DA PERSUASÃO À INDUÇÃO AO ERRO: FALSAS CENTRAIS DE ATENDIMENTO COMO TÉCNICA DE EXECUÇÃO DO ESTELIONATO DIGITAL

Cynthia Karen Martins Mariano, Tarcísio Liberato de Souza Júnior.

Universidade do Vale do Paraíba/Instituto de Pesquisa e Desenvolvimento, Avenida Shishima Hifumi, 2911, Urbanova - 12244-000 - São José dos Campos-SP, Brasil, cynthiamartins773@gmail.com, tarcisio@univap.br.

Resumo

A pesquisa analisa o golpe da falsa central de atendimento como técnica de execução do crime de estelionato digital, com enfoque na manipulação psicológica empregada para induzir a vítima em erro e possibilitar a obtenção de vantagem ilícita. O objetivo é verificar se a participação da vítima induzida a erro por falsa central de atendimento afasta a responsabilidade civil das instituições financeiras, a partir de decisões recentes do STJ, e identificar os princípios de persuasão empregados na fraude. Para tanto, foi realizada revisão de literatura, com análise de artigos científicos, doutrina, legislação e jurisprudência do Superior Tribunal de Justiça relacionadas ao tema. Os resultados indicam que a fraude explora, de forma articulada, princípios de persuasão como autoridade, urgência e prova social, o que explica por que também são vitimadas pessoas com familiaridade tecnológica e sem histórico de descuido financeiro. A distinção entre vulnerabilidade situacional e hipossuficiência do consumidor mostrou-se central para a análise, assim como a constatação de que a jurisprudência do Superior Tribunal de Justiça não adota critério automático de responsabilização, exigindo o exame das circunstâncias concretas de cada fraude e dos mecanismos de segurança disponibilizados pelas instituições financeiras. Conclui-se que a engenharia social constitui relevante instrumento de execução do estelionato contemporâneo, exigindo abordagem conjunta entre a educação digital dos usuários e o aprimoramento dos sistemas de prevenção, monitoramento e resposta a fraudes pelas instituições financeiras.
Palavras-chave: Engenharia social. Estelionato digital. Falsa central de atendimento. Persuasão psicológica. Responsabilidade civil das instituições financeiras.

Área do Conhecimento: Ciências Jurídicas – Direito Público.

Introdução

A expansão das tecnologias digitais e a crescente utilização de serviços bancários eletrônicos, aplicativos de mensagens e centrais de relacionamento remotas modificaram significativamente a forma como instituições financeiras se comunicam com seus clientes, e, na mesma medida, os mecanismos empregados pelos criminosos para a prática de fraudes. Nesse contexto, ganha destaque o chamado golpe da falsa central de atendimento, modalidade de engenharia social na qual o agente se apresenta à vítima como funcionário legítimo de uma instituição financeira, frequentemente já de posse de dados pessoais previamente obtidos, a fim de induzi-la a fornecer senhas, códigos de acesso ou a autorizar transações. Trata-se de fraude que não depende da exploração de falhas técnicas em sistemas, mas da manipulação psicológica do comportamento humano.

Do ponto de vista da psicologia da persuasão, esse tipo de golpe explora princípios relativamente estáveis do comportamento humano diante de figuras de autoridade e de situações de urgência. Isso porque a literatura sobre influência social indica que a confiança do indivíduo tende a aumentar diante de figuras investidas de autoridade e de sujeitos com quem mantém alguma relação de identificação ou cooperação (CIALDINI, 2012), circunstância que os fraudadores exploram deliberadamente ao simular, com verossimilhança, o contato de um funcionário bancário genuíno. O Superior Tribunal de Justiça já reconheceu expressamente essa dinâmica, ao afirmar que os agentes desse tipo de fraude costumam conhecer previamente os dados pessoais das vítimas e, com base neles, usam técnicas psicológicas de persuasão, a exemplo da simulação de um atendimento bancário verdadeiro, como forma de atingir seu objetivo ilícito (STJ, 2025).

No âmbito jurídico-penal, essa dinâmica caracteriza o crime de estelionato, tipificado no art. 171 do Código Penal, que pune a conduta de obter vantagem ilícita, em prejuízo alheio, mediante indução ou manutenção da vítima em erro, por meio de artifício, ardil ou qualquer outro meio fraudulento (BRASIL, 1940). Diante da sofisticação crescente das fraudes praticadas por meio eletrônico, a Lei nº 14.155/2021 alterou o art. 171 do Código Penal para acrescentar os §§ 2º-A e 2º-B, prevendo pena de reclusão de 4 a 8 anos e multa quando a fraude for cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, com causa de aumento de pena quando praticada mediante servidor mantido fora do território nacional (BRASIL, 2021). Essa alteração legislativa evidencia o reconhecimento, pelo próprio legislador, da gravidade específica da indução a erro por meios remotos, como ocorre nos golpes de falsa central.

O golpe da falsa central de atendimento apresenta, contudo, uma peculiaridade que ultrapassa a esfera penal. Como a vítima, iludida, frequentemente autoriza a operação por conta própria, discute-se em que medida essa participação afasta a responsabilidade civil das instituições financeiras. O STJ reconhece, com base na Súmula 479 (STJ, 2012) e no Tema Repetitivo 466 (STJ, [s.d.]), a responsabilidade objetiva dos bancos por fortuito interno, e desenvolveu a Teoria do Risco Concorrente, segundo a qual a culpa concorrente da vítima só se reconhece quando ela poderia inferir que sua conduta agravaria o risco do dano. Ao mesmo tempo, a Corte afirma que a responsabilidade não é automática e exige falha na prestação do serviço, como a não identificação de transações incompatíveis com o perfil do cliente

Esse quadro revela que a responsabilização não decorre de um critério automático, mas exige a análise cuidadosa das circunstâncias em que a autorização da vítima foi obtida, do grau de sofisticação da manipulação psicológica empregada e da atuação, ou omissão, das instituições financeiras em seus deveres de vigilância e segurança. Diante disso, parte-se da hipótese de que a participação ativa da vítima, induzida ao erro por técnicas de persuasão típicas do golpe da falsa central de atendimento, não é suficiente, por si só, para afastar a responsabilidade das instituições financeiras. Para testá-la, o objetivo geral é verificar se essa participação afasta a responsabilidade civil das instituições financeiras, a partir da jurisprudência recente do Superior Tribunal de Justiça (2025 e 2026). Especificamente, busca-se, em primeiro lugar, descrever o funcionamento do golpe como técnica de execução do estelionato digital, com base nos princípios de persuasão de Cialdini (2012); em segundo lugar, identificar, por meio da análise comparada de duas decisões do STJ, o critério que leva a reconhecer ou afastar a falha na prestação do serviço bancário.

Para fins deste estudo, a responsabilidade das instituições financeiras delimita-se à responsabilidade civil objetiva da instituição em que a vítima mantém a conta, por falha na prestação do serviço de segurança (art. 14 do CDC e Súmula 479 do STJ), nos casos de falsa central em que a própria vítima autoriza as operações, excluindo-se a responsabilidade penal, a da instituição que recebe os valores e a decorrente de outras modalidades de fraude.

Metodologia

A pesquisa é de natureza qualitativa e exploratória, desenvolvida por meio de revisão de literatura e abordagem jurídico-doutrinária, contemplando artigos científicos, doutrina, legislação, jurisprudência e documentos institucionais relacionados à engenharia social, ao estelionato, às fraudes eletrônicas, à manipulação psicológica, ao golpe da falsa central de atendimento e à responsabilidade das instituições financeiras. A seleção das fontes foi realizada em bases acadêmicas como SciELO e Google Acadêmico, em repositórios institucionais e em portais oficiais, utilizando os descritores engenharia social, estelionato, fraude eletrônica, falsa central de atendimento, manipulação psicológica e responsabilidade das instituições financeiras, priorizando-se publicações relevantes e atualizadas. Foram também consultadas decisões recentes do Superior Tribunal de Justiça sobre o tema, especialmente as que discutem a aplicação da Súmula 479, do Tema Repetitivo 466 e da Teoria do Risco Concorrente, as duas decisões analisadas foram selecionadas por serem da Terceira Turma, tratarem do mesmo tipo de fraude, a falsa central de atendimento, e terem chegado a resultados opostos, o que permite identificar o critério que distingue os casos.

O tratamento das fontes foi realizado de forma crítica, comparativa e interpretativa, relacionando os conceitos da literatura sobre persuasão e manipulação psicológica aos aspectos jurídico-penais

do estelionato, especialmente ao art. 171 do Código Penal e às alterações da Lei nº 14.155/2021. A jurisprudência foi examinada considerando a manipulação da vítima, sua participação nas operações e os mecanismos de segurança adotados pelas instituições financeiras, com base no art. 14 do Código de Defesa do Consumidor (BRASIL, 1990) e nos arts. 927, 931 e 932 do Código Civil, permitindo discutir a engenharia social como mecanismo de execução do estelionato digital e os desafios relacionados à prevenção e à responsabilização no ambiente digital.

Resultados

A revisão das fontes selecionadas identificou a vulnerabilidade humana como elemento recorrente nas práticas de engenharia social. Pesquisa desenvolvida com estudantes dos cursos técnicos integrados ao Ensino Médio do Instituto Federal da Paraíba constatou expressiva vulnerabilidade dos discentes diante dessas práticas, evidenciando a manipulação de pessoas como via preferencial para a obtenção de informações e bens (VIANA; ALVES; LIMA, 2022). O estudo relaciona a engenharia social à persuasão e à exploração do comportamento humano, reforçando sua relevância no campo da segurança da informação.

No campo específico do phishing, estudo sobre sua relação com a engenharia social e com o estelionato digital examinou o tratamento jurídico conferido à prática no ordenamento brasileiro e problematizou a necessidade de uma criminalização específica (FORNASIER; KNEBEL; SILVA, 2020). A conclusão aponta que medidas extrapenais podem ser mais adequadas à prevenção desses ataques, com destaque para a educação informacional, as políticas corporativas de proteção de dados e a adoção de mecanismos de segurança pelas próprias empresas de tecnologia. Na mesma direção, ao relacionar engenharia social e Big Data, constatou-se a utilização de informações coletadas para manipular usuários, o que reforça a necessidade de proteção dos indivíduos no ambiente digital (PENÊDO, 2018). Embora tratem de outras modalidades, esses achados sustentam a análise do golpe da falsa central, que se vale da mesma lógica de manipulação do comportamento humano.

No âmbito jurisprudencial, a Terceira Turma do STJ decidiu casos de falsa central de atendimento com resultados opostos. Em outubro de 2025, reconheceu a responsabilidade de instituições financeiras e de pagamento quando falhas na proteção de dados ou na identificação de transações suspeitas contribuíram para a fraude, em caso no qual foram realizadas 14 operações em um único dia, em valores incompatíveis com o padrão de movimentação do consumidor (STJ, 2025). Em 2026, no REsp 2.209.868/SP, afastou a responsabilidade do banco por não identificar falha na prestação do serviço (STJ, 2026). Em ambos os julgados, o ponto central foi a compatibilidade, ou não, das operações com o perfil do cliente, o que é analisado comparativamente na discussão.

Além disso, a análise da engenharia social mostra que a vulnerabilidade explorada não depende do conhecimento tecnológico da vítima. O uso de logotipos, nomes de instituições, dados pessoais obtidos previamente e linguagem semelhante à bancária cria uma aparência de autenticidade, de modo que a eficácia da fraude está na capacidade de construir uma situação convincente o bastante para interferir na decisão. Isso reforça o elemento "erro" do art. 171: a vítima não favorece conscientemente o criminoso, pois sua percepção da realidade foi alterada pela fraude (BRASIL, 1940).

Discussão

O golpe da falsa central de atendimento segue uma sequência reconhecível. O fraudador entra em contato como suposto funcionário do banco, já de posse de dados pessoais da vítima, alega uma operação suspeita em sua conta e a conduz a fornecer códigos, liberar acesso ou realizar transferências para supostamente proteger o patrimônio. A fraude atua, assim, sobre o processo de decisão da vítima, por meio de confiança, persuasão e medo, e permite obter vantagem ilícita sem violar diretamente os mecanismos tecnológicos da instituição financeira. Isso mostra que o resultado não decorre simplesmente de comportamento descuidado do usuário, mas de uma estratégia deliberada de manipulação psicológica.

A dimensão do problema aparece na Operação Central Fantasma, da Polícia Civil de Sergipe, que desarticulou associação criminosa especializada no golpe da falsa central bancária. O grupo tinha estrutura organizada e divisão de funções semelhante à de um call center, com integrantes

responsáveis por abordar as vítimas, obter informações sigilosas e realizar as transações, e fez vítimas em dez estados e no Distrito Federal, com prejuízo estimado em R$ 1,3 milhão (SERGIPE, 2025). O caso mostra que a engenharia social pode integrar atividade criminosa planejada para explorar a confiança das vítimas, o que afasta a ideia de simples descuido individual.

Os elementos psicológicos explorados no golpe permitem identificar, de forma quase didática, princípios de persuasão estudados na literatura sobre influência social (CIALDINI, 2012). O princípio da autoridade manifesta-se quando o criminoso se apresenta como representante da instituição financeira, valendo-se da confiança que o consumidor já deposita no banco. O da urgência, associado à ideia de escassez, aparece na alegação de que uma compra suspeita está em curso e de que é preciso agir imediatamente, o que retira da vítima o tempo de verificar a informação por outros canais. O da prova social, ou consenso, é explorado quando o fraudador menciona procedimentos supostamente padronizados do banco, dando a impressão de rotina institucional reconhecível. Já o do compromisso e da coerência opera de forma cumulativa: aceito o primeiro passo solicitado, a vítima tende a manter a mesma linha de conduta nas etapas seguintes. A combinação desses gatilhos explica por que pessoas escolarizadas, com familiaridade tecnológica e sem histórico de descuido financeiro também são vitimadas com frequência.

Com base no REsp 2.209.868/SP (STJ, 2026) e na decisão de outubro de 2025 (STJ, 2025), ambos da Terceira Turma, passa-se à análise comparada, e não à mera exposição, dos critérios que levam o Tribunal a reconhecer ou afastar a responsabilidade do banco. Nos dois casos, a técnica foi a mesma: ligação de falso funcionário, uso de dados pessoais da vítima e alegação de operação suspeita na conta. Em outubro de 2025, contudo, o correntista teve 14 operações realizadas em um único dia, em padrão dissonante do seu histórico, e o STJ entendeu que a validação dessas operações revelava defeito na prestação do serviço, pois cabe às instituições manter mecanismos capazes de detectar movimentações fora do perfil do cliente, considerando fatores como valor, horário, local e intervalo entre as operações (STJ, 2025). No REsp 2.209.868/SP, por sua vez, os dois Pix eram compatíveis com o histórico da conta, e a transferência de maior valor, de R$ 28 mil, foi feita presencialmente pela vítima, sem que ela relatasse a ligação aos funcionários da agência. O tribunal de origem concluiu que a atuação dos fraudadores, somada à conduta da própria vítima, rompeu o nexo causal, e o relator afastou a aplicação automática da Súmula 479 e do Tema 466, que pressupõem fortuito interno (STJ, 2026).

Da análise desses julgados, compreendemos que a manipulação psicológica, por mais eficaz que seja, não decide a responsabilidade: o elemento decisivo é a existência de um sinal de alerta que o banco deveria ter captado, como a incompatibilidade da operação com o perfil do cliente. A segunda é que a conduta da vítima ganha peso quando não há operação atípica a ser detectada. Nesse ponto, a literatura sobre persuasão convida a um olhar crítico, pois não procurar esclarecimentos na agência é justamente o efeito que a autoridade e a urgência buscam produzir, ao retirar o tempo e a disposição para verificar a informação por outro canal (CIALDINI, 2012). Isso não invalida o entendimento do STJ, que exige prova de defeito do serviço, mas indica que a participação da vítima deve ser valorada à luz da técnica que a conduziu ao erro, e não como simples descuido.

Conclusão

Concluímos a partir dos objetivos de verificar se a participação da vítima, induzida ao erro pelo golpe da falsa central de atendimento, afasta a responsabilidade civil da instituição financeira em que ela mantém a conta, conclui-se que a hipótese foi confirmada com uma ressalva: nos casos em que a própria vítima autoriza as operações, essa participação, isoladamente, não afasta a responsabilidade do banco, mas também não a gera de forma automática.

Quanto ao primeiro objetivo específico, verificou-se que o golpe executa o estelionato ao combinar os princípios da autoridade, da urgência, da prova social e do compromisso e coerência, o que explica a autorização dada pela própria vítima sem que se possa atribuí-la a descuido. Quanto ao segundo, a análise comparada do REsp 2.209.868/SP e da decisão de outubro de 2025 mostrou que o critério decisivo é a existência de defeito na prestação do serviço, evidenciado pela não identificação de operações incompatíveis com o perfil do cliente, e não a circunstância de a vítima ter autorizado as transações.

Assim, a engenharia social explica como a vítima é levada a agir, e o dever de segurança da instituição define se haverá dever de indenizar. A educação digital dos usuários permanece importante, mas não substitui o aprimoramento contínuo dos sistemas de monitoramento das instituições financeiras.

Referências

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal.** Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 17 ago. 2026.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor.** Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 17 ago. 2026.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 **(Código Penal)**, para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 17 ago. 2026.

CIALDINI, Robert B. **As armas da persuasão: como influenciar e não se deixar influenciar.** Rio de Janeiro: Sextante, 2012.

FORNASIER, M. de O.; KNEBEL, N. M. P.; SILVA, F. V. da. **Phishing e engenharia social: entre a criminalização e a utilização de meios sociais de proteção.** Revista Meritum, Belo Horizonte, v. 15, n. 1, p. 116-129, 2020. DOI: 10.46560/meritum.v15i1.7771. Disponível em: https://revista.fumec.br/index.php/meritum/article/view/7771. Acesso em: 17 ago. 2026.

PENÊDO, J. **A fraude no campo da informação: engenharia social, Big Data e a manipulação do usuário na rede.** Bibliotecas Universitárias: pesquisas, experiências e perspectivas, Belo Horizonte, v. 4, n. 1, p. 36-45, 2018. Disponível em: https://periodicos.ufmg.br/index.php/revistarbu/article/view/3110. Acesso em: 17 ago. 2026.

SERGIPE. **Polícia Civil do Estado de Sergipe. Operação Central Fantasma: Polícia Civil desarticula associação criminosa responsável por golpes da central bancária em 10 estados.** Aracaju, 2025. Disponível em: https://policiacivil.se.gov.br/operacao-central-fantasma-policia-civil-desarticula-associacao-criminosa-responsavel-por-golpes-da-central-bancaria-em-10-estados/. Acesso em: 17 ago. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Bancos e instituições de pagamento devem indenizar clientes por falhas que viabilizam golpe da falsa central.** Brasília, DF: STJ, 2025. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2025/21102025-Bancos-e-instituicoes-de-pagamento-devem-indenizar-clientes-por-falhas-que-viabilizam-golpe-da-falsa-central.aspx. Acesso em: 17 ago. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. REsp 2.209.868/SP. **Sem transações incompatíveis com perfil de cliente, banco não responde por golpe da falsa central.** Relator: Ministro Humberto Martins. Terceira Turma. Julgado em 16 jun. 2026. Brasília, DF: STJ, 2026. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2026/15072026-Sem-transacoes-incompativeis-com-perfil-de-cliente--banco-nao-responde-por-golpe-da-falsa-central.aspx. Acesso em: 17 ago. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Súmula 479.** Brasília, DF: Superior Tribunal de Justiça, 2012. Disponível em: https://processo.stj.jus.br/SCON/sumstj/toc.jsp?sumula=479.num. Acesso em: 17 ago. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Tema Repetitivo 466.** Responsabilidade civil objetiva das instituições financeiras por danos decorrentes de fraudes e delitos praticados por terceiros no âmbito de operações bancárias (fortuito interno). Brasília, DF: STJ, [s.d.]. Disponível em: https://processo.stj.jus.br/repetitivos/temas_repetitivos/pesquisa.jsp?novaConsulta=true&tipo_pesquisa=T&cod_tema_inicial=466&cod_tema_final=466. Acesso em: 17 ago. 2026.

VIANA, J. A. L.; ALVES, A. J. C.; LIMA, P. G. S. de. **Vulnerabilidade à Engenharia Social: um estudo com alunos do Instituto Federal da Paraíba (IFPB).** Revista Principia, [S. l.], v. 59, n. 4, p. 1344-1357, 2022. DOI: 10.18265/1517-0306a2021id5834. Disponível em: https://periodicos.ifpb.edu.br/index.php/principia/article/view/5834. Acesso em: 17 ago. 2026.