# O estado de fraude e do estelionato digital no Brasil: Evolução sistêmica, tipologias emergentes e a nova arquitetura de segurança (2020-2025)

**Ryan Maragno**
Gerente do Banco do Brasil
Unidade Segurança Institucional
Gerência de Gestão Antifraude
Email: ryan@bb.com.br

**Fauzi Anderson Yamazato**
Gerente do Banco do Brasil
Unidade Segurança Institucional
Gerência de Gestão Antifraude
E-mail: fy@bb.com.br

**Artigo de Convidado**

**RESUMO:** O artigo propõe uma análise interdisciplinar sobre a evolução das fraudes digitais no Brasil, destacando o impacto das novas tecnologias, o papel da inteligência artificial, as mudanças no perfil das vítimas e as respostas institucionais recentes. A escolha do tema busca ampliar o debate acadêmico, trazendo reflexões relevantes para o Ministério Público, instituições financeiras, gestores públicos e toda a sociedade, especialmente diante dos desafios impostos pela transformação digital e pela crescente sofisticação dos crimes patrimoniais. Acreditamos que o conteúdo pode contribuir para o aprimoramento das estratégias de prevenção, educação digital e políticas públicas, fortalecendo a atuação institucional e a proteção dos cidadãos.

**PALAVRAS-CHAVE:** fraude; estelionato digital; arquitetura de segurança.

# ENGLISH

**TITLE:** The state of digital fraud and scams in Brazil: Systemic evolution, emerging typologies, and the new security architecture (2020-2025).

**ABSTRACT:** This article proposes an interdisciplinary analysis of the evolution of digital fraud in Brazil, highlighting the impact of new technologies, the role of artificial intelligence, changes in the profile of victims, and recent institutional responses. The choice of topic seeks to broaden the academic debate, bringing relevant reflections to the Public Prosecutor's Office, financial institutions, public managers, and society as a whole, especially in light of the challenges posed by digital transformation and the increasing sophistication of property crimes. We believe that the content can contribute to improving prevention strategies, digital education, and public policies, strengthening institutional action and the protection of citizens.

**KEYWORDS**: fraud; digital scam; security architecture.

# SUMÁRIO

## 1 INTRODUÇÃO: A METAMORFOSE DA CRIMINALIDADE PATRIMONIAL

A segurança pública e a integridade financeira no Brasil passaram, entre 2020 e 2025, por uma transformação radical. Não se trata apenas do aumento expressivo dos delitos, mas de uma mudança profunda na natureza da atividade criminosa. O país vivenciou uma migração estrutural da violência física, antes predominante nas estatísticas urbanas, para a violência digital — fenômeno que especialistas denominam "Cangaço Digital" ou industrialização do estelionato.

Historicamente, o Brasil concentrou esforços no combate a crimes violentos contra o patrimônio, como roubos a transeuntes, furtos de veículos e assaltos a bancos. No entanto, dados consolidados do Anuário Brasileiro de Segurança Pública e da Federação Brasileira de Bancos (Febraban) apontam uma inflexão histórica: enquanto os crimes de rua estabilizam ou caem em várias regiões, o estelionato — especialmente em sua modalidade eletrônica — cresce exponencialmente, desafiando as capacidades tradicionais de policiamento e justiça.

Em 2024, o Brasil atingiu a marca de aproximadamente quatro golpes de estelionato consumados ou tentados por


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

minuto. Esse dado vai além da estatística criminal, evidenciando a onipresença do risco digital na vida cotidiana de cidadãos e empresas. A 19ª edição do Anuário Brasileiro de Segurança Pública revelou 2,2 milhões de casos de estelionato em um único ano, crescimento de 7,8% em relação ao período anterior, consolidando uma trajetória ascendente iniciada com a digitalização forçada pela pandemia de Covid-19.

Este relatório propõe uma análise exaustiva do ecossistema de fraudes no Brasil. Investiga as causas dessa migração criminal, impulsionada pela expansão do acesso à *internet*, bancarização digital (*banking-as-a-service*), onipresença do Pix como infraestrutura de liquidação imediata, sofisticação das táticas de engenharia social e, mais recentemente, o impacto disruptivo da Inteligência Artificial Generativa e dos *deepfakes* como vetores de ataque. Examina também a resposta institucional, desde as limitações iniciais nos mecanismos de recuperação de ativos, como o Mecanismo Especial de Devolução (MED), até os investimentos massivos do setor privado em cibersegurança e as novas regulações prudenciais do Banco Central para o horizonte de 2025.


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

## 2 ANATOMIA ESTATÍSTICA DA FRAUDE: O CENÁRIO 2023-2025

A análise quantitativa dos dados disponíveis revela a gravidade sistêmica do avanço das fraudes digitais no Brasil. Não se observa apenas um aumento na frequência dos ataques, mas também uma diversificação tática dos vetores utilizados e uma capilaridade que atinge todas as camadas demográficas da sociedade.

### 2.1 Volume, frequência e regionalização dos ataques

Os registros oficiais apontam para uma saturação dos canais digitais por tentativas de fraude. O Brasil consolidou-se como um dos maiores mercados de pagamentos instantâneos do mundo e, simultaneamente, como um laboratório global de táticas de engenharia social.

A industrialização do estelionato é evidenciada pela estatística de quatro golpes por minuto em 2024, ilustrando a automação do crime. Não se trata apenas de ataques direcionados (*spear-phishing*), mas de campanhas massivas que


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

utilizam disparadores de mensagens e *bots* para capturar credenciais em escala industrial.

A análise regional revela que o crescimento do estelionato não é uniforme, mas segue padrões de digitalização e renda. Entre 2018 e 2021, estados como Rio de Janeiro, Distrito Federal, Espírito Santo, Rio Grande do Sul e Santa Catarina apresentaram aumentos vertiginosos, com crescimento médio de 201% nesses polos, triplicando o número de casos anuais em um curto período. Essa tendência se manteve e se aprofundou até 2024.

Os prejuízos financeiros sistêmicos são igualmente alarmantes. As perdas decorrentes de fraudes digitais e golpes com cartões alcançaram a cifra recorde de R$ 10,1 bilhões em 2024, segundo dados da Febraban. Esse valor representa uma drenagem de recursos da economia formal, que passam a capitalizar facções criminosas e financiar atividades ilícitas como o tráfico de drogas e armas.

## 2.2 A prevalência dos meios de pagamento e vetores

A distribuição das fraudes pelos diferentes meios de pagamento revela as preferências táticas dos fraudadores, que


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

buscam sempre o caminho de menor resistência e maior liquidez. Embora o Pix tenha capturado a atenção pública devido à sua instantaneidade, o cartão de crédito mantém uma posição estrutural no volume de tentativas, enquanto o Pix lidera em irreversibilidade da perda para o consumidor em cenários de engenharia social.

Segundo dados da Serasa Experian e Febraban, o cartão de crédito é líder em volume de tentativas e fraudes consumadas (aproximadamente 39% dos casos), com foco em *e-commerce*, *card testing* (*bin attacks*) e roubo de dados para compras não presenciais. A clonagem física diminuiu, mas o roubo de credenciais virtuais aumentou.

O Pix apresentou crescimento de 70% nas perdas financeiras, sendo utilizado principalmente em golpes de engenharia social devido à liquidez imediata. Representa cerca de 32% dos casos de fraude quando somado a boletos.

Boletos falsos permanecem como um vetor persistente e cíclico, com alta incidência em golpes contra empresas (B2B) e pagamentos de serviços, no qual golpistas interceptam comunicações e alteram o código de barras.

Empréstimos fraudulentos estão em ascensão acelerada, com uso de dados vazados e biometria facial fraudada (*injection*


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

*attacks*) para contratação de crédito consignado e antecipação de FGTS em nome de terceiros.

No financiamento de veículos, observa-se estabilidade, mas com utilização de documentos falsificados para obtenção de crédito automotivo, muitas vezes com conivência de garagens de revenda.

É importante destacar que, segundo a Serasa Experian, as tentativas de fraudes bancárias subiram 10,4% em 2024, indicando que as instituições financeiras operam sob cerco constante. Além disso, pesquisas de opinião pública indicam que metade da população brasileira relatou ter sofrido alguma tentativa ou consumação de fraude em 2024, demonstrando a extensão epidêmica do problema e a erosão da confiança no ecossistema digital.

## 3 O ECOSSISTEMA PIX: EVOLUÇÃO FINANCEIRA E VULNERABILIDADE SISTÊMICA

O Pix, sistema de pagamentos instantâneos lançado pelo Banco Central do Brasil, consolidou-se como um sucesso global em inclusão financeira, redução de custos transacionais e eficiência econômica. No entanto, sua arquitetura, baseada em


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

transações irrevogáveis, liquidez imediata e funcionamento ininterrupto, criou inadvertidamente a infraestrutura perfeita para a monetização rápida de crimes patrimoniais.

### 3.1 A explosão das fraudes e a instantaneidade

Os dados do Banco Central revelam uma correlação direta entre a velocidade do pagamento e a atratividade para o crime: as perdas com fraudes no Pix cresceram 70% em 2024. Este crescimento desproporcional, em relação ao aumento do volume total de transações, indica que as organizações criminosas aprimoraram suas técnicas para explorar as características intrínsecas do sistema.

A instantaneidade é a principal característica que beneficia o fraudador. No antigo paradigma bancário (DOC/TED), as janelas de compensação e os horários restritos permitiam que instituições financeiras e vítimas interceptassem transações suspeitas com uma margem de tempo razoável. No Pix, o dinheiro transita entre contas em segundos, exigindo que os sistemas de detecção de fraude atuem em tempo real, na ordem de milissegundos. Isso gera um desafio tecnológico


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

imenso: equilibrar a segurança, bloqueando fraudes, sem causar fricção excessiva para o usuário legítimo.

### 3.2 O Problema Estrutural das "Contas Laranja"

A espinha dorsal da fraude via Pix não é tecnológica, mas logística: a existência massiva de "contas laranja" (contas de aluguel ou abertas com documentos falsos/roubados). Organizações criminosas recrutam indivíduos para alugar suas credenciais bancárias ou utilizam dados vazados de megavazamentos para abrir milhares de contas em bancos digitais e *fintechs*, em que os processos de Know Your Customer (KYC) podem ser menos rigorosos.

Quando uma vítima realiza uma transferência Pix sob coação (sequestro relâmpago) ou engano (engenharia social), o dinheiro não permanece na primeira conta de destino. Ele é imediatamente pulverizado em dezenas de outras contas, muitas vezes em instituições diferentes, e frequentemente convertido em criptoativos ou sacado em espécie, tornando o rastreamento manual impossível e o bloqueio de valores ineficaz sob as regras atuais.


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

### 3.3 O Fracasso do Mecanismo Especial de Devolução (MED 1.0)

Para combater as fraudes no Pix, o Banco Central instituiu o Mecanismo Especial de Devolução (MED), que, em teoria, permite à vítima ou ao banco solicitante bloquear cautelarmente e repatriar recursos provenientes de fraudes ou falhas operacionais, sem a necessidade de autorização do titular da conta recebedora. O prazo regulamentar para acionamento é de até 80 dias após a transação. No entanto, a eficácia prática do MED 1.0 tem se mostrado estatisticamente irrelevante para a maioria das vítimas, já que apenas cerca de 8% dos valores contestados são efetivamente recuperados e devolvidos.

Essa baixa efetividade decorre de limitações estruturais do mecanismo. O MED atua principalmente na chamada "primeira camada", ou seja, na conta que recebeu o dinheiro diretamente da vítima. Caso o fraudador utilize automação para transferir o valor para uma segunda conta poucos segundos após o recebimento, o MED perde sua eficácia, pois não possui autoridade automática para rastrear o dinheiro em camadas subsequentes. Além disso, o tempo de resposta entre a notificação da fraude, a análise pelo banco pagador, a


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

comunicação com o banco recebedor e o efetivo bloqueio costuma ser superior ao tempo necessário para o criminoso esvaziar a conta, tornando o processo ineficaz na maioria dos casos.

Outro fator que contribui para a ineficiência do MED é a subjetividade envolvida na identificação de "fundada suspeita de fraude". Muitas vezes, essa avaliação depende da interpretação humana ou algorítmica das instituições recebedoras, o que gera inconsistências na aceitação dos pedidos e disputas entre bancos. Assim, o MED 1.0, apesar de representar um avanço regulatório, ainda não oferece uma solução robusta para o rastreamento e recuperação de valores em fraudes digitais, especialmente diante da velocidade e sofisticação das operações criminosas.

## 4 A EVOLUÇÃO DOS GOLPES: ENGENHARIA SOCIAL E TIPOLOGIAS PREDOMINANTES

A tecnologia é, sem dúvida, um meio facilitador para a prática de fraudes, mas a vulnerabilidade explorada pelos criminosos permanece, em sua maioria, humana. A engenharia social, definida como a arte de manipular psicologicamente pessoas para que divulguem informações confidenciais ou


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

realizem ações prejudiciais, consolidou-se como o vetor de ataque mais eficiente, acessível e lucrativo para o crime organizado brasileiro.

O portfólio de golpes catalogados pela Febraban em 2024 revela uma diversidade de estratégias que exploram sentimentos básicos como medo, ganância, urgência e altruísmo. Entre as modalidades mais sofisticadas está o golpe da falsa central telefônica, em que os criminosos simulam operações bancárias legítimas para induzir a vítima a realizar transações ou instalar *softwares* de acesso remoto. O processo geralmente se inicia com uma mensagem alarmista, seguida de atendimento por uma Unidade de Resposta Audível idêntica à do banco original. O atendente, utilizando linguagem técnica impecável, constrói uma relação de confiança e induz a vítima a transferir valores para contas de terceiros, sob o pretexto de proteção ou reversão de fraude. O impacto dessa modalidade é significativo, registrando milhões de tentativas e elevadas perdas financeiras.

Outra estratégia que se destaca é o chamado golpe da "Mão Fantasma", que combina engenharia social com o uso de *malwares*. Nesse caso, o criminoso convence a vítima a instalar aplicativos de acesso remoto, como TeamViewer ou AnyDesk, sob o pretexto de suporte técnico ou atualização de cadastro.


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

Uma vez instalado o *software*, o fraudador assume o controle do dispositivo, podendo realizar transações bancárias, solicitar autenticações biométricas e manipular limites de crédito, tudo sem o conhecimento da vítima. A iliteracia digital técnica de muitos usuários contribui para o sucesso desse golpe, já que muitos não conseguem distinguir entre aplicativos legítimos e ferramentas de invasão hostil.

O golpe da tarefa, comum em aplicativos de mensageria como Telegram e WhatsApp, explora a precarização do trabalho e a necessidade econômica. A vítima é abordada com ofertas de emprego para realizar tarefas simples *online*, recebendo pagamentos iniciais via Pix. Esse mecanismo serve para criar confiança e estimular o engajamento. Em seguida, para acessar tarefas com pagamentos maiores, a vítima é induzida a realizar depósitos caução ou investimentos pré-pagos, que aumentam progressivamente. O ciclo se perpetua até que a vítima exaure seus recursos ou percebe o golpe, momento em que os criminosos desaparecem e os grupos são apagados.

Além dessas modalidades, o cenário brasileiro de fraudes digitais inclui golpes de clonagem de WhatsApp, falsas vendas em *e-commerce*, *phishing* por e-mail e SMS, falsas plataformas de investimento, troca de cartão, boletos falsos e devolução de


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

empréstimos indevidos. Cada uma dessas estratégias explora gatilhos psicológicos específicos, como urgência, oportunidade, medo, distração ou honestidade, ampliando o alcance e a eficácia das campanhas criminosas.

A análise das tipologias predominantes evidencia que, apesar da sofisticação tecnológica dos ataques, o fator humano permanece como o elo mais vulnerável da cadeia de segurança. A educação digital e o desenvolvimento de heurísticas de defesa são, portanto, elementos essenciais para mitigar o impacto das fraudes e fortalecer a resiliência da sociedade frente ao avanço do cibercrime.

## 5 A FRONTEIRA DA INTELIGÊNCIA ARTIFICIAL: DEEPFAKES, BIOMETRIA E FRAUDES SINTÉTICAS

Se a engenharia social representa o principal vetor de ataques no presente, a Inteligência Artificial (IA) desponta como a fronteira tecnológica que define o futuro imediato das fraudes digitais no Brasil. O ano de 2024 e as projeções para 2025 marcam a consolidação do uso de IA generativa por criminosos, criando o que especialistas denominam “vetores de ataque sintéticos” ou “fraude 2.0”. A popularização dessas ferramentas


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

reduziu drasticamente a barreira de entrada, permitindo que golpistas sem grande conhecimento técnico operem sistemas de alta complexidade.

Um caso paradigmático ilustra o potencial destrutivo dessa tecnologia: uma multinacional sofreu prejuízo estimado em R$ 129 milhões após um funcionário do departamento financeiro participar de uma videochamada fraudulenta. Durante a reunião, o colaborador acreditou estar dialogando com o diretor financeiro e outros executivos seniores, mas todos os participantes eram recriações digitais geradas por IA em tempo real. A sofisticação do ataque foi tamanha que os avatares utilizavam o jargão corporativo correto, discutiam projetos confidenciais e mantiveram a interação por mais de quarenta minutos. Pequenos sinais de falha visual ou dessincronização labial foram interpretados como problemas comuns de conexão, demonstrando como a tecnologia já ultrapassou a barreira da desconfiança média.

No contexto bancário, a biometria facial foi adotada massivamente como camada primária de segurança para abertura de contas e validação de transações de alto risco. Em resposta, o cibercrime desenvolveu técnicas avançadas para burlar esses sistemas, migrando dos ataques de apresentação


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

para os chamados ataques de injeção. Enquanto o método tradicional consistia em apresentar uma foto ou vídeo de alta resolução à câmera do celular, os sistemas modernos passaram a utilizar detecção de prova de vida para identificar fraudes. No entanto, os ataques de injeção representam uma ameaça mais sofisticada: o criminoso utiliza emuladores de Android ou *softwares* específicos em *smartphones* com acesso administrativo para "injetar" um fluxo de vídeo pré-gravado ou gerado por IA diretamente na API de câmera do sistema operacional. O aplicativo bancário, assim, acredita estar recebendo imagens da câmera real, quando na verdade processa um vídeo falso, capaz de simular movimentos e comandos de prova de vida. Operações policiais recentes já identificaram quadrilhas especializadas nessa modalidade, que comercializavam kits para burlar o reconhecimento facial de múltiplos bancos digitais.

As tendências críticas para 2025 apontam para o uso massivo de vozes sintéticas em golpes cibernéticos. A clonagem de voz atingiu um nível de fidelidade tal que, com apenas alguns segundos de áudio da vítima, uma IA consegue treinar um modelo capaz de reproduzir qualquer frase com o timbre, entonação e sotaque originais. Esse avanço potencializa golpes


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

como o do WhatsApp e o falso sequestro, nos quais o criminoso envia áudios desesperados com a voz exata de um familiar, aumentando drasticamente a taxa de conversão dos ataques. O áudio, para a maioria das pessoas, é um fator de autenticação de confiança, tornando esse tipo de fraude especialmente perigoso.

A incorporação da IA ao arsenal do cibercrime inaugura uma nova era de desafios para as instituições financeiras, empresas e cidadãos. O combate a essas ameaças exige não apenas o aprimoramento das tecnologias de defesa, mas também a atualização constante dos protocolos de segurança e a disseminação de práticas de educação digital, capazes de fortalecer a resiliência da sociedade diante da sofisticação crescente dos ataques sintéticos.

## 6 PERFIL DAS VÍTIMAS E PSICOLOGIA DA FRAUDE: A QUEBRA DE ESTERIÓTIPOS

A análise sociodemográfica das vítimas de estelionato digital no Brasil desafia o senso comum de que apenas idosos ou pessoas com baixo letramento digital são vulneráveis a golpes. Os dados recentes mostram uma verdadeira democratização do


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

risco, com nuances importantes entre diferentes faixas etárias e perfis sociais.

Um dos fenômenos mais surpreendentes é o aumento expressivo das fraudes digitais contra jovens da chamada geração Z, especialmente aqueles com até 25 anos. Segundo dados da Serasa Experian, esse grupo registrou um crescimento de 43% nas ocorrências apenas no primeiro semestre de 2025, superando proporcionalmente o volume de casos entre idosos. Entre os fatores que contribuem para essa vulnerabilidade juvenil estão a hiperconectividade e a exposição constante ao ambiente digital, já que os jovens realizam quase todas as suas transações por canais *online*, ampliando a superfície de risco. Além disso, o excesso de confiança típico dos nativos digitais faz com que muitos subestimem os perigos, acreditando serem imunes a golpes considerados "de velhos". Esse comportamento, aliado à propensão para clicar em *links* de promoções relâmpago, baixar aplicativos não oficiais e compartilhar senhas em redes sociais e aplicativos de mensagens, aumenta significativamente a exposição a fraudes sofisticadas.

Por outro lado, os idosos continuam sendo alvos preferenciais para golpes de engenharia social de alto valor financeiro, como o da falsa central telefônica ou do falso


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

motoboy, nos quais as economias de uma vida inteira podem ser subtraídas em questão de minutos. O impacto desses golpes vai além do prejuízo material, atingindo profundamente o psicológico das vítimas. Estudos clínicos e pesquisas acadêmicas apontam para a prevalência da chamada "Síndrome do Desamparo" entre idosos vitimados, caracterizada por sentimentos de culpa, vergonha perante a família, medo de utilizar o telefone ou o computador, irritabilidade e perda de autonomia. Muitos, após serem enganados, regridem em sua inclusão digital, abandonando ferramentas bancárias ou se tornando dependentes de terceiros para operações financeiras, o que paradoxalmente pode expô-los a novos riscos de abuso patrimonial doméstico.

Esses dados evidenciam que a vulnerabilidade à fraude digital não está restrita a um perfil específico, mas atravessa gerações e contextos sociais. A quebra de estereótipos é fundamental para o desenvolvimento de políticas públicas e estratégias de prevenção que alcancem toda a sociedade, promovendo educação digital, conscientização e suporte psicológico às vítimas. O enfrentamento do estelionato digital exige, portanto, uma abordagem multidisciplinar, capaz de


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

compreender as motivações, comportamentos e impactos das fraudes em diferentes segmentos da população brasileira.

## 7 RESPOSTA INSTITUCIONAL E O NOVO ARCABOUÇO REGULATÓRIO (2025)

Diante do cenário de calamidade pública e das perdas bilionárias causadas pelas fraudes digitais, o setor financeiro e o governo federal intensificaram suas respostas estratégicas nos anos de 2024 e 2025. O movimento foi de uma postura predominantemente reativa para a construção de uma arquitetura de segurança proativa e integrada, capaz de enfrentar os desafios impostos pela sofisticação dos ataques e pela velocidade das operações criminosas.

No âmbito privado, os bancos brasileiros realizaram investimentos massivos em tecnologia e segurança cibernética, totalizando cerca de R$ 47,4 bilhões apenas em 2024, segundo a Febraban. Esses recursos foram direcionados para o desenvolvimento de motores de risco baseados em inteligência artificial, capazes de analisar não apenas dados transacionais, mas também a biometria comportamental dos usuários. O sistema aprende padrões como a forma de digitação, o ângulo de


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

uso do celular, a velocidade do toque e os horários habituais de operação, permitindo a identificação de desvios que possam indicar fraude. Além disso, houve avanços significativos em criptografia e tokenização, protegendo dados em trânsito e em repouso, e dificultando o uso de informações vazadas por criminosos. Paralelamente, campanhas massivas de educação e conscientização foram lançadas para alertar a população sobre os *scripts* de engenharia social, buscando criar uma barreira psicológica contra a manipulação.

No campo das políticas públicas, destaca-se o lançamento e a expansão do aplicativo "Celular Seguro" pelo Ministério da Justiça e Segurança Pública. Essa ferramenta funciona como um botão de pânico federado, permitindo que o cidadão cadastre pessoas de confiança para, em caso de roubo ou furto do aparelho, acionar um alerta que bloqueia simultaneamente a linha telefônica junto à Anatel e o acesso aos aplicativos bancários das instituições parceiras. Em seus primeiros seis meses de operação, o sistema registrou mais de 57 mil alertas de bloqueio efetivos, atacando diretamente a janela de oportunidade que o criminoso possui entre o roubo físico do aparelho e a drenagem das contas bancárias. Ao reduzir essa


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

janela de horas para minutos, a ferramenta diminui o incentivo econômico ao roubo de *smartphones*.

No âmbito regulatório, o Banco Central, em parceria com o Grupo de Trabalho de Segurança do Pix, avançou no desenvolvimento do MED 2.0, com previsão de implementação escalonada a partir do final de 2025 e obrigatoriedade total em 2026. O novo mecanismo traz inovações estruturais, como a rastreabilidade em cadeia, permitindo o bloqueio de recursos em múltiplas camadas de transferências subsequentes, e o bloqueio cautelar de todas as contas vinculadas ao CPF do beneficiário identificado como fraudador, em qualquer instituição financeira. Além disso, a automação das decisões reduz a necessidade de análise humana, acelerando o tempo de resposta e diminuindo a subjetividade nos processos.

O endurecimento das regras do Pix para 2025 também merece destaque. Transferências realizadas a partir de dispositivos não cadastrados previamente pelo usuário passaram a ter limites severos de valor, dificultando que criminosos esvaziem contas a partir de aparelhos não reconhecidos. O uso ampliado do bloqueio cautelar por até 72 horas para análise de segurança, embora gere alguma fricção para o usuário legítimo,


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

tornou-se uma medida vital para a prevenção de perdas em transações atípicas.

Essas iniciativas, tanto do setor privado quanto do público, representam uma resposta coordenada e robusta ao avanço das fraudes digitais, sinalizando uma mudança de paradigma na proteção do patrimônio dos cidadãos e na preservação da confiança no sistema financeiro nacional.

## 8 PIX AUTOMÁTICO: INOVAÇÃO COM NOVOS VETORES DE RISCO

O lançamento do Pix Automático, previsto para 2025, representa mais um marco na evolução dos meios de pagamento no Brasil. A proposta é substituir o débito automático e os boletos recorrentes, trazendo maior eficiência para pagamentos de serviços essenciais, como luz, água e assinaturas de *streaming*. No entanto, essa inovação também inaugura novos vetores de risco que preocupam especialistas em segurança digital.

A funcionalidade do Pix Automático permite que o usuário autorize débitos recorrentes diretamente em sua conta, facilitando a gestão financeira e eliminando etapas burocráticas.


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

Contudo, essa praticidade pode ser explorada por criminosos em golpes de engenharia social. Um dos riscos mais discutidos é o da chamada “assinatura fantasma”, em que a vítima é induzida a autorizar um Pix Automático acreditando estar validando uma operação legítima de segurança. Caso o golpe seja bem-sucedido, o fraudador garante um fluxo de renda constante e mensal, drenando recursos da vítima até que ela perceba a fraude.

Para mitigar esses riscos, o Banco Central estabeleceu diretrizes rigorosas para o funcionamento do Pix Automático. O cancelamento da funcionalidade deve ser simplificado, imediato e acessível diretamente no aplicativo bancário, permitindo ao usuário retomar o controle de suas autorizações a qualquer momento. Além disso, os limites de segurança, como tetos diários de transações, serão compartilhados com as regras gerais do Pix, impedindo que a recorrência seja utilizada para burlar restrições e ampliar o potencial de prejuízo.

A chegada do Pix Automático reforça a necessidade de constante atualização das estratégias de prevenção e educação digital. A inovação, embora traga benefícios evidentes para a eficiência dos pagamentos, exige atenção redobrada dos usuários e das instituições financeiras para evitar que a


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

comodidade se transforme em vulnerabilidade. O equilíbrio entre praticidade e segurança será fundamental para o sucesso da nova ferramenta e para a proteção do patrimônio dos brasileiros diante das ameaças emergentes.

## 9 CONCLUSÃO E PERSPECTIVAS FUTURAS

A evolução do cenário de fraudes digitais no Brasil entre 2020 e 2025 narra uma verdadeira corrida armamentista entre a inovação financeira e o crime organizado. O país, por sua escala continental, adoção precoce de tecnologias digitais e desafios sociais, tornou-se um laboratório global tanto para novas soluções de pagamento, como o Pix, quanto para as técnicas de cibercrime que buscam explorá-las.

As evidências acumuladas ao longo dos últimos anos sugerem que a batalha contra o estelionato digital não será vencida apenas com tecnologia. Embora avanços em criptografia, biometria e inteligência artificial sejam fundamentais, o fator humano permanece como o elo mais vulnerável da cadeia de segurança. A engenharia social, ao explorar falhas do "sistema operacional humano" — como


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

medo, ganância e urgência —, continuará sendo eficaz independentemente da robustez dos sistemas tecnológicos.

Para o horizonte de 2025 a 2030, três pilares estratégicos se destacam como determinantes para a contenção do fenômeno das fraudes digitais. O primeiro é a eficácia operacional do MED 2.0, cuja capacidade de recuperar o dinheiro roubado pode desincentivar economicamente o crime. Se o roubo continuar compensando financeiramente, a indústria da fraude seguirá atraindo talentos e capital. O segundo pilar é a construção de uma identidade digital soberana e unificada, com a evolução da Carteira de Identidade Nacional e sua integração profunda com bases biométricas bancárias e governamentais, visando eliminar a proliferação de contas laranja e a falsidade ideológica na abertura de contas. Por fim, a educação digital como política de Estado se torna imprescindível, migrando a conscientização de segurança de uma "dica ocasional" para uma competência básica do cidadão, tão fundamental quanto a alfabetização ou a segurança no trânsito. A criação de uma "imunidade de rebanho" digital é essencial para reduzir a eficácia das campanhas massivas de fraude.

O chamado "Cangaço Digital" é uma realidade consolidada e estrutural. O desafio nacional agora é construir


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

defesas civis, jurídicas e tecnológicas capazes de mitigar seus danos em uma sociedade que se tornou, para o bem e para o mal, irreversivelmente conectada.

## REFERÊNCIAS

ALVES, Ana Paula Branco Alves. Pix Automático: quais cuidados devem ser tomados com a nova ferramenta?. *Forbes*, 2025. Disponível em: https://forbes.com.br/forbes-money/2025/06/pix automatico-quais-cuidados-devem-ser-tomados-com-a-nova-ferramenta/. Acesso em: 26 nov. 2025.

ARAGAKY, Caroline. Tentativas de fraudes bancárias sobem 10,4% em 2024, diz Serasa. *CNN Money*, 2025. Disponível em: https://www.cnnbrasil.com.br/economia/financas/tentativas-de-fraudes bancarias-sobem-104-em-2024-diz-serasa/. Acesso em: 26 nov. 2025.

BARRA, Helena; LEÃO, Luan. Brasil registra cerca de 4 golpes de estelionato por minuto em 2024. *CNN Brasil*, 2024. Disponível em: https://www.cnnbrasil.com.br/nacional/brasil/brasil-registra-cerca-de-4-golpes-de-estelionato-por-minuto-em-2024/. Acesso em: 26 nov. 2025.

FRAUDES bancárias bateram R$ 10 bi em 2024; 'cangaço digital', diz diretor da PF. *InfoMoney*, 2025. Disponível em:


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

https://www.infomoney.com.br/politica/fraudes-bancarias-bateram-r-10-bi-em-2024-cangaco-digital-diz-diretor-da-pf/. Acesso em: 26 nov. 2025.

GOLPES causaram prejuízo de R$ 10,1 bi em 2024, diz Febraban. *Poder 360*, 2025. Disponível em: https://www.poder360.com.br/poder-economia/golpes-causaram-prejuizo-de-r-101 bi-em-2024-diz-febraban/. Acesso em: 26 nov. 2025.

MOURA, Bruno de Freitas. Metade dos brasileiros sofreu fraude em 2024, diz Serasa Experian. *Agência Brasil*, 2025. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2025 03/metade-dos-brasileiros-sofreu-fraude-em-2024-diz-serasa-experian. Acesso em: 26 nov. 2025.

19ª EDIÇÃO do Anuário Brasileiro de Segurança Pública revela 2,2 milhões de casos de estelionato no país em 2024. *Anuário Brasileiro de Segurança Pública*, 2025. Disponível em: https://fontesegura.forumseguranca.org.br/19a-edicao-do-anuario-brasileiro-de-seguranca-publica-revela-22-milhoes-de-casos-de-estelionato-no-pais-em-2024-com-crescimento-de-78-em-relacao-ao-ano-anterior/. Acesso em: 26 nov. 2025.

PERDAS com fraudes no Pix crescem 70% em 2024, mostram dados do BC. *CNN Brasil*, 2025. Disponível em: https://www.cnnbrasil.com.br/economia/financas/perdas-com-fraudes no-pix-crescem-70-em-2024-mostram-dados-do-bc/. Acesso em: 26 nov. 2025.


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551

REDA, Paulo. Instituições financeiras investem R$ 47,4 bilhões em segurança cibernética. *Estadão*, 2024. Disponível em: https://www.estadao.com.br/economia/negocios/instituicoes f inanceiras-investem-r-474-bilhoes-em-seguranca-cibernetica/. Acesso em: 26 nov. 2025.

ROUBO e furto de celulares caem no Brasil, mas estelionato dispara, chegando a 4 casos por minuto. *Exame*, 2025. Disponível em: https://exame.com/brasil/roubo-e-furto-de-celulares-caem-no-brasil-mas-estelionato-dispara-chegando-a-4-casos-por-minuto/. Acesso em: 26 nov. 2025.

SANTOS, Thiago do Amaral. MED 2.0: Como a nova Resolução reforça a segurança do Pix. *Okai*, 2025. Disponível em: https://okai.com.br/blog/med-20-como-a-nova-resolucao-reforca-a-seguranca-do-pix. Acesso em: 26 nov. 2025.


Revista do Ministério Público Militar, a. 53, n. 50, Brasília, 1º sem. 2026, pp. 13-42, CC BY 4.0, DOI: https://zenodo.org/records/18175551