IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO II

D597

Direito penal, processo penal e constituição II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Gustavo Noronha de Avila; Matheus Felipe De Castro; Flavia Piccinin Paz – Florianópolis: CONPEDI, 2026.

Inclui bibliografia
ISBN: 978-65-5274-601-6
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito penal. 3. Processo penal. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO II

Apresentação

Em mais uma edição do CONPEDI Virtual, o Grupo de Trabalho de Direito Penal apresenta uma coletânea de estudos que refletem a profundidade e a diversidade das discussões contemporâneas na área.

Primeiramente, no trabalho intitulado UMA ANÁLISE DO TIPO OBJETIVO DO CRIME DE GESTÃO TEMERÁRIA DE INSTITUIÇÃO FINANCEIRA, os autores Roberta Arrechea , Priscila Alencar Veríssimo de Souza têm como objetivo O presente artigo analisa o tipo objetivo do crime de gestão temerária de instituição financeira, previsto no parágrafo único do artigo 4º da Lei nº 7.492/1986, à luz do princípio da legalidade penal. Adotando metodologia qualitativa, de natureza jurídico-dogmática e crítico-bibliográfica, a pesquisa examina a indeterminação dos elementos “gestão” e “temerária”, demonstrando como a ausência de critérios legais precisos compromete a previsibilidade da norma penal e amplia a margem de discricionariedade judicial.

Na sequência, o artigo A CONDENAÇÃO DE OFÍCIO NO PROCESSO PENAL BRASILEIRO: (IN)COMPATIBILIDADE DO ART. 385 DO CÓDIGO DE PROCESSO PENAL COM O SISTEMA ACUSATÓRIO CONSTITUCIONAL, de autoria de Cassius Guimaraes Chai , Gabryella Moreira Amaral dos Santos , Anna Júlia Vieira da Silva, busca O artigo analisa a compatibilidade do art. 385 do Código de Processo Penal com o sistema acusatório instituído pela Constituição Federal de 1988.

Ainda sobre temas relevantes, o estudo CRIMINALIDADE TRANSNACIONAL E JUSTIÇA GLOBAL: ENTRE OS LIMITES DO DIREITO PENAL CLÁSSICO E O PAPEL

como propósito O presente artigo analisa o fenômeno do lawfare como forma contemporânea de instrumentalização estratégica do Direito e das instituições jurídicas, compreendendo-o para além da simples judicialização da política ou do ativismo judicial. Parte-se da premissa de que o Direito, nas democracias contemporâneas, passou a operar também como tecnologia de poder, sendo utilizado em disputas políticas, econômicas e geopolíticas por meio da mobilização estratégica de normas, procedimentos e narrativas jurídicas.

Em seguida, o artigo PROTEÇÃO PENAL DA ORDEM ECONÔMICA: A ATUAÇÃO PREVENTIVA DO DIREITO PENAL NOS CRIMES ECONÔMICOS ENQUANTO DEFENSOR DE BENS SUPRAINDIVIDUAIS, de autoria de Allaymer Ronaldo Regis Dos Bernardos Bonesso , Lucas Bertolucci Barbosa de Lima , Vinícius Bernardino, objetiva A economia sendo um elemento fundamental para a humanidade não podia ter sido esquecida pelo Direito, por isso foi incorporada como um bem jurídico digno de tutela penal, o que deu origem a embates sobre como proceder para a proteção desse bem. É nesse contexto que surge o debate acerca da legitimidade do Direito Penal para intervir na defesa da ordem econômica de modo preventivo, com base na lógica de crimes de perigos, tese que recebe muitas críticas, contudo, o presente artigo busca defendê-la, explicando o porquê ser legítima a repressão prévia aos crimes econômicos.

Outro ponto de destaque é o estudo DEPOIMENTO ESPECIAL E ESCUTA ESPECIALIZADA POR VIDEOCONFERÊNCIA NA PROTEÇÃO INTEGRAL DE CRIANÇAS E ADOLESCENTES: ANÁLISE CRÍTICA DA LEI Nº 13.431/2017 E SEUS DESAFIOS DE EFETIVAÇÃO., de Aline de Andrade Lourenço , Gustavo Henrique de Andrade Cordeiro, que busca O presente artigo analisa criticamente os mecanismos processuais instituídos pela Lei nº 13.431/2017 — escuta especializada e depoimento especial por videoconferência — como instrumentos de proteção integral de crianças e adolescentes vítimas ou testemunhas de violência no Brasil. Diante do quadro alarmante de violência sexual contra menores revelado pelo 19º Anuário Brasileiro de Segurança Pública (2025), o estudo investiga em que medida tais mecanismos são suficientes para garantir a não

baseada na análise de referenciais legais, doutrinários e empíricos relacionados à proteção integral da infância e da adolescência no Brasil.

Em um contexto similar, o trabalho ADPF N.º 635 E MINISTÉRIO PÚBLICO DESAFIOS DO CONTROLE EXTERNO DA ATIVIDADE POLICIAL À LUZ DO CONTROLE DE CONVENCIONALIDADE, de Francisco Antonio Nieri Mattosinho , Laura Bianchi Picinin, visa Este artigo analisa a atuação do Ministério Público no controle externo da atividade policial à luz da jurisprudência da Corte Interamericana de Direitos Humanos e da ADPF n.º 635, com enfoque em territórios socialmente vulneráveis marcados pela governança criminosa. Parte-se da seguinte pergunta-problema: em que medida a atuação do Ministério Público no controle externo da atividade policial atende aos parâmetros fixados pela Corte Interamericana de Direitos Humanos e pela ADPF n.º 635?.

Abordando questões cruciais, o artigo IDENTIDADE DE GÊNERO, CÁRCERE E PODER JUDICIÁRIO: ANÁLISE DAS DECISÕES DO STJ SOBRE PESSOAS TRANS PRIVADAS DE LIBERDADE, de autoria de Pamella Bauer Velasco , Tatiane Lemos Nascente, tem como objetivo O presente trabalho analisa em que medida a identidade de gênero de pessoas trans privadas de liberdade é observada no sistema carcerário brasileiro, considerando a tensão entre a autodeterminação do sujeito e o poder decisório do Poder Judiciário. Parte-se da hipótese de que o sistema prisional brasileiro ainda opera sob uma lógica cisnormativa e binária, na qual o reconhecimento da identidade de gênero permanece condicionado à discricionariedade judicial e a critérios institucionais, produzindo limitações à autonomia dos sujeitos e violações de direitos fundamentais.

Ainda no campo das discussões atuais, o estudo FRAUDE ELETRÔNICA NO SISTEMA “PIX”: CONCEITO, PRINCÍPIOS, PREVENÇÃO, COMBATE, INVESTIGAÇÃO E RESPONSABILIZAÇÃO PENAL, de Thiago Braga Parente, busca O presente trabalho aborda o tema da fraude eletrônica praticada por meio do Pix, o sistema de pagamento instantâneo criado pelo Banco Central do Brasil em 2020. Em poucos anos, o Pix passou a

e na Colômbia. O problema central consiste em verificar em que medida os requisitos legais e os mecanismos de controle judicial revelam maior rigidez ou flexibilidade em cada ordenamento.

Outro relevante estudo é O SISTEMA DAS NULIDADES PROCESSUAIS PENAIS COMO INSTRUMENTO DE LIMITAÇÃO DO PODER PUNITIVO ESTATAL: CRÍTICA À RELATIVIZAÇÃO DAS NULIDADES ABSOLUTAS PELOS TRIBUNAIS SUPERIORES BRASILEIROS, de Marcelo Queiroz Alves De Oliveira , Rodrigo Suzana Guimarães , Adriano da Silva Ribeiro, que objetiva O presente artigo analisa o sistema das nulidades processuais penais no direito brasileiro, com enfoque na distinção entre nulidades absolutas e relativas e na crescente tendência de relativização das nulidades absolutas pelos tribunais superiores. A partir do estudo da tipicidade dos atos processuais penais, dos princípios regentes das nulidades, tais como o do prejuízo, da instrumentalidade das formas, da convalidação, do interesse e da causalidade, e das espécies de atos defeituosos (irregulares, inexistentes e nulos), o trabalho examina como o Supremo Tribunal Federal e o Superior Tribunal de Justiça vêm exigindo, de forma reiterada, a comprovação do prejuízo concreto e a arguição em momento oportuno mesmo nas hipóteses de nulidade absoluta.

A pesquisa O NOVO MARCO LEGAL DE COMBATE AO CRIME ORGANIZADO NO BRASIL: ENTRE A EXPANSÃO DO PODER PUNITIVO E A RECONFIGURAÇÃO DAS GARANTIAS PENAIS, desenvolvida por Cristian Kiefer Da Silva , Rafaela Cristina Alves Lisboa, tem como finalidade O presente trabalho tem por objetivo analisar o novo marco legal de combate ao crime organizado no Brasil, a partir das recentes reformas legislativas em matéria penal, processual penal e de execução penal ocorridas na contemporaneidade. Busca-se compreender, sob uma perspectiva crítica, os fundamentos político-criminais que orientam o endurecimento do sistema punitivo, especialmente no que se refere ao aumento de penas, à restrição de benefícios na execução penal, à ampliação de mecanismos de controle estatal e a criação de novos tipos penais incriminadores.

Com foco em aspectos específicos, o artigo A NOVA POSITIVAÇÃO DO PRINCÍPIO DO NE BIS IN IDEM E SEUS ATUAIS DESAFIOS NO DIREITO BRASILEIRO NAS RELAÇÕES ESPECIAIS DE SUJEIÇÃO, de autoria de Henrique Ribeiro Cardoso , André Felipe Santos de Souza , Madson Lima De Santana, tem como objetivo O presente artigo investiga a positivação do princípio do ne bis in idem no ordenamento jurídico brasileiro, compreendida em duas camadas. A primeira, de matriz supralegal, foi inaugurada em 1992 pelos Decretos nº 592 e nº 678, que incorporaram, respectivamente, o Pacto Internacional dos Direitos Civis e Políticos e a Convenção Americana sobre Direitos Humanos, positivando a vedação ao bis in idem segundo os critérios complementares do idem crimen e do idem factum.

Ainda sobre a temática, o estudo ESTUPRO DE VULNERÁVEL: A DERROTABILIDADE COMO MECANISMO PARA APLICAÇÃO DA EXCEÇÃO DE ROMEU E JULIETA, de Leandro Ernani Freitag, busca O presente artigo analisa a aplicabilidade da teoria da derrotabilidade como mecanismo para flexibilizar a rígida configuração do crime de estupro de vulnerável, especificamente nos casos que se enquadram na exceção de Romeu e Julieta. O objetivo da pesquisa é verificar como a teoria da derrotabilidade, inspirada nas formulações de Herbert Hart, pode ser utilizada para evitar punições desproporcionais e injustas em situações de estupro de vulnerável que não apresentem real lesividade ao bem jurídico tutelado, diante dos particulares detalhes do caso concreto submetido à análise judicial.

A pesquisa POPULISMO PENAL E EROSÃO DOS PRINCÍPIOS CONSTITUCIONAIS: IMPACTOS NA DEMOCRACIA BRASILEIRA DA PROPOSTA DE IMPLEMENTAÇÃO DA PENA DE MORTE E PRISÃO PERPÉTUA, desenvolvida por Saulo de Medeiros Torres, tem como finalidade O presente artigo analisa os impactos do populismo penal midiático na erosão das garantias fundamentais no Brasil, com foco na proposta legislativa do Deputado Kim Kataguiri que visa instituir a pena de morte e a prisão perpétua. Partindo de uma abordagem qualitativa e exploratória, com base em revisão bibliográfica e análise

no contexto da democracia brasileira contemporânea. Parte-se do reconhecimento de que a circulação intencional de desinformação representa um risco existencial à integridade dos processos democráticos, à confiança pública e à estabilidade institucional.

Abordando a complexidade do tema, o artigo INQUÉRITO POLICIAL E RESQUÍCIOS DO SISTEMA INQUISITÓRIO SOB A ÓTICA DA OBRA “O PROCESSO”, DE FRANZ KAFKA, de autoria de Yasmim Zanuto Leopoldino, tem como objetivo O artigo disserta acerca do livro “O Processo”, de Franz Kafka, que trata da história de Josef K., o qual foi surpreendido com a instauração de procedimento judicial em seu desfavor, cujo objeto não foi elucidado ao acusado em nenhuma oportunidade durante a trama.

Finalmente, o estudo OS LIMITES CONSTITUCIONAIS DA AUTOMAÇÃO DECISÓRIA NO PROCESSO PENAL: UMA ANÁLISE DO JUIZ-ROBÔ À LUZ DA GARANTIA DE JUIZ PREVIAMENTE DETERMINADO, de Gabriel Gaska Nascimento , Jacinto Nelson de Miranda Coutinho, busca O artigo examina a compatibilidade entre a hipótese do juiz-robô autônomo e o princípio do juiz natural no ordenamento constitucional brasileiro. Parte-se da constatação de que a crescente incorporação de sis-temas de inteligência artificial no âmbito judicial, inicialmente voltada à automação de tarefas auxiliares, aproxima-se progressivamente do núcleo da jurisdição, suscitando a indagação sobre a legitimidade de decisões integralmente produzidas por algoritmos.

Por fim, o trabalho PRESUNÇÃO DE INOCÊNCIA E ÔNUS DA PROVA NO PROCESSO PENAL: UMA ANÁLISE DO DELITO DE RECEPTAÇÃO, de autoria de Analiz Bernardon Torre , Martina Leão Gutierrez , Clarice Beatriz da Costa Söhngen, tem como objetivo O artigo analisa a persistência de traços inquisitoriais no processo penal brasileiro, focando na problemática da inversão do ônus da prova no crime de receptação sob a ótica do modelo acusatório e das garantias da Constituição de 1988. Por meio de pesquisa bibliográfica e análise jurisprudencial comparativa entre o STJ e o STF, o estudo objetiva demonstrar que a exigência de que o réu comprove a origem lícita do bem ou a ausência de

crimes de homicídio doloso no Brasil, destacando seus impactos sobre a prevenção criminal e sobre a efetivação do direito fundamental à vida. Parte-se da seguinte problemática: como um país que figura entre os primeiros colocados nos índices globais de violência letal pode enfrentar baixas taxas de esclarecimento de homicídios, evidenciando falhas estruturais nas instituições responsáveis pela investigação e responsabilização penal?.

Desejamos a todos uma excelente leitura e que as reflexões aqui apresentadas contribuam para o avanço crítico das ciências criminais no Brasil.

Matheus Felipe Castro – UNOESC/UFSC

Gustavo Noronha de Ávila – UEM

Flávia Piccinin Paz Gubert - UNESPAR

FRAUDE ELETRÔNICA NO SISTEMA “PIX”: CONCEITO, PRINCÍPIOS, PREVENÇÃO, COMBATE, INVESTIGAÇÃO E RESPONSABILIZAÇÃO PENAL

ELECTRONIC FRAUD IN THE "PIX" SYSTEM: CONCEPT, PRINCIPLES, PREVENTION, COMBAT, INVESTIGATION, AND CRIMINAL LIABILITY

Thiago Braga Parente

Resumo

O presente trabalho aborda o tema da fraude eletrônica praticada por meio do Pix, o sistema de pagamento instantâneo criado pelo Banco Central do Brasil em 2020. Em poucos anos, o Pix passou a ser utilizado por cerca de 80% da população brasileira — e, quase na mesma velocidade, tornou-se alvo preferencial de organizações criminosas que exploram engenharia social, phishing, vishing, clonagem de WhatsApp e acesso não autorizado a dispositivos. O trabalho percorre o marco regulatório, com destaque para a Lei nº 14.155/2021, que introduziu o tipo penal de fraude eletrônica no art. 171, § 2º - A, do Código Penal; analisa o Mecanismo Especial de Devolução (MED) e o seu redesenho como MED 2.0 pela Resolução BCB nº 493/2025; e discute os desafios investigativos, a responsabilidade civil objetiva das instituições financeiras (Súmula 479/STJ) e as perspectivas de aperfeiçoamento do sistema. A metodologia é qualitativa, com revisão bibliográfica, análise doutrinária, exame de jurisprudência e estudo dos normativos do BCB.

Palavras-chave: Golpe do pix, Fraude eletrônica, Mecanismo especial de devolução (med) investigação criminal, Responsabilização penal

Abstract/Resumen/Résumé

This paper addresses the issue of electronic fraud perpetrated through Pix., Brazil's instant payment system created by the Central Bank in 2020. Within a few years, Pix was adopted by approximately 80% of the Brazilian population — and, almost as quickly, became a prime target for criminal organizations exploiting social engineering, phishing, vishing, WhatsApp cloning, and unauthorized device access. The study reviews the regulatory framework,

1- INTRODUÇÃO

O Pix, lançado pelo Banco Central do Brasil (BCB) em novembro de 2020, mudou de forma bastante profunda a maneira como os brasileiros lidam com dinheiro. Em menos de cinco anos, ele se tornou o meio de pagamento mais usado no país, alcançando aproximadamente 80% da população. Disponível a qualquer hora, gratuito para pessoas físicas e capaz de liquidar transações em segundos, o sistema democratizou o acesso ao sistema financeiro — mas também criou oportunidades novas para práticas criminosas que se tornaram, com o tempo, cada vez mais sofisticadas.

Há uma ironia inerente ao mecanismo: a velocidade que faz do Pix um serviço tão conveniente é exatamente a propriedade que o torna arriscado. Uma transação concluída em segundos é, na prática, irreversível pelo usuário. Não existe botão de desfazer. Os criminosos perceberam esse ponto cedo e passaram a explorar técnicas de engenharia social que manipulam psicologicamente as vítimas para as induzir a transferir valores de forma aparentemente voluntária — sem que haja qualquer invasão técnica do sistema bancário. Esse detalhe, paradoxalmente, complica tanto a responsabilização dos autores quanto as tentativas de recuperar o dinheiro perdido.

No campo normativo, o ordenamento jurídico respondeu à altura com a edição da Lei nº 14.155/2021, que criou o tipo penal específico de fraude eletrônica (art. 171, § 2.º-A, do Código Penal), agravou penas para condutas praticadas em ambiente digital e estabeleceu regras de competência processual penal. O BCB, por sua vez, instituiu o Mecanismo Especial de Devolução (MED), depois aprimorado pelo MED 2.0 (Resolução BCB nº 493/2025), voltado ao rastreamento de valores que, com frequência, se pulverizam por múltiplas contas em questão de minutos.

O presente estudo pretende percorrer — de forma organizada, mas sem perder de vista a complexidade do fenômeno — os aspectos conceituais, normativos, investigativos e repressivos da fraude eletrônica vinculada ao Pix, prestando atenção especial ao papel das instituições financeiras, à tensão entre privacidade e interesse público e às perspectivas de evolução desse sistema de combate.

2 - CONCEITO E MODALIDADES DA FRAUDE ELETRÔNICA NO SISTEMA PIX

No direito penal brasileiro, a fraude eletrônica encontra sua definição legal no art. 171, § 2.º-A, do Código Penal, com redação dada pela Lei nº 14.155/2021. O dispositivo tipifica a conduta de obter vantagem ilícita por meio de "artifício, ardil ou qualquer outro meio fraudulento", utilizando dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem violação de mecanismo de segurança ou de acesso a conta bancária.

A doutrina enquadra a fraude eletrônica como espécie do gênero estelionato (art. 171, caput), crime que tem o patrimônio como bem jurídico tutelado. Na modalidade eletrônica, a conduta se caracteriza especialmente pela ausência de contato presencial entre criminoso e vítima, pelo uso de meios informáticos como instrumentos da fraude e pela capacidade de atingir vítimas em escala massiva, algo que o ambiente digital facilita de maneira quase natural (SANTOS, 2025; TRIVINO, 2024).

Vale destacar a distinção em relação ao furto mediante fraude (art. 155, § 4º, II): no estelionato, a vítima é induzida a erro e entrega o bem ao agente de forma ativa; no furto, o bem é subtraído sem que ela perceba no momento da conduta. No universo Pix, a diferença tem relevância prática nos casos em que o criminoso acessa o aplicativo bancário da vítima e realiza a transferência por conta própria, sem qualquer participação ativa dela — situação que pode se enquadrar como furto qualificado ou invasão de dispositivo informático (art. 154-A do CP), a depender das circunstâncias.

O caso a ser estudado aqui é o do "golpe do Pix" que abrange uma série de modus operandi que compartilham o mesmo denominador: a utilização do sistema de pagamento instantâneo como instrumento ou destino de valores fraudulentos. Entre as principais modalidades identificadas pela doutrina e pelos órgãos de segurança pública, destacam-se:

a) *Phishing e smishing:* o criminoso envia mensagens eletrônicas — por e-mail, SMS ou aplicativos de mensagens — simulando comunicações oficiais de bancos, órgãos públicos ou plataformas de comércio eletrônico. Os links contidos nessas mensagens direcionam a vítima para páginas falsas que capturam suas credenciais bancárias. Trata-se de uma das técnicas mais disseminadas no ecossistema de fraudes digitais (TRIVINO, 2024; CONAMP, 2021).

b) *Vishing*: variante vocal do *phishing.* O criminoso liga para a vítima se passando por funcionário de banco, operadora ou autoridade e, mediante engenharia social, a qual induz a vítima a fornecer senhas, tokens ou a realizar transferências Pix para contas sob seu controle.

c) Clonagem de WhatsApp: o agente obtém acesso à conta do aplicativo de mensagens da vítima — por SIM *swap,* captura de código de verificação ou engenharia social — e se passa

por ela para solicitar transferências Pix a seus contatos, normalmente alegando alguma emergência financeira (SANTOS, 2025).

d) Golpe do falso suporte: o criminoso se apresenta como técnico de segurança ou atendente bancário e convence a vítima a instalar aplicativos de acesso remoto (RATs). Com o controle do dispositivo, realiza transferências Pix sem o consentimento da vítima.

e) Golpe do falso comprovante: o fraudador apresenta comprovante de Pix falsificado ou agendado (ainda não efetivado) para induzir a entrega de produto ou serviço sem que o pagamento tenha sido concretizado.

f) Pix sob coação: modalidade associada ao chamado "sequestro relâmpago", em que a vítima é fisicamente forçada a realizar transferências Pix, frequentemente após ter o celular subtraído.

g) Golpe do falso investimento: o agente promete rentabilidade fraudulenta e induz a vítima a transferir valores via Pix para uma suposta aplicação financeira, o que pode caracterizar também pirâmide financeira ou estelionato agravado.

3 - PRINCÍPIOS JURÍDICOS ENVOLVIDOS

A resposta penal às fraudes digitais sempre esbarrou no desafio clássico da anterioridade da norma incriminadora. O art. 1º do Código Penal e o art. 5.º, XXXIX, da Constituição Federal de 1988 consagram o princípio da legalidade: não há crime sem lei anterior que o defina (*nullum crimen, nulla poena sine lege*).

Durante anos, os ilícitos praticados em ambiente digital foram tipificados de forma analógica, com recurso ao estelionato genérico (art. 171, caput) — solução que suscitava debates razoavelmente sérios sobre violação ao princípio da taxatividade.

A Lei nº 14.155/2021 veio preencher essa lacuna ao introduzir tipo penal específico para a fraude eletrônica, encerrando boa parte das discussões sobre enquadramento analógico e conferindo maior segurança jurídica à persecução penal (TJDFT, 2022). Ainda assim, autores como TRIVINO (2024) e membros da CONAMP (2021) advertem que a técnica legislativa adotada — basicamente a adaptação de tipos penais concebidos no século XX — carrega o risco de obsolescência acelerada diante da velocidade com que a tecnologia evolui.

3.1 Princípio da Intervenção Mínima e Proporcionalidade

A criminalização da fraude eletrônica deve ser lida também sob o prisma da intervenção mínima, que reserva o direito penal aos bens jurídicos mais relevantes quando os demais ramos do ordenamento se mostram insuficientes. No caso das fraudes via Pix, a amplitude dos danos patrimoniais e a incapacidade das esferas cível e administrativa de oferecer resposta verdadeiramente dissuasória justificam a tutela penal.

Ao mesmo tempo, a proporcionalidade exige que as penas sejam compatíveis com a gravidade do dano. A Lei nº 14.155/2021 majorou a pena do estelionato eletrônico para reclusão de 4 a 8 anos (art. 171, § 2º-A), bem acima do estelionato simples (1 a 5 anos), o que sinaliza reconhecimento legislativo da maior lesividade da modalidade eletrônica — capaz, em tese, de vitimar milhões de pessoas de forma simultânea e coordenada.

3.2 Princípio da Proteção de Dados e Privacidade

A persecução penal dos crimes digitais coloca em tensão constante dois valores constitucionais: a proteção à privacidade (art. 5º, X e XII, CF) e o interesse público na repressão criminal. A Lei Geral de Proteção de Dados (LGPD — Lei nº 13.709/2018) regula o tratamento de dados pessoais e estabelece bases legais para seu compartilhamento, incluindo o cumprimento de obrigação legal ou regulatória e o atendimento ao poder público (arts. 7.º, II e III).

Nas investigações de fraudes Pix, o acesso a dados bancários, registros de transações e chaves Pix é praticamente indispensável para identificar os autores. Esse acesso, contudo, submete-se ao regime da Lei Complementar nº 105/2001 (sigilo bancário) e exige, em regra, autorização judicial fundamentada.

A exceção, que é a requisição direta pelas autoridades fazendárias nos termos do art. 6.º da LC 105/2001, foi declarada constitucional pelo STF no RE 601.314 (Tema 225). A tensão entre privacidade e interesse público na investigação de crimes digitais é, hoje, um dos pontos mais sensíveis do direito processual penal contemporâneo (TRIVINO, 2024).

4 - O SISTEMA PIX E O MECANISMO ESPECIAL DE DEVOLUÇÃO (MED)

4.1 Arquitetura do Sistema Pix

O Pix é um arranjo de pagamento regulado pelo BCB por meio da Resolução BCB nº 1/2020 (Regulamento do Pix), operacionalizado pelo Sistema de Pagamentos Instantâneos (SPI). Sua estrutura repousa em quatro pilares principais: disponibilidade ininterrupta, 24 horas por dia e 7 dias por semana, inclusive em feriados; liquidação bruta em tempo real; interoperabilidade entre todos os participantes do sistema financeiro; e uso de chaves "Pix" (CPF/CNPJ, e-mail, número de telefone ou chave aleatória) para identificação das contas.

A liquidação imediata e a irreversibilidade da transação são vantagens operacionais inegáveis — mas é justamente isso que cria o ambiente propício à fraude. Uma vez que o valor é creditado na conta do recebedor, o sistema não dispõe de mecanismo automático de cancelamento. O MED foi criado precisamente para tentar contornar essa limitação.

4.2 O Mecanismo Especial de Devolução (MED)

O MED é o conjunto de regras e procedimentos operacionais criado pelo BCB para viabilizar a devolução de um Pix em casos de fraude, golpe ou falha operacional. Regulamentado inicialmente pela Resolução BCB nº 103/2021, o mecanismo funciona como uma espécie de trava de segurança pós-transacional: ao ser acionado, permite ao banco do pagador solicitar o bloqueio cautelar dos valores na conta do recebedor enquanto a suspeita de fraude é apurada.

O fluxo do MED segue etapas padronizadas: a vítima registra contestação junto à instituição de origem em até 80 dias corridos da transação; o banco pagador notifica o banco recebedor em até 30 minutos; o banco recebedor realiza o bloqueio cautelar; as instituições têm até 11 dias para análise conjunta; confirmada a fraude, a devolução deve ocorrer em até 96 horas. Se a conta estiver sem saldo, o banco recebedor monitora entradas por até 90 dias na tentativa de recuperação parcial.

Os dados são reveladores da escala do problema: em 2022, foram registradas 1,5 milhão de solicitações de devolução pelo MED; em 2023, 2,5 milhões; em 2024, quase 5 milhões — crescimento de 98% em apenas um ano. Os prejuízos chegaram a R$ 4,9 bilhões em 2023, alta de 70% frente ao ano anterior. Apesar disso, apenas 31% dos pedidos de 2024 foram aprovados total ou parcialmente, e o valor efetivamente recuperado representou somente 9% do total contestado. Os números revelam um mecanismo que, na sua configuração original, estava claramente aquém das necessidades.

4.3 O MED 2.0 e a Resolução BCB nº 493/2025

Em agosto de 2025, o BCB publicou a Resolução BCB nº 493, Foi criado o MED 2.0, que representa o aperfeiçoamento significativo do sistema de recuperação de valores. A principal novidade é a modalidade de "Recuperação de Valores", que permite o rastreamento e bloqueio de recursos suspeitos não apenas na conta de destino da transação original, mas também em transferências subsequentes. O BCB denomina essa funcionalidade de "rastreamento de rotas".

O MED 2.0 permite o rastreamento em até cinco transferências subsequentes, em um período de até 11 dias adicionais após a contestação. O que antes era facultativo para as instituições financeiras torna-se obrigatório a partir de 2 de fevereiro de 2026. Complementarmente, a Instrução Normativa BCB nº 589 regulamentou o "botão de contestação", disponível nos aplicativos bancários desde outubro de 2025, que permite à vítima registrar a contestação diretamente pelo autoatendimento.

A lógica por trás do MED 2.0 parte de um diagnóstico preciso: o dinheiro oriundo de golpes é rapidamente "pulverizado" — distribuído em cascata por múltiplas contas — como estratégia dos grupos criminosos para dificultar o rastreamento. O novo mecanismo tenta acompanhar esse fluxo, aumentando substancialmente as chances de recuperação. Se vai funcionar na prática, só os dados dos próximos meses dirão.

5 - DESAFIOS NO ENFRENTAMENTO DA FRAUDE ELETRÔNICA

5.1 Velocidade Tecnológica versus Rigidez Normativa

O principal desafio estrutural no combate às fraudes digitais é o gap temporal entre a evolução das técnicas criminosas e a capacidade de resposta do ordenamento jurídico. Enquanto o legislador redige e aprova normas, os criminosos já desenvolveram novos vetores de ataque. A Lei nº 14.155/2021, aplaudida como avanço quando de sua aprovação, já dá sinais de insuficiência diante de modalidades emergentes — como o uso de inteligência artificial para clonagem de voz (*deepfake* de áudio) em golpes de *vishing,* ou a exploração do próprio MED como instrumento de fraude reversa, situação em que o criminoso aciona o mecanismo de devolução de forma fraudulenta para recuperar valores de transações legítimas (SANTOS, 2025).

5.2 Anonimato e Jurisdição Digital

Identificar os autores de fraudes digitais é uma tarefa obstaculizada por múltiplos fatores: o uso de VPNs para mascarar endereços IP; a utilização de contas abertas com documentos falsos ou de "laranjas" — pessoas que emprestam ou vendem suas contas; a rápida pulverização dos valores entre múltiplas contas em diferentes instituições; e o eventual envolvimento de servidores no exterior, o que cria problemas de jurisdição e exige cooperação jurídica internacional via MLATs.

A Operação *Per Saltum*, deflagrada pela Polícia Civil de São Paulo em 2022, ilustra bem essa complexidade: identificou organização criminosa que combinava *phishing, vishing* e engenharia social para fraudar contas de municípios, com células especializadas em funções distintas — captação de dados, lavagem de dinheiro, cooptação de correntistas e ataques a entes públicos. A investigação evidenciou que as medidas assecuratórias concebidas em 1941 ainda não acompanharam a dinâmica da criminalidade financeira digital.

5.3 Prova Digital e Cadeia de Custódia

A produção probatória em crimes cibernéticos exige conhecimento técnico especializado e observância rigorosa dos protocolos de preservação da cadeia de custódia (arts. 158-A a 158-F do CPP, incluídos pela Lei nº 13.964/2019). Logs de acesso, registros de transações, metadados de mensagens eletrônicas, endereços IP e histórico de chaves Pix constituem elementos probatórios que, se colhidos sem o procedimento técnico adequado, podem ter sua validade jurídica comprometida — o que, na prática, pode inviabilizar a persecução.

A coleta dessas evidências demanda peritos em computação forense cuja disponibilidade nas unidades de polícia judiciária estadual ainda é insuficiente em relação à demanda, especialmente nas regiões Norte e Nordeste. Esse déficit estrutural compromete a efetividade da persecução penal e, indiretamente, alimenta a sensação de impunidade que retroalimenta a criminalidade digital.

5.4 Privacidade, Sigilo Bancário e Interesse Público

A investigação de fraudes Pix colide de frente com o regime da LGPD e com a Lei Complementar nº 105/2001. O acesso a informações de transações, titulares de chaves Pix e registros de movimentação financeira é indispensável para identificar os autores — mas só pode ser realizado, em regra, mediante autorização judicial prévia.

A questão se torna especialmente delicada quando envolve dados de terceiros que aparecem na cadeia transacional sem serem os perpetradores da fraude — os "laranjas" ou titulares de contas utilizadas como "passagem" de valores. Nesses casos, o compartilhamento de dados com as autoridades de segurança pública deve observar os princípios da necessidade, finalidade e proporcionalidade previstos na LGPD (art. 7.º, VI, e art. 23). O interesse público na repressão criminal deve ser ponderado com o direito fundamental à privacidade, sob controle judicial.

6 - PREVENÇÃO E EDUCAÇÃO DIGITAL

6.1 Prevenção no Nível Individual

A prevenção primária das fraudes via Pix começa na educação do usuário para o reconhecimento das técnicas de engenharia social. As medidas protetivas recomendadas pelo BCB, pela FEBRABAN e por especialistas em segurança da informação incluem: jamais fornecer senhas, tokens ou códigos de verificação por telefone; verificar a identidade do recebedor antes de confirmar qualquer transferência; ativar a autenticação em dois fatores nos aplicativos bancários e de mensagens; configurar limites reduzidos para transações noturnas; e conferir o extrato bancário para confirmar o crédito antes de entregar produtos ou serviços.

Essas medidas são simples, mas a sua efetividade depende de um nível de alfabetização digital que ainda está longe de ser universalizado no Brasil — o que torna a educação financeira e digital não apenas desejável, mas necessária como política pública.

6.2 Prevenção no Nível Institucional

As instituições financeiras ocupam posição central na prevenção. O BCB impõe aos participantes do sistema Pix obrigações de monitoramento de transações atípicas e adoção de mecanismos de detecção de comportamentos suspeitos. Entre as medidas institucionais de

destaque estão os sistemas de análise comportamental baseados em inteligência artificial e machine learning, capazes de identificar padrões incompatíveis com o perfil histórico do correntista; controles de *onboarding* que dificultem a abertura de contas com documentos falsos; e políticas de comunicação proativa ao cliente sobre tentativas de golpe em curso.

O marco regulatório da Política Nacional de Cibersegurança (PNCiber) e as determinações do BCB sobre gerenciamento de riscos operacionais também impõem obrigações de resposta a incidentes e de reporte ao regulador, compondo um sistema de governança que complementa as ações preventivas individuais.

7 - INVESTIGAÇÃO CRIMINAL E DESCOBERTA DE AUTORES

7.1 Órgãos e Estruturas de Investigação

A persecução penal dos crimes cibernéticos, incluindo as fraudes Pix, é atribuição das polícias judiciárias — Polícia Federal, quando há bens, serviços ou interesses da União envolvidos, e Polícias Civis estaduais nas demais hipóteses. Em vários estados, foram criadas delegacias especializadas em crimes cibernéticos (NUCIBER, DRCI e equivalentes), com estrutura técnica voltada especificamente para o ambiente digital.

Com a edição do §4º do art. 70 do CPP, incluído pela Lei nº 14.155/2021, a competência para processar e julgar o estelionato eletrônico praticados mediante fraude eletrônica/bancária, no Brasil, passou a ser o do domicílio do domicílio da vítima. Esse entendimento foi consolidado pelo STJ no julgamento do CC 180832-RJ e o CC 185983-DF, e superando o entendimento Súmulas 521 do STF e 244 do STJ.

A modificação legislativa buscou dar efetividade na persecução penal e facilitar o acesso da vítima à justiça, evitando deslocamentos desnecessários e complexidades processuais. Além disso, é uma regra relevante, tendo em vista necessidade de que seja evitado vítima precise litigar no foro do golpista, dificilmente identificado a *priori*.

7.2 Técnicas de Investigação Digital

A identificação dos autores de fraudes Pix combina técnicas tradicionais de investigação com métodos especializados de computação forense. Os procedimentos mais relevantes

incluem: requisição de dados cadastrais e registros de transações junto às instituições financeiras, mediante autorização judicial; análise de logs de acesso e metadados de conexão com pedido de quebra de sigilo telemático; uso de OSINT (*Open Source Intelligence*) para coleta de informações publicamente disponíveis em redes sociais e bases abertas; interceptação telemática (Lei nº 9.296/1996), mediante autorização judicial; e infiltração policial em ambientes digitais, com debate doutrinário ainda aberto sobre sua extensão às redes online.

O rastreamento de chaves Pix é uma das ferramentas mais eficazes disponíveis: por meio do CPF, CNPJ, e-mail ou número de telefone vinculado à chave receptora, é possível identificar o titular da conta beneficiária. Contudo, criminosos frequentemente utilizam contas de laranjas ou documentos fraudulentos, o que obriga a investigação a se aprofundar na cadeia de transferências subsequentes.

7.3 Prova por Identificação em Ambiente Digital

Em crimes cibernéticos, a identificação do autor frequentemente resulta de uma convergência de evidências indiretas: dados cadastrais da conta receptora, endereço IP de acesso ao sistema bancário, histórico de transações da conta suspeita, registros de geolocalização do dispositivo e comunicações eletrônicas obtidas via interceptação judicial. A soma desses elementos permite a formação de prova circunstancial robusta, suficiente para embasar denúncia e eventual condenação.

Em casos que envolvem organizações criminosas, o art. 3.º da Lei nº 12.850/2013 autoriza meios investigativos adicionais, como a colaboração premiada, a captação ambiental de sinais eletromagnéticos e a infiltração policial. Aplicados ao ambiente digital, esses instrumentos ampliam significativamente o poder investigativo do Estado — mas exigem, em contrapartida, controle judicial rigoroso para que não degenerem em abusos.

8 - O PAPEL DAS INSTITUIÇÕES FINANCEIRAS: RESPONSABILIDADE CIVIL E DEVERES REGULATÓRIOS

A responsabilidade civil das instituições financeiras por danos decorrentes de fraudes praticadas por terceiros no âmbito de operações bancárias está sedimentada na Súmula nº 479 do STJ: "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias."

O fundamento jurídico repousa na teoria do risco da atividade e na aplicação do Código de Defesa do Consumidor (CDC), Lei nº 8.078/1990), em especial seus arts. 14, §1º, o qual trata do defeito na prestação de serviços, combinado com a Súmula 297 do STJ. A qualificação do fortuito como interno decorre da compreensão de que os riscos inerentes à atividade bancária, incluindo fraudes de terceiros, integram o modelo de negócio da instituição e não constituem causa excludente de responsabilidade.

Em outubro de 2025, o STJ consolidou orientação específica sobre o golpe da falsa central de atendimento: o ministro Ricardo Villas Bôas Cueva reafirmou que a responsabilidade objetiva das instituições abrange os casos em que a fraude é viabilizada por falha na segurança dos sistemas ou pela validação de operações atípicas, alheias ao perfil do correntista, sem que a instituição tenha adotado medidas preventivas adequadas.

Há, contudo, uma mitigação jurisprudencial relevante: a responsabilidade bancária pode ser afastada quando demonstrada culpa exclusiva do consumidor, no caso em que a vítima, por negligência grave, forneceu voluntariamente seus dados a terceiros em contexto que afastaria a responsabilidade da instituição. Esse é um ponto ainda controvertido, especialmente quanto à extensão da culpa concorrente como fator de redução da indenização.

Ademais, além da responsabilidade civil, as instituições financeiras submetem-se a deveres regulatórios impostos pelo BCB, que incluem: implantação de sistemas de detecção de fraudes em tempo real com bloqueio automático de transações atípicas; mecanismos de autenticação robusta em operações de maior valor ou perfil incomum; participação obrigatória no MED e, a partir de fevereiro de 2026, no MED 2.0; reporte de incidentes ao BCB; e programas de educação financeira e comunicação proativa ao cliente.

A abertura de contas com verificação insuficiente de identidade é o motivo de responsabilização nesse caso, pois é o mecanismo que permite a criação de contas de laranjas usadas para receber e pulverizar valores fraudulentos. O Informativo Extraordinário nº 29 do STJ (2026) consolidou o entendimento de que a validação de operações suspeitas, atípicas e alheias ao perfil do correntista configura defeito na prestação do serviço bancário, ensejando reparação de danos materiais e morais.

9- REPRESSÃO PENAL: MARCO NORMATIVO E JURISPRUDÊNCIA

9.1 A Lei nº 14.155/2021 e o Tipo Penal de Fraude Eletrônica

A Lei nº 14.155/2021, publicada em 27 de maio de 2021, é o principal marco normativo penal no combate às fraudes digitais. Suas alterações mais relevantes foram as seguintes:

a) Art. 171, § 2º-A, do CP (fraude eletrônica): pena de reclusão de 4 a 8 anos e multa para o estelionato cometido mediante utilização de redes sociais, contatos telefônicos, correio eletrônico fraudulento ou qualquer outro meio fraudulento análogo. A pena é agravada se o crime é cometido com servidor ou infraestrutura digital no exterior (§ 2º-B: acréscimo de até 2/3).

b) Art. 154-A, § 1º, do CP (invasão de dispositivo informático): pena agravada para reclusão de 1 a 4 anos (antes era de 3 meses a 1 ano), com majorante de 2/3 se a invasão resultar em prejuízo econômico.

c) Art. 155, § 4º-B, do CP (furto por dispositivo eletrônico): reclusão de 4 a 8 anos e multa para o furto cometido mediante utilização de dispositivo eletrônico ou informático.

d) Art. 70, § 4º, do CPP (competência): nos crimes de estelionato cometidos por redes sociais, contatos telefônicos ou e-mail, a competência é do foro do local onde a vítima efetuou a transferência, ou do seu domicílio.

Sobre o tema, o STJ tem construído importante acervo jurisprudencial sobre a fraude eletrônica. Entre os posicionamentos mais relevantes estão: a distinção entre furto mediante fraude (art. 155, § 4.º, II) e estelionato eletrônico (art. 171, § 2.º-A), centrada no papel ativo ou passivo da vítima; a aplicação imediata da regra de competência do art. 70, § 4.º, como norma processual de eficácia imediata; e a possibilidade de aplicação cumulativa da causa de aumento prevista no art. 171, § 4.º (vítima idosa ou vulnerável).

A jurisprudência estadual tem confirmado a tipicidade de golpes de *WhatsApp*, falsa central de atendimento, *phishing* e clonagem de aplicativos bancários no art. 171, § 2.º-A. O debate doutrinário mais vivo ainda diz respeito às hipóteses em que a vítima não fornece dados ativamente, mas é induzida a realizar a transferência — situação em que o papel da vítima é central para definir o enquadramento típico entre estelionato e furto.

Quanto à tipificação do crime do "golpe do Pix" e suas penas, é possível sintetizar o assunto seguinte forma: o estelionato eletrônico em sua forma básica (art. 171, §2º-A) prevê reclusão de 4 a 8 anos e multa; se praticado contra idoso ou vulnerável (art. 171, § 4.º), a pena é aumentada de 1/3 ao dobro; se cometido com infraestrutura digital no exterior (art. 171, § 2º-B), há acréscimo de até 2/3; e se praticado por organização criminosa (art. 2.º, §4.º, Lei nº 12.850/2013), há agravamento adicional. Em todas as hipóteses, são cabíveis medidas

cautelares reais sobre valores e bens adquiridos com o produto do crime, nos termos dos arts. 125 e seguintes do CPP.

10 - PERSPECTIVAS E PROPOSTAS DE APERFEIÇOAMENTO

A análise do ecossistema de combate às fraudes Pix revela três eixos prioritários de aperfeiçoamento: normativo, institucional e tecnológico. No plano normativo, é necessária a revisão da legislação penal para incorporar modalidades emergentes — como o uso de inteligência artificial generativa para *deepfakes* de voz e vídeo em golpes de *vishing* — sem recorrer à analogia vedada pelo princípio da legalidade.

Uma lei específica sobre investigação de crimes cibernéticos, com disciplina clara dos poderes do Estado em ambiente digital e das garantias dos investigados, poderia superar a atual fragmentação normativa.

No plano institucional, é urgente criar e fortalecer delegacias especializadas em crimes cibernéticos em todas as unidades federativas, com orçamento adequado para peritos em computação forense e capacitação permanente de delegados e investigadores. A cooperação entre o BCB, a ANPD, as polícias judiciárias e o Ministério Público deveria ser formalizada em protocolos que permitam o compartilhamento ágil de informações financeiras sem prejuízo das garantias individuais.

No plano tecnológico, o aprimoramento dos sistemas de detecção de fraudes pelas instituições financeiras, com uso de inteligência artificial para análise comportamental, e a implementação plena do MED 2.0 são os instrumentos mais imediatos disponíveis mais modernos. A médio prazo, mecanismos robustos de identidade digital (biometria, autenticação multifator resistente a *phishing*) para abertura de contas e realização de transações de maior valor poderão reduzir significativamente o problema das contas de laranjas.

11- CONCLUSÃO

O “golpe do Pix” é expressão bastante ilustrativa de como a aceleração tecnológica pode subverter a lógica de sistemas projetados para beneficiar a sociedade, convertendo suas próprias virtudes — velocidade, ubiquidade e acessibilidade — em vetores de risco. O fenômeno demanda resposta multidimensional, que articule prevenção, repressão e reparação em um sistema coerente e minimamente eficaz.

A Lei nº 14.155/2021 representou avanço normativo real, ao introduzir tipo penal específico para a fraude eletrônica e majorar penas para crimes cometidos em ambiente digital. A efetividade da repressão penal, porém, ainda é limitada pela insuficiência das estruturas investigativas, pela dificuldade de identificar autores no ambiente digital e pela velocidade com que as técnicas fraudulentas evoluem. O risco de obsolescência legislativa é concreto e demanda postura proativa do legislador.

No plano civil, a consolidação da responsabilidade objetiva das instituições financeiras pela Súmula 479 do STJ representa garantia importante para as vítimas — mas não pode substituir o investimento das próprias instituições em medidas preventivas robustas, que são, em última análise, muito mais eficazes do que a reparação a posteriori.

O MED e sua evolução para o MED 2.0 demonstram que o BCB assumiu protagonismo regulatório no combate às fraudes, mas os dados de recuperação de apenas 9% dos valores contestados em 2025 revelam que o caminho ainda é longo. A tensão entre privacidade e interesse público na investigação criminal permanece como questão constitucional não inteiramente resolvida, exigindo equilíbrio permanente sob supervisão judicial.

Em síntese, o enfrentamento eficaz do "golpe do Pix" exige mais do que resposta penal: requer a construção de um ecossistema de segurança financeira digital que envolva Estado, instituições financeiras, usuários e sociedade civil em uma arquitetura colaborativa, orientada pela proteção da dignidade humana e do patrimônio das pessoas que dependem do sistema de pagamentos instantâneos para conduzir sua vida cotidiana.

REFERÊNCIAS

BANCO CENTRAL DO BRASIL. **Mecanismo Especial de Devolução (MED) — Aprimoramentos: MED 2.0**. Apresentação no Circuito Pix. Brasília: BCB, 2025. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/pix/MED/MED_2-0_Circuito_Pix-Dia_1.pdf. Acesso em: maio 2025.

BANCO CENTRAL DO BRASIL. **Guia de implementação dos procedimentos de devolução no Pix, com ênfase no Mecanismo Especial de Devolução** — versão 4.1. Brasília: BCB, 2025. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/pix/Guia_MED.pdf. Acesso em: maio 2025.

BANCO CENTRAL DO BRASIL. Resolução BCB nº 1, de 12 de agosto de 2020. Institui o Pix e aprova o Regulamento do Pix. Brasília: BCB, 2020.

BANCO CENTRAL DO BRASIL. Resolução BCB nº 103, de junho de 2021. Estabelece o Mecanismo Especial de Devolução no âmbito do Pix. Brasília: BCB, 2021.

BANCO CENTRAL DO BRASIL. Resolução BCB nº 493, de agosto de 2025. Institui aprimoramentos ao Mecanismo Especial de Devolução (MED 2.0). Brasília: BCB, 2025.

BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Brasília: Presidência da República, 1940. Arts. 154-A, 171, §§ 2.º-A e 2.º-B incluídos pela Lei nº 14.155/2021.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Torna mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; altera o Código Penal e o Código de Processo Penal. Brasília: Presidência da República, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: Presidência da República, 2018.

BRASIL. Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras. Brasília: Presidência da República, 2001.

BRASIL. Lei nº 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção de prova, infrações penais correlatas e o procedimento criminal. Brasília: Presidência da República, 2013.

CONAMP — ASSOCIAÇÃO NACIONAL DOS MEMBROS DO MINISTÉRIO PÚBLICO. Lei nº 14.155/2021 dos crimes cibernéticos. Artigo de Sauvei Lai. Rio de Janeiro: CONAMP, 2021. Disponível em: https://www.conamp.org.br/publicacoes/artigos-juridicos/8468-lei-14-155-2021-dos-crimes-ciberneticos.html. Acesso em: maio 2025.

SANTOS, Maiza Silva. A fraude eletrônica como nova modalidade de estelionato. *Dissertação (Mestrado em Direito)* — Universidade Nove de Julho, São Paulo, 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Súmula nº 479**. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Brasília: STJ, 2012.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Súmula nº 297**. O Código de Defesa do Consumidor é aplicável às instituições financeiras. Brasília: STJ, 2004.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Informativo de Jurisprudência Extraordinário nº 29** — 20 janº 2026. Responsabilidade de bancos e instituições de pagamento por golpes que viabilizam fraudes. Brasília: STJ, 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. AgInt no AREsp 2.690.893/DF. Decisão de 17 fev. 2025. Fraude bancária. Responsabilidade. Súmula 479/STJ. Brasília: STJ, 2025.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS (TJDFT). O novo crime de fraude eletrônica e o princípio da legalidade. Brasília: TJDFT, 2022. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade. Acesso em: maio 2025.

TRIVINO, Aline Melsone Marcondes. Crimes cibernéticos: como a nova tecnologia desafia o direito penal brasileiro. *Dissertação (Mestrado em Direito Penal)* — Pontifícia Universidade Católica de São Paulo, São Paulo, 2024.

ALMEIDA, Ruanh Neres de. [Título do artigo]. Artigo científico. Pontifícia Universidade Católica de Goiás, Goiânia, 2024.

POLÍCIA CIVIL DO ESTADO DE SÃO PAULO. Operação Per Saltum — quadrilha que usou Pix para roubar prefeituras de SP e MG. Notícia de 18 out. 2022. São Paulo, 2022.

DATARUDDER. MED PIX: o Mecanismo Especial de Devolução. Análise e dados. 2025. Disponível em: https://datarudder.com/med-pix/. Acesso em: maio 2025.

REVISTAIFT. Crimes cibernéticos: fraude eletrônica e a efetividade da legislação brasileira. Disponível em: https://revistaft.com.br/crimes-ciberneticos-fraude-eletronica-e-a-efetividade-da-legislacao-brasileira/. Acesso em: maio 2025.