

GOLPES VIRTUAIS: O ANONIMATO E A ANÁLISE DOS DESAFIOS DA INVESTIGAÇÃO PENAL.

**ONLINE SCAMS: ANONYMITY AND AN ANALYSIS OF THE CHALLENGES
FOR CRIMINAL INVESTIGATION.**

Ciências Sociais Aplicadas • 27/10/2026

REGISTRO DOI: [10.70773/revistatopicos/792992685](https://doi.org/10.70773/revistatopicos/792992685)

Luis Felipe Gomes Pereira¹

Maila Rocha Feitosa Herênio²

RESUMO

A expansão das tecnologias digitais e a utilização do Pix modificaram a forma de realização de pagamentos e transferências, mas também passaram a integrar diferentes modalidades de golpes virtuais. Nesse contexto, a investigação penal enfrenta dificuldades para identificar os responsáveis pelas fraudes, especialmente diante da utilização de diferentes contas, recursos digitais e mecanismos destinados à movimentação dos valores. O presente artigo analisa os desafios enfrentados pela investigação penal brasileira na identificação da autoria de golpes praticados via Pix, considerando as barreiras ao rastreamento digital e a utilização das chamadas “contas-laranja”. A pesquisa possui abordagem qualitativa, natureza aplicada e caráter exploratório e descritivo, desenvolvida por meio de pesquisa bibliográfica e documental, com utilização do método dedutivo. A análise realizada demonstra que a identificação de uma conta, de uma chave Pix ou de outro registro digital não é suficiente, isoladamente, para determinar a autoria da fraude. Verificou-se que a movimentação dos valores entre diferentes contas e instituições pode dificultar a reconstrução do percurso financeiro e o avanço da investigação. Nesse cenário, o rastreamento do fluxo financeiro, a análise das evidências digitais e o compartilhamento de informações entre instituições financeiras e autoridades constituem elementos relevantes para ampliar a apuração. Conclui-se que a investigação dos golpes via Pix não deve se limitar à identificação da primeira conta relacionada à fraude, sendo necessário a análise conjuntamente com os elementos digitais e financeiros disponíveis para possibilitar o avanço da apuração dos possíveis envolvidos.

Palavras-chave: Contas-laranja; Golpes virtuais; Pix.

ABSTRACT

The expansion of digital technologies and the use of Pix have

transformed the way payments and transfers are made but have also given rise to various forms of online fraud. In this context, criminal investigations face difficulties in identifying those responsible for fraud, particularly given the use of multiple accounts, digital tools and mechanisms designed to move funds. This article analyses the challenges faced by Brazilian criminal investigations in identifying the perpetrators of scams carried out via Pix, considering the barriers to digital tracing and the use of so-called “straw-man accounts”. The research adopts a qualitative approach; it is applied in nature and exploratory and descriptive in character, and was conducted through bibliographic and documentary research, using the deductive method. The analysis carried out demonstrates that the identification of an account, a Pix key or another digital record is not, on its own, sufficient to determine the perpetrator of the fraud. It was found that the movement of funds between different accounts and institutions can hinder the reconstruction of the financial trail and the progress of the investigation. In this context, the tracing of financial flows, the analysis of digital evidence and the sharing of information between financial institutions and the authorities are key elements in expanding the investigation. It can be concluded that investigations into Pix-based scams should not be limited to identifying the first account linked to fraud; rather, it is necessary to analyze the available digital and financial evidence in conjunction to enable the investigation into those potentially involved to progress.

Keywords: Online scams; Pix Straw-man accounts.

1. INTRODUÇÃO

A expansão das tecnologias digitais e a utilização de meios eletrônicos modificaram a realização de pagamentos e

transferências no cenário atual, destacando-se o Pix pela rapidez e praticidade nas operações financeiras. Ao mesmo tempo, o ambiente digital passou a ser amplamente utilizado para a prática de fraudes e golpes virtuais, impondo novos desafios à investigação penal, especialmente no tocante ao rastreamento e à apuração de informações digitais e financeiras.

O estelionato no ordenamento jurídico brasileiro está previsto no art. 171 do Código Penal. Doutrinadores como Capez (2020) e Andreucci (2014) conceituam a conduta pela obtenção de vantagem ilícita mediante indução ou manutenção da vítima em erro. Com o avanço tecnológico e alterações legislativas como as Leis nº 14.155/2021 e nº 15.397/2026, tipificou-se a fraude eletrônica e a conduta de cessão de conta bancária ("conta-laranja").

Gonçalves e Henriques (2023) destacam o crescimento do estelionato virtual impulsionado pelo uso intensivo da internet, enquanto Moreira, Martins e Mantovani (2024), Cunha (2026) e Melo (2026) abordam o papel das "contas-laranja" e da utilização fraudulenta de dados de terceiros para ocultar a autoria dos golpes.

Sob a ótica da prova digital, Saad, Rossi e Partata (2024) e Badaró (2021) apontam características essenciais desses elementos, tais como a imaterialidade, volatilidade e a necessidade de métodos forenses próprios para sua conservação e análise. Embora as transações via Pix deixem registros e contem com mecanismos de acompanhamento, como o rastreamento do Banco Central e o Mecanismo Especial de Devolução (MED), a simples identificação de uma chave Pix, de um registro digital ou da titularidade de uma conta receptora não é suficiente para determinar quem efetivamente planejou ou executou a fraude.

A rápida pulverização dos valores em sucessivas contas de diferentes instituições e a conversão de recursos criam barreiras ao rastreamento digital. Assim, o problema de pesquisa consiste em verificar de que forma as barreiras no rastreamento digital dificultam o avanço da investigação penal para além das chamadas “contas-laranja”, na identificação dos possíveis mandantes de golpes praticados via Pix.

A relevância e importância deste trabalho fundamentam-se na necessidade de compreender que a apuração penal não deve se limitar à simples localização da primeira conta vinculada à fraude. Como a titularidade formal de uma conta não comprova por si só a participação consciente do indivíduo no delito, faz-se indispensável analisar o fluxo financeiro e as evidências digitais de forma integrada. A pesquisa contribui para a ciência jurídica e para a sociedade ao discutir as possibilidades e os limites da atuação das autoridades e instituições financeiras no aprimoramento das investigações de fraudes em meios de pagamento instantâneos.

Diante desse cenário, o objetivo geral do presente artigo é a análise dos desafios enfrentados pela investigação penal brasileira na identificação da autoria de golpes praticados via Pix, considerando as barreiras ao rastreamento digital e a utilização das “contas-laranja”.

Como objetivos específicos, busca-se a compreensão da dinâmica dos golpes virtuais, do estelionato eletrônico e do funcionamento do Pix na prática delitiva, identificação da natureza jurídica e o papel das “contas-laranja” e do anonimato na dispersão de recursos e na ocultação de dados, o exame das particularidades da prova digital e os instrumentos de rastreamento e cruzamento de dados digitais e

financeiros, e por fim, a discussão dos limites e das possibilidades de aprimoramento da investigação penal para avançar das contas receptoras iniciais até a identificação dos reais mandantes.

2. GOLPES VIRTUAIS E A UTILIZAÇÃO DO PIX NA PRÁTICA DELITIVA

A expansão das tecnologias digitais modificou as formas de comunicação, de circulação de informações e de realização de operações financeiras. Ao mesmo tempo em que esses recursos proporcionaram maior rapidez às relações sociais e econômicas, também passaram a integrar diferentes formas de prática delitiva. Nesse contexto, os chamados golpes virtuais podem envolver a utilização de recursos tecnológicos para induzir vítimas em erro e obter vantagem ilícita.

No ordenamento jurídico brasileiro, o estelionato está previsto no art. 171 do Código Penal. O dispositivo estabelece a obtenção de vantagem ilícita, em prejuízo alheio, mediante indução ou manutenção de alguém em erro por meio fraudulento (BRASIL, 1940). A legislação também prevê modalidade específica de fraude eletrônica, relacionada à utilização de recursos tecnológicos na prática da conduta.

Nesse sentido, segundo Capez, o crime de estelionato caracteriza-se pela utilização de meios fraudulentos, em que o agente engana a vítima ou a mantém em erro, fazendo com que ela tenha uma percepção equivocada da realidade, sem o uso de violência ou grave ameaça (Capez, 2020, p. 842).

No mesmo contexto, Andreucci explica que o estelionato ocorre quando o agente utiliza meios enganosos para induzir ou manter a

vítima em erro com a finalidade de obter vantagem ilícita. (Andreucci, 2014). Assim, a vítima, acreditando na boa-fé do agente, acaba entregando voluntariamente bens ou valores após ser manipulada e convencida de que a promessa ou acordo será cumprido. Dito isso, surgiu uma nova modalidade chamada “Estelionato virtual”.

O estelionato virtual corresponde a uma forma de fraude praticada no ambiente digital, na qual o agente utiliza tecnologias e a internet para aplicar golpes que se enquadram nas disposições do artigo 171 do Código Penal Brasileiro. Nesse tipo de crime, o autor busca obter vantagem ilícita para si ou para terceiros, provocando prejuízo à vítima por meio de práticas enganosas capazes de levá-la ao erro. (Gonçalves; Henriques, 2023).

Também é destacado que determinados acontecimentos recentes contribuíram para a ampliação desse tipo de delito. Durante a pandemia de COVID-19, medidas de distanciamento social foram adotadas em vários países para conter a disseminação do vírus, com isso, surgiu uma ferramenta essencial que possibilitou e facilitou os pagamentos online.

Com isso, diversas atividades passaram a ser realizadas de forma remota, como trabalho, estudos e serviços em geral. Esse cenário levou a um aumento significativo do uso simultâneo de dispositivos conectados à internet, fator que acabou favorecendo o crescimento das fraudes digitais, incluindo o estelionato virtual. (Gonçalves; Henriques, 2023, p. 8).

A fraude eletrônica foi introduzida no Código Penal pela Lei nº 14.155/2021. Posteriormente, o dispositivo sofreu nova alteração pela

Lei nº 15.397/2026, passando a contemplar, entre outros meios, a utilização de redes sociais, contatos telefônicos, correio eletrônico fraudulento, duplicação de dispositivo eletrônico ou aplicação de internet (BRASIL, 2021; BRASIL, 2026).

A utilização de recursos digitais pode fazer com que uma fraude seja desenvolvida mediante diferentes etapas. A comunicação com a vítima, a obtenção de informações, a realização da operação financeira e a movimentação posterior dos valores podem envolver instrumentos distintos. Para a investigação, essa multiplicidade pode exigir o exame conjunto de elementos digitais e financeiros.

A prova digital possui características próprias que devem ser consideradas durante sua obtenção e utilização. Saad, Rossi e Partata (2024) analisam justamente as particularidades das provas digitais e os direitos fundamentais que podem ser afetados pelas medidas destinadas à sua obtenção. Para os autores, a obtenção desses elementos demanda requisitos capazes de orientar sua utilização no processo penal.

Nesse sentido, a identificação de determinado registro, conta ou dispositivo não deve ser automaticamente confundida com a identificação da autoria. O elemento encontrado precisa ser analisado dentro do contexto da investigação e relacionado aos demais dados disponíveis. Essa distinção será importante para compreender, posteriormente, os limites existentes entre o rastreamento de informações e a efetiva atribuição de responsabilidade.

2.1. O Pix e Sua Utilização nas Transações Fraudulentas

O Pix constitui sistema de pagamentos instantâneos instituído pelo Banco Central do Brasil por meio da Resolução BCB nº 1, de 12 de agosto de 2020, que instituiu o arranjo de pagamentos Pix e aprovou seu Regulamento. Sua utilização permite a realização de operações de pagamento e transferência de recursos por meio da infraestrutura estabelecida para o funcionamento do arranjo (Banco Central do BRASIL, 2020).

A utilização do Pix também passou a integrar diferentes formas de movimentação financeira relacionadas à prática de fraudes. Em determinadas situações, o mecanismo de pagamento pode ser utilizado para o recebimento de valores obtidos mediante fraude, fazendo com que a transferência realizada pela vítima passe a integrar a sequência de movimentações financeiras relacionadas ao fato investigado. Nesse contexto, a operação realizada por meio do Pix pode constituir um dos elementos a serem analisados durante a apuração da ocorrência.

Além disso, o Pix passou a ser utilizado em diferentes modalidades de golpes, nas quais os criminosos procuram induzir a vítima a realizar voluntariamente uma transferência. Entre as práticas apresentadas pela Universidade Federal do Rio de Janeiro estão a clonagem de contas de WhatsApp, a utilização de perfis falsos e a falsa central bancária. Também são mencionadas situações envolvendo supostos benefícios ou falhas relacionadas ao sistema, utilizadas para convencer a vítima a realizar a operação (Universidade Federal do Rio de Janeiro, 2021).

O uso do pix nessas práticas demonstra que as transações fraudulentas podem envolver estratégias destinadas a induzir a vítima à realização da transferência. Recentemente, surgiram golpes

mediante adulteração de códigos QR e pela chamada “Taxa do Pix”, em que criminosos utilizam mensagens com identidade visual da Receita Federal para alegar uma suposta cobrança e induzir a vítima a realizar um pagamento por boleto ou Pix (Universidade Federal do Rio de Janeiro, 2021).

Portanto, verifica-se que o Pix, ao proporcionar maior rapidez e praticidade às transações financeiras, também passou a ser utilizado em diferentes modalidades de golpes, nas quais a vítima é induzida a realizar a transferência. As características dessas práticas demonstram que a utilização desta ferramenta nas fraudes envolve diferentes estratégias para obtenção dos valores, tornando relevante a compreensão dos mecanismos utilizados nessas transações.

2.2. As Chamadas “Contas-Laranja” nos Golpes Praticados Via Pix

De Sanctis (2014) define a chamada "conta laranja" como a conta de depósitos ou de operações financeiras mantida sob o nome de pessoa física ou jurídica seja ela real ou fictícia que disponibiliza seus dados de forma consciente ou inadvertida. Para o autor, a finalidade precípua desse expediente é dissimular o real proprietário dos recursos e inviabilizar a reconstrução do caminho percorrido pelos valores ilícitos.

As contas-laranja são abordadas na literatura acadêmica em sua relação com o estelionato e as fraudes financeiras em ambientes digitais. Moreira, Martins e Mantovani (2024) analisam a utilização de indivíduos e empresas como intermediários para ocultar a identidade dos verdadeiros autores dos golpes. O estudo também relaciona essas práticas ao uso fraudulento de dados bancários e

pessoais das vítimas e à expansão dos meios de pagamento instantâneos, como o Pix.

No âmbito jurídico, a Lei nº 15.397/2026 passou a prever expressamente a cessão de conta bancária para o trânsito de recursos relacionados à atividade criminosa. O art. 171, § 2º, VII, do Código Penal estabelece a conduta de quem cede, gratuitamente ou mediante pagamento, conta bancária para que nela transitem recursos destinados ao financiamento de atividade criminosa ou que dela sejam provenientes. A previsão passou a integrar especificamente o dispositivo denominado “Cessão de conta-laranja” (BRASIL, 2026).

Melo (2026) analisa a nova previsão penal relacionada à cessão de conta-laranja e diferencia essa conduta do estelionato. Segundo sua análise, enquanto o estelionato envolve a obtenção de vantagem financeira ilícita mediante fraude, a cessão de conta-laranja se caracteriza pela cessão da conta bancária para que nela transitem recursos relacionados à atividade criminosa. A análise, portanto, permite distinguir a utilização da conta como instrumento financeiro da própria conduta de sua cessão.

A utilização de uma conta bancária vinculada a uma fraude não permite, por si só, concluir que seu titular tenha participado conscientemente do delito. Conforme Cunha (2026), a configuração do crime de cessão de conta laranja exige dolo, de modo que a simples disponibilização da conta a terceiro, quando realizada de forma neutra ou desatenta, não é suficiente para caracterizar a conduta criminosa.

É necessário que o agente tenha consciência de que a conta será utilizada para o trânsito de recursos destinados a atividade criminosa ou provenientes dela, ainda que não conheça todos os detalhes do delito subjacente. Assim, a titularidade ou disponibilização da conta deve ser analisada juntamente com os elementos que permitam verificar a existência de consciência e vontade na conduta do agente. (Cunha, 2026).

Essa diferenciação também aparece na discussão acadêmica sobre contas-laranja e roubo de identidade. Moreira, Martins e Mantovani (2024) descrevem a utilização fraudulenta de dados bancários e pessoais das vítimas em práticas financeiras fraudulentas, incluindo situações relacionadas à obtenção indevida de empréstimos. Nesse contexto, os dados de determinada pessoa podem aparecer vinculados a uma operação sem que essa circunstância, isoladamente considerada, permita estabelecer sua participação consciente na fraude.

A cessão de conta laranja é caracterizada, nos termos do art. 171, § 2º, VII, do Código Penal, pela conduta de quem:

“Cede, gratuita ou onerosamente, conta bancária para que nela transitem recursos destinados ao financiamento de atividade criminosa ou que dela sejam fruto” (BRASIL, 1940).

A respeito dessa conduta, Cunha (2026) destaca a necessidade de interpretar restritivamente o tipo penal, considerando a finalidade da disponibilização da conta e sua relação com a circulação de recursos vinculados a atividades criminosas, especialmente no contexto das fraudes.

Badaró e Bottini (2022, p. 90) entendem que o aspecto central da conduta não está propriamente em ocultar os valores, mas na utilização de recursos de origem ilícita no âmbito da economia formal. A partir dessa compreensão, a consumação da cessão de conta laranja ocorre com a disponibilização da conta bancária para a circulação de recursos destinados ao financiamento de atividade criminosa.

Nesse contexto, a conduta não pressupõe necessariamente a conversão de valores ilícitos em recursos aparentemente legítimos. O objetivo pode estar relacionado à própria movimentação ou utilização desses valores para finalidades vinculadas à atividade criminosa.

2.3. O Anonimato e a Dificuldade de Identificação dos Envolvidos

A utilização de recursos tecnológicos na prática de golpes pode dificultar a identificação dos indivíduos envolvidos. O ambiente digital permite que determinadas condutas sejam realizadas por diferentes meios, enquanto os dados utilizados na fraude podem estar relacionados a pessoas distintas daquela que efetivamente obtém o benefício decorrente da prática.

Nesse contexto, a utilização de contas laranjas apresenta relação com a dificuldade de identificação dos responsáveis pelos golpes. Moreira, Martins e Mantovani (2024) observam que:

Por meio desse golpe, não só dinheiro é roubado, mas também dados bancários, proporcionando acesso total à conta da vítima, possibilitando que sejam realizados empréstimos em nome dela, sem prejudicar o autor do crime, que obtém benefício próprio, causando prejuízos a terceiros. Frequentemente, os autores conseguem escapar do crime devido ao cenário ser predominantemente tecnológico, o que lhes permite evitar a detecção pelas autoridades e se eximir de sua responsabilidade civil. (Moreira; Martins; Mantovani, 2024, p. 558).

A utilização de dados bancários também pode integrar a dinâmica dessas práticas. Conforme o trabalho analisado, os dados podem ser utilizados para proporcionar acesso à conta da vítima e possibilitar a realização de empréstimos em seu nome. Dessa forma, a fraude pode envolver não apenas a movimentação de valores, mas também a utilização de informações pertencentes a terceiros.

A identificação dos envolvidos, nesse cenário, relaciona-se às diferentes formas pelas quais os recursos tecnológicos e os dados bancários podem ser empregados na prática dos golpes. A presença de informações vinculadas a determinada pessoa ou conta não permite, isoladamente, estabelecer todas as circunstâncias relacionadas à prática fraudulenta.

3. A PROVA DIGITAL E O RASTREAMENTO DIGITAL E FINANCEIRO

A prova digital possui características próprias que a diferenciam dos meios de prova tradicionais, sobretudo em razão da forma como seus elementos são constituídos e apresentados. Nesse sentido, sua compreensão exige considerar a natureza digital dos dados que podem servir à reconstrução dos fatos investigados.

Segundo Badaró (2021), a prova digital caracteriza-se por ter origem em uma manipulação eletrônica de dados, que são conservados e transmitidos em linguagem digital. Diferentemente das provas tradicionais, esses elementos não apresentam materialidade imediatamente constatável, razão pela qual sua utilização na reconstrução dos fatos exige a observância de métodos próprios da computação forense.

Saad, Rossi e Partata (2024) destacam que a prova digital possui características próprias, entre as quais estão a imaterialidade, a volatilidade e o desprendimento do suporte físico. Os autores apontam ainda que os dados digitais podem ser reproduzidos por meio de cópias fiéis e que sua compreensão depende da utilização de equipamentos capazes de processá-los e apresentá-los em linguagem natural.

A compreensão dessas particularidades permite perceber que a prova digital exige procedimentos próprios para sua adequada análise. Badaró (2021) destaca que as características específicas desse meio de prova demandam métodos próprios de computação forense, abrangendo sua obtenção, conservação, análise e apresentação dos resultados. Assim, essas características devem ser consideradas na apreciação dos elementos obtidos em meio digital.

A obtenção de elementos digitais pode ocorrer por diferentes meios, de acordo com a natureza dos dados e com o local em que estão armazenados. Saad, Rossi e Partata (2024) apontam que as provas digitais podem ser obtidas por meio de interceptação telemática, coleta de dados após a apreensão de dispositivos eletrônicos, requisição de informações a terceiros, como provedores de conexão

e aplicações de internet, além do acesso remoto mediante softwares específicos.

A diversidade dos meios de obtenção demonstra que os dados digitais podem ser coletados por diferentes procedimentos, conforme as circunstâncias da investigação (Saad; Rossi; Partata, 2024). A preservação desses elementos também assume importância, especialmente diante da necessidade de assegurar sua integridade e autenticidade após a coleta (BRASIL, 2022).

No contexto dos golpes praticados por meio do Pix, os registros das operações financeiras podem integrar o conjunto de elementos digitais analisados durante a investigação. Desse modo, os dados relacionados às transações podem ser examinados em conjunto com outras informações obtidas na apuração dos fatos.

3.1. O Rastreamento das Transações Realizadas Pelo Pix

A utilização do Pix deixa registros associados às operações realizadas, permitindo que uma transação seja examinada a partir das informações que a acompanham. Essa característica possui relevância quando determinada operação está relacionada a uma fraude, pois possibilita observar a conta de destino e as movimentações posteriores relacionadas aos valores.

Segundo o Banco Central do Brasil (2026), o rastreamento pode ser realizado mediante o mapeamento do caminho percorrido pelos valores a partir da transação inicial. Esse procedimento pode representar, por meio de um grafo de rastreamento, as diferentes contas pelas quais os recursos passaram e as transações subsequentes relacionadas a esse percurso.

Esse acompanhamento permite reconstruir o percurso dos recursos a partir da transação inicial, alcançando também as movimentações realizadas posteriormente. O Banco Central do Brasil define o grafo de rastreamento como o mapeamento do caminho percorrido pelos recursos desde a transação de origem, permitindo identificar as operações subsequentes relacionadas ao desvio dos valores (Banco Central do BRASIL, 2026).

O rastreamento também está relacionado ao Mecanismo Especial de Devolução (MED). Conforme o Banco Central do Brasil (2026), o processo de Recuperação de Valores permite rastrear transações e bloquear recursos suspeitos de envolvimento em fraude não apenas na conta de destino da operação original, mas também em transações subsequentes. O mecanismo, portanto, amplia o acompanhamento do percurso financeiro quando há suspeita de fraude ou golpe.

A existência desses registros permite acompanhar a circulação dos valores ao longo das operações realizadas, reunindo informações correspondentes às diferentes etapas desse percurso. Assim, o rastreamento oferece uma visão mais abrangente da sequência financeira formada pelas transações relacionadas, permitindo que seus registros sejam examinados conjuntamente no curso da apuração.

3.2. O Cruzamento de Dados Digitais e Financeiros na Investigação

O rastreamento das operações financeiras pode ser relacionado a outros elementos obtidos durante a investigação, permitindo uma análise mais ampla da dinâmica da fraude. Nesse sentido, as

informações financeiras podem ser confrontadas com registros digitais e demais dados disponíveis, de modo que diferentes elementos sejam examinados conjuntamente.

A existência de mecanismos de compartilhamento dessas informações também alcança as operações realizadas pelo Pix. Conforme consta na ADI 7.276/DF, a Declaração de Informações de Meios de Pagamentos (DIMP) prevê a prestação mensal e automática de informações sobre pagamentos, transferências de recursos e transações eletrônicas realizadas pelo Pix às unidades federadas (BRASIL, 2024).

O cruzamento desses dados permite analisar as movimentações financeiras em conjunto com outros registros da investigação. Isso é relevante porque a identificação de uma conta ou de uma determinada operação não estabelece, isoladamente, a autoria da fraude. A reunião dos elementos disponíveis pode contribuir para uma compreensão mais abrangente da dinâmica dos fatos.

4. DAS “CONTAS-LARANJA” À IDENTIFICAÇÃO DE POSSÍVEIS MANDANTES

A utilização de contas-laranja constitui um dos obstáculos para a identificação dos responsáveis pelos golpes praticados por meio do Pix. Isso ocorre porque os valores provenientes da fraude podem ser direcionados para contas pertencentes a terceiros, que passam a atuar como intermediários no recebimento dos recursos, dificultando a identificação do verdadeiro autor do delito.

Nesse sentido, o Tribunal de Justiça de São Paulo reconheceu que a utilização de pessoas interpostas para o recebimento do proveito ilícito pode ter como finalidade ocultar a identidade do criminoso,

sendo possível, ainda, que o titular da conta figure apenas como intermediário ou tenha sido vítima de fraude na abertura da conta (São Paulo, 2026, p. 5).

Brandão (2022) observa que os golpes praticados por meio do Pix podem envolver contas-laranja criadas fraudulentamente em nome de terceiros ou contas já existentes utilizadas sem o conhecimento de seus titulares. A utilização dessas contas permite que os valores provenientes dos crimes sejam direcionados a pessoas que, em determinadas situações, não correspondem aos responsáveis pela fraude.

Portanto, as contas-laranja podem representar apenas uma das etapas da atuação dos envolvidos, sem necessariamente revelar quem está por trás da fraude. Por isso, a identificação dos responsáveis exige que a investigação ultrapasse a simples verificação do titular da conta utilizada, considerando também os elementos relacionados à própria movimentação dos valores.

4.1. O Rastreamento do Fluxo Financeiro e Sua Relação com a Investigação da Autoria

A utilização de contas-laranja não se limita ao recebimento inicial dos valores obtidos por meio do golpe. A movimentação dos recursos pode prosseguir por diferentes contas, fazendo com que a identificação da primeira conta de destino não represente todo o percurso financeiro relacionado à fraude, tornando a identificação ainda mais difícil.

Maragno e Yamazato (2026) descrevem que, após uma transferência realizada por Pix, os valores podem ser imediatamente pulverizados em dezenas de outras contas, inclusive de instituições diferentes.

Segundo os autores, essa movimentação pode ser acompanhada da conversão dos recursos em criptoativos ou de seu saque em espécie, circunstâncias que tornam o rastreamento manual dos valores impossível nas condições analisadas.

Nesse sentido, o rastreamento do fluxo financeiro pode fornecer elementos para a investigação das diferentes contas envolvidas na circulação dos valores. A partir da análise dessas movimentações, a investigação pode avançar para além da identificação do primeiro destinatário, considerando as demais contas pelas quais os recursos foram posteriormente movimentados.

A investigação dos golpes praticados por meio do Pix envolve não apenas a análise das operações realizadas, mas também a atuação das instituições financeiras e das autoridades responsáveis pela apuração dos fatos. As informações produzidas no curso das transações podem contribuir para identificar as contas envolvidas e acompanhar as operações relacionadas à fraude.

Nesse sentido, o Banco Central do Brasil informa que as operações realizadas pelo Pix são rastreáveis, permitindo a identificação de contas envolvidas em fraudes e facilitando a atuação da polícia e do Poder Judiciário. O sistema também dispõe de mecanismos de compartilhamento de informações entre as instituições participantes, destinados à identificação e ao tratamento de indícios de fraude (Banco Central do BRASIL, 2026).

A cooperação com as autoridades também foi ampliada. O Banco Central passou a permitir que polícias, Ministérios Públicos e outros órgãos com atribuições legais de persecução penal consultem diretamente dados cadastrais vinculados às chaves Pix de usuários

sob investigação. Entre as informações disponibilizadas estão nome, CPF ou CNPJ, instituição de relacionamento, agência e conta, além de dados referentes à chave Pix. (Banco Central do BRASIL, 2026).

Dessa forma, a atuação conjunta permite que as informações relacionadas às transações e às contas utilizadas nas fraudes sejam consideradas de maneira integrada. Esse intercâmbio amplia os elementos disponíveis para a investigação e pode contribuir para o esclarecimento da dinâmica das operações e para a identificação dos envolvidos.

4.2. Possibilidades e Limites para o Aprimoramento da Investigação de Golpes Via Pix

O aprimoramento da investigação dos golpes praticados por meio do Pix depende do desenvolvimento de mecanismos capazes de acompanhar a movimentação dos recursos após a primeira transferência. Nesse sentido, o Banco Central aperfeiçoou o MED para permitir o mapeamento dos valores para além da primeira conta receptora, alcançando outras contas utilizadas na dispersão dos recursos e possibilitando o bloqueio e a devolução de valores relacionados à fraude (Banco Central do BRASIL, 2026).

Além dos mecanismos financeiros, a integração entre diferentes instituições constitui outra possibilidade de aprimoramento. O Ministério da Justiça e Segurança Pública destaca a importância da interoperabilidade de bases de dados e do com-partilhamento de informações em tempo real entre instituições financeiras, operadoras, plataformas digitais e autoridades policiais para tornar mais efetiva a resposta às fraudes digitais (BRASIL, 2026).

Apesar desses avanços, permanecem limites relacionados à própria dinâmica dos golpes, especialmente diante da rapidez com que os recursos podem ser movimentados e da participação de diferentes agentes e setores. O enfrentamento das fraudes, portanto, não depende apenas da identificação da primeira conta utilizada, mas da capacidade de acompanhar a cadeia de movimentações e integrar as informações disponíveis.

5. RESULTADOS E ANÁLISES

A pesquisa realizada permitiu identificar que os golpes praticados por meio do Pix apresentam dificuldades próprias para a investigação penal, principalmente em razão da utilização de meios digitais e da dinâmica das transações financeiras. Apesar de as operações deixarem registros que podem ser utilizados na investigação, esses registros precisam ser analisados em conjunto com outras informações para que possam contribuir para a identificação dos envolvidos.

A análise também demonstrou que a investigação desses crimes não se resume à identificação da pessoa vinculada a determinada conta ou operação. A utilização de contas de terceiros, a circulação dos valores entre diferentes contas e a possibilidade de utilização de diferentes recursos durante a fraude dificultam a reconstrução dos fatos. Nesse sentido, a análise das evidências digitais e financeiras assume importância para que a investigação não permaneça limitada ao primeiro elemento identificado.

Outro ponto observado foi a necessidade de articulação entre as informações produzidas pelas instituições financeiras e aquelas obtidas pelas autoridades responsáveis pela investigação. Os

mecanismos existentes permitem ampliar os dados disponíveis sobre as operações e auxiliar no acompanhamento dos valores. Entretanto, as próprias características das transações realizadas por meio do Pix, especialmente sua rapidez e a possibilidade de dispersão dos recursos, impõem limites à apuração.

Diante disso, os resultados da pesquisa indicam que o principal desafio da investigação dos golpes via Pix está em transformar os registros deixados pelas operações em elementos capazes de esclarecer a dinâmica da fraude e contribuir para a identificação de seus responsáveis. A análise das contas utilizadas, do percurso dos valores e das demais informações disponíveis deve ocorrer de forma conjunta, permitindo que a investigação avance além da constatação inicial de que determinado golpe foi realizado.

6. CONSIDERAÇÕES FINAIS

Este trabalho analisa os desafios enfrentados pela investigação penal diante dos golpes praticados por meio do Pix, considerando as dificuldades de rastreamento digital e a utilização de contas de terceiros. A partir desta pesquisa, verifica-se que a existência de registros digitais e financeiros não é suficiente, por si só, para determinar a autoria da fraude, sendo necessária a análise conjunta das informações produzidas durante a investigação.

Nesse sentido, conclui-se que as dificuldades de identificação dos responsáveis estão relacionadas à própria dinâmica dos golpes, especialmente quando os valores são movimentados entre diferentes contas e instituições. A identificação da primeira conta utilizada pode representar apenas o início da apuração, tornando

necessário acompanhar as movimentações posteriores e relacioná-las aos demais elementos disponíveis.

Também se verificou que os mecanismos de rastreamento financeiro e o compartilhamento de informações entre instituições e autoridades podem contribuir para o desenvolvimento da investigação. Contudo, esses instrumentos não eliminam as dificuldades existentes, pois a rapidez das transações e a utilização de diferentes meios para movimentação dos valores podem dificultar a reconstrução completa da fraude.

Dessa forma, em resposta ao problema proposto, a pesquisa conclui que o avanço da investigação dos golpes via Pix depende da capacidade de ultrapassar a identificação inicial da conta ou do registro digital e analisar o conjunto de informações relacionadas à fraude. Assim, o rastreamento dos valores, a análise das evidências digitais e a atuação integrada das instituições constituem elementos relevantes para ampliar a apuração e possibilitar a identificação dos possíveis responsáveis, sem que a localização de uma conta, isoladamente, seja tratada como prova definitiva de autoria.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDREUCCI, Ricardo Antonio. **Manual de Direito Penal**. 10 ed. São Paulo: Saraiva, 2014.

BADARÓ, Gustavo Henrique; BOTTINI, Pierpaolo Cruz. **Aspectos penais e processuais penais: comentários à Lei 9.613/1998, com alterações da Lei 12.683/2012**. 5. ed. rev., atual e ampl. São Paulo: Thomson Reuters Brasil, 2022.

BADARÓ, Gustavo. **Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia.** Boletim IBCCRIM, São Paulo, ano 29, n. 343, p. 7-9, jun. 2021. Disponível em: Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia | Boletim IBCCRIM https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325/627. Acesso em: 25 set. 2026.

BANCO CENTRAL DO BRASIL. **Guia de implementação dos procedimentos de devolução no Pix, com ênfase no Mecanismo Especial de Devolução – versão 4.2.** Brasília, DF: Banco Central do Brasil, 2026. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/pix/Regulamento_Pix/versoes_futuras/Guia_MED-versao4-2.pdf. Acesso em: 25 set. 2026.

BANCO CENTRAL DO BRASIL. **Pix fica mais eficiente no combate a fraudes e crimes.** Brasília, DF: Banco Central do Brasil, 2026. Disponível em: <https://www.bcb.gov.br/detalhenoticia/709/noticia>. Acesso em: 14 set. 2026.

BANCO CENTRAL DO BRASIL. **Pix: segurança.** Brasília, DF: Banco Central do Brasil, [s. d.]. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/pix-seguranca>. Acesso em: 25 set. 2026.

BANCO CENTRAL DO BRASIL. **Relatório de Gestão do Pix 2023-2025.** Brasília, DF: Banco Central do Brasil, 2026. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/pix/relatorio_d_e_gestao_pix/relatorio_gestao_pix_2026.pdf. Acesso em: 14 set. 2026.

BANCO CENTRAL DO BRASIL. **Resolução BCB nº 1, de 12 de agosto de 2020. Institui o arranjo de pagamentos Pix e aprova o seu Regulamento.** Brasília, DF: Banco Central do Brasil, 2020. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=1&tipo=Resolu%C3%A7%C3%A3o%20BCB&>. Acesso em: 12 set. 2026.

BRANDÃO, Ana Elise Azevedo. **Responsabilidade dos bancos em caso de golpe e sequestro do Pix.** Folha Online, 12 nov. 2022. Disponível em: <https://www.folhaonline.es/artigo-responsabilidade-dos-bancos-em-caso-de-golpe-e-sequestro-do-pix/>. Acesso em: 14 set. 2026.

BRASIL. Câmara dos Deputados. **Grupo de Trabalho destinado a elaborar proposição legislativa em substituição ao Código de Processo Penal. Texto final – prova digital.** Brasília, DF: Câmara dos Deputados, 2022. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/gt-anteprojeto-do-novo-codigo-de-processo-penal/outros-documentos/O.TEXTOFINALProvaDigitalart.298at320.pdf/view>. Acesso em: 9 out. 2026.

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: 11 set. 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: 11 set. 2026.

BRASIL. **Lei nº 15.397, de 30 de abril de 2026. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), a fim de majorar as penas previstas para os crimes de furto, roubo, estelionato, receptação, receptação de animal e interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, bem como para tipificar os crimes de receptação de animal doméstico e de fraude bancária.** Brasília, DF: Presidência da República, 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15397.htm. Acesso em: 12 set. 2026.

BRASIL. **Ministério da Justiça e Segurança Pública. Sedigi defende integração entre setores para prevenir fraudes digitais.** Brasília, DF, 2026. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias-1/sedigi-defende-integracao-entre-setores-para-prevenir-fraudes-digitais>. Acesso em: 14 set. 2026.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 7.276 Distrito Federal. Relatora: Ministra Cármen Lúcia.** Brasília, DF: Supremo Tribunal Federal, 9 set. 2024. Disponível em: https://alcantara.pro.br/portal/wp-content/uploads/2024/09/Acordao_ADI-7276.pdf. Acesso em: 25 set. 2026.

CAPEZ, Fernando. **Curso de direito penal, v. 2: parte especial: arts. 121 a 212.** 20. ed. São Paulo: Saraiva Educação, 2020.

CUNHA, Rogério Sanches. **Lei 15.397/26: cessão de conta laranja, interpretação restritiva e limites penais.** Meu Site Jurídico, 4 maio 2026. Disponível em: <https://meusitejuridico.editorajuspodivm.com.br/2026/05/04/lei-15-397-26-cessao-de-conta-laranja-interpretacao-restritiva-e-limites-penais/>. Acesso em: 16 out. 2026.

DE SANCTIS, Fausto Martin. **Lavagem de Dinheiro: Teoria e Prática Penal.** São Paulo: Editora Revista dos Tribunais, 2014.

GONÇALVES, Samuel Martins; HENRIQUES, Thiago Alves. **Crimes digitais: análise sobre o estelionato virtual. Cadernos Jurídicos, 2023.** Disponível em: <https://revista.fadipa.br/index.php/cjuridicas/article/view/576/525>. Acesso em: 12 set. 2026.

MARAGNO, Ryan; YAMAZATO, Fauzi Anderson. **O estado de fraude e do estelionato digital no Brasil: evolução sistêmica, tipologias emergentes e a nova arquitetura de segurança (2020-2025).** Revista do Ministério Público Militar, Brasília, v. 53, n. 50, p. 13-42, 2026. DOI: 10.5281/zenodo.18175551. Disponível em: <https://revista.mpm.mp.br/rmpm/article/view/512/483>. Acesso em: 14 set. 2026.

MELO, Luis Felipe Muniz. **Notas sobre o crime de cessão de conta laranja (art. 171, § 2º, inciso VI, do CP). Jornal de Ciências Criminais, [S. l.], v. 1, 2026.** Disponível em: <https://jcc.ibccrim.org.br/artigos/notas-sobre-o-crime-de-cessao-de-conta-laranja-art-171-%C2%A72o-inciso-vi-do-cp>. Acesso em: 12 set. 2026.

MOREIRA, Camila Viríssimo R. S.; MARTINS, Gabriel Sevulski; MANTOVANI, Jhenifer Matilde. **Desvendando o estelionato: o mundo secreto das contas laranjas e do roubo de identidade.**

Anais do CDU – Congresso de Direito UniCesumar, [S. l.], p. 561–564, 2024. Disponível em:

<https://lgpublica.com/index.php/anaiscd�/article/view/206/221>.

Acesso em: 12 set. 2026.

SAAD GIMENES, Marta C.; ROSSI, Helena Costa; PARTATA, Pedro H. **A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais.** Revista Brasileira de Direito Processual Penal, Porto Alegre, v. 10, n. 3, e1071, set./dez. 2024. DOI: 10.22197/rbdpp.v10i3.1071. Disponível em:

<https://www.scielo.br/j/rbdpp/a/s94cLkSsHMDKmg5kf4YCkHk/>.

Acesso em: 11 set. 2026.

SÃO PAULO (Estado). **Tribunal de Justiça. Acórdão nº 20368726. São Paulo, 2026.** Disponível em:

<https://esaj.tjsp.jus.br/cjsg/jsp/verificarLoginArquivo.jsp?cdAcordao=20368726&cdForo=0>. Acesso em: 9 out. 2026.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO. **Pix: 6 golpes. Segurança da Informação** — TIC/UFRJ, 15 jun. 2021. Disponível em: <https://seguranca.tic.ufrj.br/noticias/pix-6-golpes/>. Acesso em: 12 set. 2026.

¹ Acadêmico(a) do Curso de Direito da Faculdade de Educação Santa Terezinha – FEST, Imperatriz-MA. E-mail: [acesse o artigo original para visualizar o e-mail](#)

² Advogada. Professora. Bacharel em Direito pela Universidade Federal do Maranhão (UFMA). Licenciada em Filosofia (UniBF). Especialista em Direito Tributário (UniBF). Pós-graduanda em Direito Penal. E-mail: [acesse o artigo original para visualizar o e-mail](#)