividades de inteligência policial, desde que observados os limites legais e éticos.

O problema central desta pesquisa é o seguinte: de que maneira a engenharia social pode ser utilizada como ferramenta de inteligência policial pela Polícia Militar do Pará sem comprometer direitos fundamentais e garantias constitucionais?

O objetivo geral consiste em analisar as aplicações e os limites da engenharia social na atuação da PMPA. Como objetivos específicos, pretende-se:

(a) conceituar engenharia social e inteligência policial; (b) identificar formas legítimas de utilização preventiva e defensiva pela PMPA; (c) examinar limites jurídicos, éticos e institucionais; e (d) propor diretrizes para o fortalecimento da segurança institucional e da atividade de inteligência.

A pesquisa justifica-se pela crescente incidência de fraudes digitais e pela necessidade de atualização das práticas de inteligência policial diante da criminalidade cibernética. Dados recentes indicam aumento expressivo dos riscos digitais no Brasil, evidenciando a importância de estratégias preventivas baseadas em educação digital e proteção do fator humano (INFOMONEY, 2026).

2 FUNDAMENTAÇÃO TEÓRICA

Engenharia social: conceito e evolução

A engenharia social pode ser definida como o emprego de técnicas de persuasão, manipulação psicológica e exploração comportamental para obtenção de informações sigilosas, acesso indevido a sistemas ou realização de ações em benefício do agente manipulador. Diferentemente dos ataques exclusivamente técnicos, a engenharia social direciona-se às pessoas, explorando aspectos emocionais e cognitivos.

Santos (2013) destaca que o ser humano constitui o elo mais vulnerável da cadeia de segurança da informação, razão pela qual organizações devem investir não apenas em tecnologia, mas também em conscientização e treinamento contínuo.

As cartilhas do Tribunal de Justiça do Pará enfatizam que golpes de engenharia social frequentemente utilizam identidade visual de instituições públicas, mensagens urgentes e

simulação de autoridade para induzir vítimas a fornecer dados pessoais, códigos bancários e credenciais de acesso (TJPA, 2026).

Inteligência policial e produção de conhecimento

A inteligência policial compreende o conjunto de atividades destinadas à obtenção, análise e disseminação de conhecimentos necessários ao planejamento e à execução das ações de segurança pública. Seu objetivo principal é apoiar a tomada de decisão estratégica, tática e operacional.

No âmbito da PMPA, a inteligência policial deve contribuir para prevenção criminal, proteção institucional, gestão de riscos e apoio às operações policiais. A análise de padrões comportamentais utilizados por criminosos em golpes digitais pode gerar conhecimento útil para ações preventivas, campanhas educativas e identificação de ameaças emergentes.

Engenharia social e criminalidade digital

O crescimento das fraudes digitais evidencia a centralidade da engenharia social na criminalidade contemporânea. O Ministério Público de Santa Catarina ressalta que organizações criminosas passaram a utilizar intensamente técnicas de manipulação psicológica em fraudes bancárias, falsos atendimentos, sequestros virtuais e golpes financeiros, exigindo resposta integrada do sistema de justiça e dos órgãos de segurança pública (MPSC, 2026).

O Tribunal de Contas da União identificou falhas no combate a golpes que utilizam identidade de órgãos públicos, demonstrando que a confiança institucional pode ser explorada por criminosos em larga escala (TCU, 2026).

3 A MISSÃO CONSTITUCIONAL DA PMPA E A PREVENÇÃO DE FRAUDES

A Constituição Federal atribui às polícias militares a preservação da ordem pública. Essa missão envolve não apenas repressão criminal, mas também prevenção, orientação social e proteção da coletividade. Campanhas de conscientização sobre golpes via Pix realizadas por diversas polícias militares demonstram que a educação preventiva constitui instrumento relevante de redução da vitimização (CLUBE FM, 2026; ITAÚNA ALERTA, 2026).

No contexto paraense, a PMPA pode ampliar ações de polícia comunitária e comunicação social voltadas à prevenção de fraudes digitais, fortalecendo o vínculo de confiança com a população e reduzindo oportunidades para criminosos.

Limites jurídicos e éticos

O uso de técnicas de engenharia social por agentes públicos deve observar os princípios constitucionais da legalidade, moralidade, proporcionalidade, privacidade e dignidade da pessoa humana. A obtenção de informações mediante fraude, dissimulação abusiva ou induzimento ilícito pode comprometer direitos fundamentais e gerar nulidades, responsabilidade administrativa, civil e penal.

Portanto, qualquer utilização de técnicas inspiradas em engenharia social no contexto policial deve restringir-se a atividades autorizadas em lei, especialmente ações de treinamento, simulação controlada, conscientização e proteção institucional.

4 METODOLOGIA

A pesquisa caracteriza-se como qualitativa, exploratória e descritiva. Optou-se por abordagem qualitativa por permitir análise aprofundada de conceitos, normas, práticas institucionais e implicações éticas relacionadas à engenharia social e à inteligência policial.

Quanto aos procedimentos técnicos, realizou-se pesquisa bibliográfica e documental. Foram examinadas obras acadêmicas, legislações, cartilhas institucionais, relatórios e publicações especializadas sobre segurança da informação, inteligência policial e fraudes digitais.

5

As principais fontes utilizadas foram: Constituição Federal de 1988; monografia de Santos (2013); cartilhas do Tribunal de Justiça do Pará; publicações sobre golpes via Pix; artigo do Ministério Público de Santa Catarina; relatório do Tribunal de Contas da União; e notícias recentes sobre riscos digitais no Brasil.

A análise dos dados ocorreu mediante técnica de análise de conteúdo temática, organizada em quatro categorias: conceito de engenharia social, aplicações em inteligência policial, riscos e limites, e contribuições para a missão institucional da PMPA.

Como se trata de pesquisa bibliográfica e documental, não houve coleta de dados pessoais nem participação de seres humanos, inexistindo necessidade de submissão a comitê de ética.

5 RESULTADOS E DISCUSSÃO

Aplicações legítimas da engenharia social na PMPA

A análise das fontes consultadas permitiu identificar quatro aplicações legítimas da engenharia social que se mostram compatíveis com a missão institucional da Polícia Militar do

Pará (PMPA). Embora o termo “engenharia social” esteja frequentemente associado à prática criminosa de manipulação de pessoas para obtenção indevida de informações ou vantagens, seus conhecimentos e métodos também podem ser empregados sob uma perspectiva defensiva, educativa e preventiva. Nesse sentido, sua utilização pela instituição deve estar direcionada à redução de vulnerabilidades humanas, à prevenção de crimes e ao fortalecimento da segurança institucional.

Uma primeira aplicação refere-se às **campanhas preventivas e à educação digital**. A PMPA pode utilizar conhecimentos relacionados à engenharia social em ações educativas destinadas à população, demonstrando, de maneira acessível, como criminosos utilizam técnicas de persuasão, criação de situações de urgência, falsas identidades e outros mecanismos de manipulação psicológica para induzir vítimas à realização de transferências, ao fornecimento de dados pessoais ou ao acesso a links fraudulentos. Essa abordagem apresenta especial relevância diante do crescimento dos golpes praticados por meio de aplicativos de mensagens, falsas centrais bancárias e fraudes envolvendo o Pix. A atuação preventiva, nesse contexto, contribui para ampliar a capacidade de autoproteção da população e fortalecer a prevenção primária da criminalidade.

A segunda aplicação está relacionada ao treinamento interno e à segurança institucional. A realização de exercícios e simulações controladas, como testes educativos de phishing e outras ações de conscientização, pode contribuir para avaliar o grau de preparação dos policiais militares e servidores diante de tentativas de manipulação. O objetivo, nesse caso, não deve ser a punição individual, mas a identificação de vulnerabilidades e a adoção de medidas corretivas.

Essa perspectiva permite transformar situações simuladas em oportunidades de aprendizagem, fortalecendo a cultura organizacional de segurança e reduzindo a possibilidade de que informações institucionais sejam comprometidas por comportamentos decorrentes de desconhecimento ou falta de treinamento.

Uma terceira possibilidade consiste na análise do *modus operandi* empregado por criminosos. O conhecimento sobre as técnicas de manipulação utilizadas em golpes e fraudes pode fornecer subsídios para a atividade de inteligência policial, especialmente na identificação de padrões, tendências e comportamentos recorrentes. A análise sistemática dessas estratégias permite compreender como determinados grupos criminosos selecionam suas vítimas, estabelecem contato, constroem relações de confiança e conduzem a vítima até a concretização da fraude. A transformação desse conhecimento em informação de inteligência pode subsidiar

alertas preventivos, orientar ações policiais e contribuir para o planejamento de estratégias de prevenção.

A quarta aplicação está relacionada ao apoio às ações de polícia comunitária. A disseminação de informações preventivas em escolas, associações comunitárias, espaços públicos e meios de comunicação constitui importante mecanismo de aproximação entre a PMPA e a sociedade. Ao orientar os cidadãos sobre os principais sinais de uma tentativa de engenharia social e sobre os cuidados necessários diante de solicitações suspeitas, a instituição amplia sua atuação preventiva e fortalece a participação da comunidade na proteção contra a criminalidade. Essa abordagem também contribui para consolidar uma imagem institucional associada à orientação, à prevenção e à proteção do cidadão.

Dessa forma, os resultados indicam que os conhecimentos relacionados à engenharia social podem ser empregados pela PMPA sob uma perspectiva predominantemente defensiva e preventiva. A questão central não está na utilização da manipulação como mecanismo de atuação policial, mas na compreensão de como ela é empregada por criminosos para, a partir desse conhecimento, desenvolver mecanismos de proteção, capacitação e prevenção compatíveis com a preservação da ordem pública e com os direitos fundamentais.

Benefícios institucionais

7

Os resultados da análise também apontam benefícios relevantes tanto para as atividades-meio quanto para as atividades-fim da Polícia Militar do Pará. Nas atividades administrativas e de suporte, o conhecimento sobre engenharia social pode contribuir diretamente para a redução dos riscos relacionados ao vazamento de informações, ao comprometimento de credenciais e ao acesso indevido a sistemas institucionais. Considerando que parte significativa das atividades administrativas depende de recursos tecnológicos e do compartilhamento de informações, a dimensão humana da segurança da informação assume papel estratégico.

Nesse sentido, a adoção de ações permanentes de conscientização pode contribuir para fortalecer a segurança da informação, proteger sistemas administrativos e ampliar a cultura organizacional de segurança. A proteção dos recursos tecnológicos não depende exclusivamente de equipamentos, programas ou mecanismos de autenticação, mas também da capacidade dos usuários de reconhecer situações suspeitas e adotar comportamentos seguros. Conforme destaca Santos (2013), o fator humano constitui elemento de grande relevância nos incidentes relacionados à segurança da informação, tornando a conscientização dos usuários uma dimensão essencial da proteção institucional.

Nas atividades-fim, os benefícios estão associados principalmente à prevenção de fraudes contra os cidadãos, à produção de conhecimento para a atividade de inteligência, ao apoio ao policiamento ostensivo e ao fortalecimento da confiança social na instituição. Ao conhecer as técnicas utilizadas pelos criminosos, o policial militar pode estar mais preparado para reconhecer situações que envolvam tentativas de fraude e orientar adequadamente as vítimas ou potenciais vítimas.

A utilização desses conhecimentos também pode ampliar a capacidade preventiva da atividade de inteligência policial. Informações obtidas a partir da análise de ocorrências, denúncias, padrões de golpes e comportamentos criminosos podem ser sistematizadas e transformadas em produtos de inteligência destinados à prevenção. Dessa maneira, o conhecimento sobre engenharia social deixa de ser apenas uma questão relacionada à segurança digital e passa a integrar uma abordagem mais ampla de proteção da sociedade.

Esses benefícios estão relacionados à missão constitucional das polícias militares, especialmente no que se refere à preservação da ordem pública. A Constituição Federal estabelece, em seu artigo 144, que a segurança pública constitui dever do Estado e responsabilidade de todos, sendo exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio (BRASIL, 1988). Assim, a incorporação de conhecimentos relacionados à engenharia social pode representar uma estratégia de modernização institucional diante das transformações provocadas pela expansão da criminalidade em ambientes digitais.

Limites operacionais e constitucionais

Embora os resultados evidenciem possibilidades de aplicação da engenharia social em ações preventivas e de inteligência, a pesquisa também identificou limites operacionais, jurídicos e constitucionais que precisam ser observados pela PMPA. A utilização desses conhecimentos não pode significar a autorização para práticas indiscriminadas de manipulação, monitoramento ou obtenção de informações. Pelo contrário, qualquer iniciativa institucional deve estar submetida aos princípios que orientam a Administração Pública e à legislação vigente.

O primeiro limite é o da legalidade. A atuação policial deve ocorrer dentro dos limites estabelecidos pelo ordenamento jurídico. Técnicas destinadas à obtenção de informações mediante fraude, indução ilícita ou violação de direitos não podem ser empregadas de maneira arbitrária. O fato de determinada técnica ser utilizada por criminosos ou possuir potencial para

produzir informações não significa que sua utilização pela instituição policial seja automaticamente legítima. A finalidade pública deve estar acompanhada de fundamento jurídico e de procedimentos adequados de controle.

Outro aspecto fundamental é o princípio da proporcionalidade. As medidas de segurança e prevenção devem ser adequadas aos riscos identificados, necessárias para alcançar a finalidade pretendida e proporcionais aos impactos que possam produzir sobre os direitos individuais. Assim, exercícios internos de conscientização, por exemplo, devem possuir objetivos previamente definidos, critérios transparentes e mecanismos que impeçam a exposição ou constrangimento desnecessário dos participantes.

A privacidade constitui igualmente um limite essencial. Informações pessoais, comunicações e dados institucionais devem receber tratamento compatível com a legislação aplicável. O monitoramento de comunicações ou o acesso a determinados dados não pode ser realizado simplesmente em razão da conveniência operacional. Quando houver necessidade de medidas sujeitas à autorização legal ou judicial, deverão ser observados os procedimentos correspondentes.

Também deve ser preservada a dignidade da pessoa humana. A utilização de técnicas de conscientização, treinamento ou simulação não deve resultar em práticas humilhantes, discriminatórias ou abusivas. A finalidade educativa deve prevalecer sobre qualquer intenção de exposição individual. Essa preocupação é especialmente importante em ambientes institucionais nos quais existe relação hierárquica, pois a aplicação inadequada de determinados exercícios pode produzir efeitos contrários aos objetivos de segurança pretendidos.

Dessa maneira, os limites identificados demonstram que a engenharia social não deve ser compreendida como instrumento indiscriminado de investigação ou coleta de informações. Seu uso institucional deve estar orientado pela prevenção, pela capacitação e pela proteção, sempre respeitando os direitos fundamentais e os parâmetros jurídicos que regulam a atividade policial.

Comparação com outros estudos

Os resultados encontrados apresentam convergência com a literatura e com as fontes analisadas sobre segurança da informação e criminalidade digital. Santos (2013) destaca a importância do fator humano nos incidentes de segurança da informação, aspecto que se mostra particularmente relevante para compreender a engenharia social. A vulnerabilidade não está

necessariamente apenas nos sistemas tecnológicos, mas também na capacidade dos indivíduos de reconhecer e resistir às estratégias de manipulação utilizadas por terceiros.

Essa compreensão também encontra correspondência em informações recentes relacionadas ao crescimento das fraudes digitais. As fontes analisadas indicam que criminosos vêm utilizando mecanismos de engenharia social associados à identidade de instituições públicas, serviços financeiros e outras organizações de confiança para aumentar a credibilidade de suas abordagens. O Ministério Público de Santa Catarina, por exemplo, discute a relação entre fraudes cibernéticas, engenharia social e novas formas de criminalidade organizada, evidenciando a necessidade de respostas institucionais compatíveis com a transformação do fenômeno criminal (MPSC, 2026).

Na mesma direção, informações divulgadas pelo Tribunal de Contas da União apontam para a existência de falhas relacionadas a golpes digitais que utilizam indevidamente a identidade de órgãos públicos, demonstrando que a confiança depositada nas instituições pode ser explorada por criminosos para aumentar a eficácia das fraudes (TCU, 2026). Esse cenário reforça a necessidade de que os órgãos públicos, incluindo as instituições de segurança, desenvolvam estratégias permanentes de prevenção e conscientização.

A contribuição específica desta pesquisa consiste em deslocar essa discussão para o contexto da Polícia Militar do Pará, relacionando a engenharia social não apenas à segurança da informação, mas também à inteligência policial e à prevenção criminal. A partir dessa perspectiva, propõe-se que a PMPA desenvolva mecanismos institucionais capazes de transformar o conhecimento sobre as técnicas de manipulação utilizadas por criminosos em ações de capacitação, produção de conhecimento e prevenção.

Portanto, a principal contribuição do estudo está na proposição de uma abordagem integrada, na qual a segurança da informação, a inteligência policial, a polícia comunitária e a educação preventiva atuem de maneira complementar. Essa integração pode ampliar a capacidade institucional de antecipar riscos e reduzir vulnerabilidades, sem ultrapassar os limites impostos pelo ordenamento jurídico.

Proposta de modelo institucional para a PMPA

Com base nos resultados obtidos, propõe-se a criação de um Programa Permanente de Prevenção à Engenharia Social da Polícia Militar do Pará, destinado a integrar ações de capacitação, segurança da informação, inteligência e prevenção comunitária. A proposta parte da compreensão de que a vulnerabilidade humana não pode ser enfrentada por ações isoladas ou

exclusivamente tecnológicas, sendo necessária uma política institucional contínua de conscientização e prevenção.

O primeiro eixo do programa seria a capacitação anual obrigatória de policiais militares e servidores que atuam nas atividades administrativas e operacionais. A capacitação deveria abordar os principais mecanismos utilizados em golpes e tentativas de manipulação, incluindo reconhecimento de mensagens fraudulentas, proteção de credenciais, cuidados com informações institucionais e procedimentos de comunicação de incidentes. A formação contínua permitiria atualizar os conhecimentos dos integrantes da corporação diante da rápida transformação das estratégias criminosas.

O segundo eixo seria constituído por simulações controladas de phishing e outras situações de engenharia social, realizadas exclusivamente para fins educativos e de avaliação institucional. Essas atividades deveriam ser previamente regulamentadas, possuir finalidade claramente definida e evitar qualquer forma de exposição ou punição individual. Os resultados poderiam ser utilizados para identificar necessidades de treinamento e aperfeiçoar os mecanismos de segurança existentes.

O terceiro eixo envolveria a elaboração de um protocolo institucional de resposta a incidentes relacionados à engenharia social. Esse protocolo deveria estabelecer procedimentos para identificação, comunicação, registro, contenção e análise de ocorrências envolvendo tentativas de obtenção indevida de informações. A existência de fluxos previamente definidos poderia reduzir o tempo de resposta e facilitar a produção de conhecimento sobre os incidentes.

O quarto eixo corresponderia ao desenvolvimento de campanhas educativas destinadas à comunidade. A PMPA poderia utilizar suas ações de polícia comunitária, redes institucionais, palestras, escolas e outros espaços de aproximação social para orientar a população sobre os principais mecanismos utilizados em golpes digitais. A prevenção seria fortalecida pela divulgação de informações simples e práticas, especialmente sobre falsas mensagens, solicitações de transferências, perfis fraudulentos e uso indevido da identidade de instituições públicas.

Por fim, o quinto eixo seria baseado na integração com órgãos de inteligência e estruturas de segurança cibernética. A troca de informações entre instituições pode contribuir para a identificação de padrões, tendências e novas modalidades de fraude. A atuação integrada também pode favorecer a elaboração de alertas preventivos e o aperfeiçoamento das respostas institucionais diante de ameaças que ultrapassam os limites de uma única organização.

A implantação de um programa dessa natureza poderia fortalecer a resiliência institucional da PMPA e ampliar sua capacidade de prevenção diante da evolução da criminalidade digital. Mais do que incorporar uma nova técnica ao repertório policial, a proposta representa uma mudança de perspectiva: compreender a engenharia social como fenômeno criminal, identificar suas vulnerabilidades e utilizar esse conhecimento de maneira ética, legal e preventiva para proteger tanto os integrantes da instituição quanto a sociedade paraense.

Em síntese, os resultados demonstram que a engenharia social pode constituir importante campo de conhecimento para a Polícia Militar do Pará, desde que sua utilização seja orientada por objetivos legítimos de prevenção, capacitação, inteligência e proteção institucional. A adoção de medidas permanentes e integradas pode contribuir para fortalecer as atividades-meio e atividades-fim da corporação, aproximando a atuação policial das novas demandas impostas pela transformação tecnológica da criminalidade.

6 CONCLUSÃO

O estudo demonstrou que a engenharia social constitui fenômeno central da criminalidade digital contemporânea e representa desafio relevante para a segurança pública brasileira. No contexto da Polícia Militar do Pará, verificou-se que técnicas associadas à engenharia social podem ser utilizadas legitimamente em ações preventivas, educativas e de proteção institucional, contribuindo para a produção de conhecimento de inteligência e para a redução da vitimização da população.

Os resultados evidenciaram que o emprego defensivo da engenharia social fortalece tanto as atividades-meio quanto as atividades-fim da PMPA, especialmente no campo da segurança da informação, prevenção de fraudes e polícia comunitária. Entretanto, a pesquisa também demonstrou que seu uso operacional encontra limites constitucionais claros relacionados à legalidade, proporcionalidade, privacidade e dignidade da pessoa humana.

Conclui-se que a PMPA deve adotar abordagem predominantemente preventiva e institucional, evitando práticas invasivas ou enganosas incompatíveis com o Estado Democrático de Direito. Recomenda-se a implementação de políticas permanentes de conscientização, treinamento e gestão de riscos humanos, bem como a elaboração de protocolos normativos específicos para atividades de inteligência relacionadas à segurança digital.

Do ponto de vista teórico, o artigo contribui para o debate sobre inteligência policial e segurança da informação no âmbito das polícias militares brasileiras. Do ponto de vista prático,

oferece diretrizes aplicáveis à realidade da PMPA, fortalecendo sua missão constitucional de polícia ostensiva e preservação da ordem pública em ambiente cada vez mais digitalizado.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília: Senado Federal, 1988.

CLUBE FM 93.5. Polícia Militar alerta para crescimento de golpes via Pix e uso de engenharia social. Disponível em: <https://share.google/tl6Uwaw3ExrnTr7sH>. Acesso em: 18 jun. 2026.

INFOGRÁFICO ROSEMBERG. Infográfico sobre engenharia social e golpes digitais. Disponível em: <https://share.google/NiMRj6Fvf5XEndkwJ>. Acesso em: 18 jun. 2026.

INFOMONEY. A cada 13 minutos surgiu um novo risco digital no Brasil em 2026, mostra Serasa. Disponível em: <https://www.infomoney.com.br/minhas-financas/a-cada-13-minutos-surgiu-um-novo-risco-digital-no-brasil-em-2026-mostra-serasa/>. Acesso em: 18 jun. 2026.

ITAÚNA ALERTA. Golpes via Pix crescem e Polícia Militar reforça alerta à população. Disponível em: https://www.instagram.com/reel/DXEW_wEOymE/. Acesso em: 18 jun. 2026.

MPSC – MINISTÉRIO PÚBLICO DE SANTA CATARINA. Fraudes cibernéticas e engenharia social: a resposta do Ministério Público à nova criminalidade organizada. Disponível em: <https://www.mpsc.mp.br/w/artigo/fraudes-cibern%C3%A9ticas-e-engenharia-social-a-resposta-do-minist%C3%A9rio-p%C3%BAblico-%C3%Ao-nova-criminalidade-organizada>. Acesso em: 18 jun. 2026.

PRAIA GRANDE. 45º BPM. Atenção Golpe do Pix. Disponível em: <https://www.instagram.com/reel/DXOyRYKjbQ2/>. Acesso em: 18 jun. 2026.

SANTOS, Jorge Fabricio. Engenharia Social: o fator humano no incidente de segurança da informação. 2013. Monografia (Especialização em Gestão da Segurança da Informação) – Universidade do Sul de Santa Catarina, Tubarão, 2013. Disponível em: https://www.researchgate.net/publication/387098915_ENGENHARIA_SOCIAL_O_fator_humano_no_incidente_de_Seguranca_da_Informacao. Acesso em: 28 jul. 2026.

TCU – TRIBUNAL DE CONTAS DA UNIÃO. TCU identifica falhas no combate a golpes digitais que usam identidade de órgãos públicos. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-identifica-falhas-no-combate-a-golpes-digitais-que-usam-identidade-de-orgaos-publicos>. Acesso em: 18 jun. 2026.

TJPA – TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ. Cartilhas interativas de prevenção à engenharia social – Engenharia Social. Disponível em: <https://share.google/mdWdKi8NOhXGZKAih>. Acesso em: 18 jun. 2026.

VIVA.COM.BR. E-commerce sofreu mais 368 mil tentativas de fraude no 1º trimestre. Disponível em: <https://viva.com.br/tecnologia/e-commerce-sofreu-mais-368-mil-tentativas-de-fraude-no-1-trimestre.html>. Acesso em: 18 jun. 2026.

FUNCHAL, Alexandre. Engenharia Social: o maior perigo dos golpes digitais em 2025/2026. Disponível em: <https://pt.linkedin.com/pulse/engenharia-social-o-maior-perigo-dos-golpes-digitais-em-funchal-79b6f>. Acesso em: 18 jun. 2026.