

A nova repressão penal aos golpes digitais: análise crítica da Lei nº 15.397/2026 e seus impactos nos crimes patrimoniais digitais

The new criminal repression of digital scams: a critical analysis of Law nº 15.397/2026 and its impacts on digital property crimes

Erinaldo Alves dos Santos¹, Letícia Pordeus Ferreira², Beatriz de Oliveira Matos³, Lourival Antônio Simões de Farias⁴, Davi Dantas Alves⁵, Rose Jenniffer Lopes Leandro⁶, Ivanessa Sousa Videres de Sena⁷ e Ciro Pereira Batista⁸

v. 14/ n. 3 (2026)
Julho/Setembro

Aceito para publicação em 16/06/2026.

¹Doutorando em Planejamento e Dinâmicas Territoriais no Semiárido pela Universidade do Estado do Rio Grande do Norte, Pau dos Ferros, Rio Grande do Norte. ORCID: 0009-0008-6108-2691. E-mail:

erinaldoasantos9@gmail.com;

²Graduada em Direito pela Universidade Federal de Campina Grande, Sousa, Paraíba. ORCID: 0009-0007-9518-3215. E-mail: leticiapordeus01@gmail.com;

³Graduada em Direito pela Universidade Federal de Campina Grande, Sousa, Paraíba. ORCID: 0009-0006-9948-3859. E-mail: beatrizomatos@hotmail.com;

⁴Mestre em Sistemas Agroindustriais pela Universidade Federal de Campina Grande, Pombal, Paraíba. ORCID: 0009-0006-7187-8488. E-mail: farias.lourival@hotmail.com;

⁵Doutorando em Ciências Sociais pela Universidade Federal do Rio Grande do Norte, Natal, Rio Grande do Norte. ORCID: 0000-0003-3324-9075. E-mail: davipb70@gmail.com;

⁶Especialista em Direitos Humanos e Pluralidades pela Universidade Federal de Campina Grande, Sousa, Paraíba. ORCID: 0009-0003-3287-1118. E-mail: roselopes.advocacia@gmail.com;

⁷Professor da Faculdade Gilgal, Sousa, Paraíba. ORCID: 0009-0004-9936-3641. E-mail: isena.advocacia@gmail.com;

⁸Graduado em Direito pela Universidade Federal de Campina Grande, Sousa, Paraíba. ORCID: 0009-0002-8156-1055. E-mail: pereiraciro95@gmail.com.

<https://www.gvaa.com.br/revista/index.php/RDG>

RESUMO: O presente artigo analisa criticamente a Lei nº 15.397/2026 e seus impactos sobre os crimes patrimoniais digitais, especialmente furto mediante fraude eletrônica, furto e roubo de aparelhos celulares, estelionato eletrônico, cessão de conta bancária para trânsito de recursos ilícitos, receptação e fraudes bancárias. O problema de pesquisa consiste em verificar se a majoração de penas nos crimes patrimoniais digitais representa medida penal eficaz ou manifestação de Direito Penal simbólico. A pesquisa adota abordagem qualitativa, bibliográfica, documental e jurídico-dogmática, com método dedutivo e análise crítico-político-criminal da legislação penal, da doutrina, da jurisprudência e de dados institucionais. Utilizam-se como fontes normativas o Código Penal, o Código de Processo Penal, a Lei nº 14.155/2021 e a Lei nº 15.397/2026, além de dados do DataSenado, da Febraban, do Banco Central do Brasil e do Anuário Brasileiro de Segurança Pública. Conclui-se que a Lei nº 15.397/2026 representa atualização normativa relevante ao reconhecer a centralidade dos dispositivos eletrônicos, das fraudes digitais e das contas intermediárias na criminalidade patrimonial contemporânea. Todavia, a elevação abstrata de penas não enfrenta, isoladamente, a estrutura econômica, tecnológica e probatória dos golpes digitais. A eficácia da nova lei depende de investigação especializada, rastreabilidade financeira, bloqueio célere de ativos, cooperação bancária, integração de bases de dados, proteção das vítimas e respeito aos limites constitucionais da culpabilidade, proporcionalidade e intervenção mínima.

Palavras-chave: crimes patrimoniais digitais; Lei nº 15.397/2026; estelionato eletrônico; conta laranja; Direito Penal simbólico.

ABSTRACT: This article critically analyzes Law No. 15,397/2026 and its impacts on digital property crimes, especially electronic fraud theft, theft and robbery of mobile phones, electronic fraud, the assignment of bank accounts for the transfer of illicit funds, receiving stolen goods, and banking fraud. The research problem is to determine whether the increase in penalties for digital property crimes constitutes an effective criminal policy measure or a manifestation of symbolic criminal law. The study adopts a qualitative, bibliographic, documentary, and legal-dogmatic approach, using a deductive method and a critical criminal-policy analysis of criminal legislation, legal doctrine, case law, and institutional data. The normative sources include the Brazilian Penal Code, the Code of Criminal Procedure, Law No. 14,155/2021, and Law No. 15,397/2026, as well as institutional data from DataSenado, Febraban, the Central Bank of Brazil, and the Brazilian Public Security Yearbook. The article concludes that Law No. 15,397/2026 is a relevant normative update, as it recognizes the central role of electronic devices, digital fraud, and intermediary bank accounts in contemporary property crimes. However, the abstract increase in penalties does not, by itself, confront the economic, technological, and evidentiary structure of digital scams. The effectiveness of the new law depends on specialized investigation, financial traceability, rapid asset freezing, banking cooperation, database integration, victim protection, and respect for constitutional limits such as culpability, proportionality, and minimum

criminal intervention.

Keywords: digital property crimes; Law No. 15,397/2026; electronic fraud; mule accounts; symbolic criminal law.

1 CONSIDERAÇÕES INICIAIS

A criminalidade patrimonial brasileira passa por uma transformação que não pode ser compreendida apenas como deslocamento de delitos tradicionais para a internet. O furto, o roubo, a receptação e o estelionato continuam sendo categorias penais centrais, mas a sua execução prática foi reorganizada por ecossistemas digitais, financeiros e comunicacionais. O patrimônio da vítima já não é atingido apenas pela subtração física de um bem ou pela fraude presencial: ele pode ser vulnerado por phishing, falsas centrais bancárias, clonagem de aplicativos de mensagem, engenharia social, manipulação de dados pessoais, transferências instantâneas, contas intermediárias e exploração posterior de celulares subtraídos.

Essa mutação é empiricamente perceptível. Pesquisa divulgada pelo DataSenado em 2024 apontou que 24% dos brasileiros com mais de 16 anos declararam ter perdido dinheiro, nos 12 meses anteriores, em razão de algum crime cibernético, incluindo clonagem de cartão, fraude na internet ou invasão de contas bancárias. Em números absolutos, a estimativa indicada foi superior a 40,85 milhões de pessoas. O mesmo levantamento ressaltou que não há perfil socioeconômico claro das vítimas, o que indica fenômeno distribuído de modo amplo na população brasileira (Senado Federal, 2024).

No mesmo sentido, o Anuário Brasileiro de Segurança Pública de 2025 registrou 2.166.552 estelionatos no Brasil em 2024, com crescimento de 7,8% em relação a 2023. Os estelionatos por meio eletrônico chegaram a 281.206 registros, com crescimento de 17%. O relatório também observa que, enquanto os roubos diminuíram, os estelionatos se consolidaram como nova tendência dos crimes patrimoniais no país (Fórum Brasileiro de Segurança Pública, 2025).

A expansão das transações financeiras digitais amplia a superfície de risco. A Pesquisa Febraban de Tecnologia Bancária de 2026 indica que o setor bancário brasileiro alcançou 240,8 bilhões de transações em 2025, com forte protagonismo dos canais digitais e do mobile banking. O Pix com movimentação financeira pelo mobile banking atingiu 29,419 bilhões de transações em 2025, crescimento de 19% em relação a 2024 (FEBRABAN; Deloitte, 2026). Esses dados não significam que a digitalização bancária seja causa do crime, mas demonstram que a vida patrimonial se deslocou para ambientes nos quais rapidez, escala, interoperabilidade e autenticação remota se tornaram elementos essenciais.

É nesse cenário que se insere a Lei nº 15.397, de 30 de abril de 2026. A norma alterou o Código Penal para majorar penas de furto, roubo, estelionato, receptação e interrupção ou perturbação

de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública. Também tratou da receptação de animal doméstico e de fraudes vinculadas ao ambiente bancário (Brasil, 2026). No campo dos crimes patrimoniais digitais, destacam-se a elevação da pena do furto mediante fraude eletrônica, a previsão mais severa para subtração de celular, computador, tablet ou dispositivo eletrônico semelhante, a ampliação da fraude eletrônica e a criminalização da cessão de conta bancária para trânsito de recursos destinados ao financiamento de atividade criminosa ou dela provenientes.

O problema de pesquisa deste artigo é o seguinte: o aumento de pena nos crimes patrimoniais digitais representa medida penal eficaz para enfrentar golpes digitais ou configura manifestação de Direito Penal simbólico?

A hipótese sustentada é que a Lei nº 15.397/2026 possui relevância dogmática e político-criminal ao atualizar parcialmente a resposta penal diante da criminalidade patrimonial digital, mas sua eficácia preventiva será limitada se permanecer isolada de medidas estruturais de prevenção, investigação tecnológica, cooperação bancária, bloqueio célere de valores, rastreabilidade financeira, integração de bases de dados e proteção das vítimas. A simples elevação abstrata de penas tende a produzir resposta simbólica quando o Estado substitui capacidade investigativa e política pública por endurecimento legislativo.

O objetivo geral consiste em analisar criticamente os impactos da Lei nº 15.397/2026 nos crimes patrimoniais digitais. Como objetivos específicos, pretende-se examinar a digitalização dos crimes patrimoniais, comparar a Lei nº 15.397/2026 com o regime anterior e com a Lei nº 14.155/2021, analisar dogmaticamente furto eletrônico, estelionato eletrônico, conta laranja, receptação e subtração de celulares, discutir dados empíricos sobre golpes digitais e avaliar os limites constitucionais da nova repressão penal.

A justificativa é jurídica, social e político-criminal. Jurídica, porque a reforma altera categorias clássicas dos crimes contra o patrimônio. Social, porque golpes digitais e subtrações de celulares atingem milhões de vítimas e geram perdas que extrapolam o valor econômico imediato. Político-criminal, porque a efetividade do Direito Penal depende menos da severidade abstrata da pena e mais da capacidade estatal de prevenir, investigar, bloquear valores, recuperar ativos e responsabilizar proporcionalmente os agentes envolvidos.

2 METODOLOGIA

A pesquisa possui natureza qualitativa, bibliográfica, documental e jurídico-dogmática. Adota-se o método dedutivo, partindo-se da análise da função do Direito Penal em um Estado

Democrático de Direito para examinar a resposta legislativa específica aos crimes patrimoniais digitais. A investigação combina análise normativa, doutrinária, jurisprudencial e empírica.

A pesquisa bibliográfica utiliza doutrina penal recente e materiais acadêmicos sobre proteção de bens jurídicos, intervenção mínima, culpabilidade, proporcionalidade, expansão penal, ação penal, competência e crimes contra o patrimônio. A pesquisa documental examina o Código Penal, o Código de Processo Penal, a Lei nº 12.965/2014, a Lei nº 13.709/2018, a Lei nº 14.155/2021 e a Lei nº 15.397/2026.

A análise empírica utiliza fontes institucionais, especialmente DataSenado, Febraban, Banco Central do Brasil e Fórum Brasileiro de Segurança Pública. A metodologia também se apoia em análise crítico-político-criminal, pois o objetivo não é apenas descrever alterações legislativas, mas avaliar se a resposta penal adotada é compatível com a estrutura real dos golpes digitais.

Não se pretende medir causalmente o impacto da Lei nº 15.397/2026, até porque a sua vigência é recente e ainda não há série histórica suficiente para aferir efeitos práticos. O que se propõe é avaliar se o desenho normativo da reforma é coerente com a dinâmica dos crimes patrimoniais digitais e com os limites constitucionais da responsabilidade penal.

3 A DIGITALIZAÇÃO DOS CRIMES PATRIMONIAIS

Os crimes patrimoniais digitais apresentam uma característica decisiva: a separação entre o momento da manipulação da vítima, a movimentação financeira e o beneficiário final da vantagem ilícita. Em golpes por aplicativos de mensagem, falsa central bancária ou phishing, o agente que fala com a vítima pode não ser o titular da conta recebedora; o titular da conta pode não ser o idealizador do golpe; o sacador ou transferidor subsequente pode atuar apenas em uma etapa de dispersão; e o beneficiário final pode permanecer oculto por sucessivas transferências.

Essa fragmentação explica por que a resposta penal tradicional, centrada apenas no autor imediato da fraude, mostra-se insuficiente. A criminalidade patrimonial digital opera por divisão funcional: captadores de dados, operadores de engenharia social, administradores de perfis falsos, titulares de contas laranja, operadores de saque, receptadores de aparelhos, desbloqueadores, revendedores e lavadores de valores. O crime não é apenas um evento isolado; é uma cadeia operacional.

O celular ocupa papel central nesse processo. Ele concentra aplicativos bancários, mensagens, e-mails, senhas salvas, autenticações em dois fatores, redes sociais, fotografias, documentos digitais e carteiras virtuais. Por isso, o furto ou roubo de aparelho eletrônico pode ser apenas a porta de entrada para outras infrações. O Anuário Brasileiro de Segurança Pública registrou, em 2024, 917.748

celulares roubados ou furtados no Brasil, sendo 419.232 roubados e 498.516 furtados (Fórum Brasileiro de Segurança Pública, 2025).

Mais importante que a quantidade de aparelhos subtraídos é a baixa capacidade de recuperação e devolução. O Anuário informa que, em 2024, quinze unidades da Federação reportaram 35.666 celulares recuperados, e apenas nove unidades informaram a quantidade de aparelhos restituídos aos proprietários, totalizando 19.756 devoluções. O próprio relatório destaca que cerca de 8% dos aparelhos roubados conseguem ser recuperados pelas forças policiais e de segurança pública (Fórum Brasileiro de Segurança Pública, 2025).

A consequência dogmática é relevante: a subtração de celular não pode ser compreendida somente pelo valor de revenda do aparelho. Em muitos casos, o bem subtraído é simultaneamente objeto material do furto ou roubo e instrumento de acesso a novos bens jurídicos: patrimônio bancário, privacidade, dados pessoais, identidade digital e confiança nas comunicações. Isso justifica maior atenção normativa, mas não autoriza afastar garantias penais básicas.

A Lei Geral de Proteção de Dados Pessoais reforça essa leitura ao tratar a proteção de dados pessoais como tutela vinculada à liberdade, privacidade e livre desenvolvimento da personalidade. A LGPD também adota princípios como segurança, prevenção, responsabilização e prestação de contas no tratamento de dados pessoais (Brasil, 2018). Assim, a criminalidade patrimonial digital não atinge apenas dinheiro ou bens móveis. Ela explora a vulnerabilidade informacional como meio de lesão patrimonial.

4 A LEI Nº 14.155/2021 COMO ANTECEDENTE NORMATIVO

A Lei nº 14.155/2021 foi o principal antecedente normativo da Lei nº 15.397/2026 no campo dos crimes patrimoniais digitais. Ela alterou o art. 154-A do Código Penal, agravando a invasão de dispositivo informático, e introduziu figuras qualificadas no furto e no estelionato cometidos por meios eletrônicos. No furto, criou-se o art. 155, §4º-B, com pena de reclusão de 4 a 8 anos e multa quando o furto mediante fraude fosse cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem violação de mecanismo de segurança, utilização de programa malicioso ou meio fraudulento análogo (Brasil, 2021).

No estelionato, a Lei nº 14.155/2021 introduziu a fraude eletrônica no art. 171, §2º-A, com pena de reclusão de 4 a 8 anos e multa quando a fraude fosse cometida com informações fornecidas pela vítima ou por terceiro induzido a erro por redes sociais, contatos telefônicos, correio eletrônico fraudulento ou meio análogo. Também criou causas de aumento relacionadas a servidor mantido fora do território nacional e vítima idosa ou vulnerável (Brasil, 2021).

Dogmaticamente, a distinção entre furto mediante fraude eletrônica e estelionato eletrônico permanece decisiva. No furto mediante fraude, a fraude serve para burlar vigilância, sistema de proteção ou percepção da vítima, de modo que a coisa é retirada sem entrega voluntária juridicamente relevante. No estelionato, a fraude induz ou mantém a vítima em erro, levando-a a entregar voluntariamente a vantagem. A doutrina penal mantém essa distinção a partir da estrutura dos tipos patrimoniais: no furto, há subtração; no estelionato, há obtenção de vantagem mediante induzimento ou manutenção da vítima em erro (Mirabete; Fabbrini, 2025b).

A distinção é mais do que acadêmica. Ela interfere na capitulação, na pena, na competência, na identificação do sujeito passivo e na dinâmica probatória. Em uma fraude bancária por engenharia social, se a vítima é convencida a fazer o Pix, tende-se ao estelionato eletrônico. Se o agente captura senha por malware ou manipula sistema para movimentar a conta sem ato voluntário da vítima, a hipótese se aproxima do furto mediante fraude eletrônica.

A Lei nº 14.155/2021 também alterou o art. 70 do Código de Processo Penal, inserindo o §4º, segundo o qual, nos crimes do art. 171 do Código Penal praticados mediante depósito, cheque sem fundos ou transferência de valores, a competência será definida pelo domicílio da vítima; havendo pluralidade de vítimas, firma-se pela prevenção. Essa mudança foi relevante porque deslocou a competência em determinadas fraudes patrimoniais para o local da vítima, reduzindo a irracionalidade de obrigá-la a acompanhar investigação em localidade distante, escolhida pelo fraudador (Brasil, 1941; Cadernos Sistematizados, 2026b).

5 A LEI Nº 15.397/2026 E O NOVO REGIME DOS CRIMES PATRIMONIAIS DIGITAIS

A Lei nº 15.397/2026 aprofunda o movimento iniciado pela Lei nº 14.155/2021. A nova lei não se limita a inserir tipos digitais; ela majora penas de crimes patrimoniais clássicos e revaloriza objetos que, na sociedade digital, possuem função superior ao seu preço de mercado.

No furto, o caput do art. 155 passa a prever pena de reclusão de 1 a 6 anos e multa. O repouso noturno, antes majorado em um terço, passa a gerar aumento de metade. O furto mediante fraude eletrônica, previsto no art. 155, §4º-B, passa a ter pena de reclusão de 4 a 10 anos e multa. A subtração de aparelho de telefonia celular, computador, tablet ou dispositivo eletrônico semelhante também passa a receber pena de 4 a 10 anos e multa (Brasil, 2026).

A opção legislativa indica reconhecimento de que o celular é objeto patrimonial sensível. Porém, a técnica legislativa exige cautela. A pena de 4 a 10 anos para a subtração de qualquer celular pode criar problemas de proporcionalidade quando aplicada sem distinção entre situações de alta gravidade e furtos sem violência, sem organização e sem exploração posterior de dados. O valor

funcional do aparelho justifica tratamento mais severo, mas a individualização judicial deve impedir que a qualificadora produza punição desproporcional em casos de reduzida ofensividade concreta.

No roubo, a Lei nº 15.397/2026 aumenta a pena do caput para reclusão de 6 a 10 anos e multa, além de inserir causas relacionadas à subtração de aparelho de telefonia celular, computador, tablet ou dispositivo eletrônico semelhante. Também eleva a pena do latrocínio consumado para 24 a 30 anos. A conexão com crimes digitais ocorre porque o roubo físico do celular frequentemente viabiliza crimes posteriores, como invasão de contas, transferências, extorsões digitais e revenda para receptadores especializados (Brasil, 2026).

No estelionato, a nova lei introduz a chamada cessão de conta bancária no art. 171, §2º, VII: ceder, gratuita ou onerosamente, conta bancária para que nela transitem recursos destinados ao financiamento de atividade criminosa ou que dela sejam fruto. Essa inovação é dogmaticamente relevante porque desloca a atenção para a infraestrutura financeira do golpe. Os golpes digitais não se sustentam apenas pela comunicação fraudulenta com a vítima; dependem de contas aptas a receber e dispersar valores.

A conta laranja, todavia, deve ser interpretada à luz da responsabilidade penal subjetiva. A simples titularidade de conta usada em fraude não basta para condenação. É necessário demonstrar que o titular cedeu a conta, gratuita ou onerosamente, com consciência de que nela transitariam recursos destinados ao financiamento de atividade criminosa ou provenientes dela. O dolo pode ser direto, quando o agente sabe da finalidade criminosa, ou eventual, quando assume conscientemente o risco diante de circunstâncias inequívocas. Mas não se deve presumir dolo apenas pela movimentação atípica.

Esse ponto é constitucionalmente sensível. Pessoas vulneráveis podem ser aliciadas, enganadas, coagidas ou instrumentalizadas por organizações criminosas. Há diferença entre quem conscientemente vende o uso da conta para receber dinheiro de golpes, quem empresta conta sabendo da finalidade ilícita, quem desconfia fortemente e adere ao risco, quem age com negligência e quem também é vítima de manipulação. O Direito Penal não pode converter dificuldade investigativa em presunção de culpabilidade.

A Lei nº 15.397/2026 também altera a fraude eletrônica do art. 171, §2º-A, ampliando o texto para incluir a duplicação de dispositivo eletrônico ou aplicação de internet entre os meios típicos. Essa atualização é coerente com golpes que envolvem clonagem de aplicativos de mensagem, duplicação de acesso, simulação de ambiente bancário e uso de aplicações falsas (Brasil, 2026).

Outro ponto relevante é a revogação do art. 171, §5º, do Código Penal, que havia tornado o estelionato, em regra, crime de ação penal pública condicionada à representação. A revogação tende a restaurar a ação penal pública incondicionada para o estelionato, com impactos práticos

importantes: reduz a dependência de manifestação formal da vítima, facilita a persecução em golpes massivos e evita arquivamentos por ausência de representação em contextos de múltiplas vítimas. Contudo, por se tratar de norma com repercussão material sobre o exercício da pretensão punitiva, deve-se observar a irretroatividade da norma prejudicial ao acusado para fatos anteriores à vigência da nova lei.

Na receptação, a Lei nº 15.397/2026 aumenta a pena do art. 180 para reclusão de 2 a 6 anos e multa. A relevância dessa alteração para crimes digitais está na cadeia de circulação econômica dos celulares subtraídos. A receptação não é etapa posterior irrelevante; ela retroalimenta o furto e o roubo, cria mercado de revenda, peças, desbloqueio e pode abrir caminho para exploração de dados pessoais e bancários.

Por fim, a ementa da Lei nº 15.397/2026 menciona a tipificação de fraude bancária. No texto normativo, entretanto, a resposta legislativa aparece principalmente na ampliação da fraude eletrônica, na criminalização da cessão de conta bancária e no endurecimento de crimes patrimoniais praticados contra instituições financeiras. A técnica legislativa, nesse ponto, merece crítica: a ementa sugere categoria autônoma, mas o texto exige leitura sistemática para identificar onde a fraude bancária foi efetivamente normatizada.

6 ANÁLISE COMPARATIVA DAS ALTERAÇÕES INTRODUZIDAS PELA LEI Nº 15.397/2026

A Lei nº 15.397/2026 não instituiu um microssistema autônomo de crimes patrimoniais digitais. Sua técnica legislativa foi mais fragmentada: alterou tipos penais já existentes, elevou penas e inseriu hipóteses qualificadas, majoradas ou equiparadas em crimes clássicos contra o patrimônio. Por essa razão, a compreensão da reforma exige leitura comparativa entre três momentos normativos: o regime tradicional do Código Penal, a atualização promovida pela Lei nº 14.155/2021 e o endurecimento introduzido pela Lei nº 15.397/2026.

No furto simples, a alteração mais evidente foi a elevação do teto da pena. O art. 155, caput, que tradicionalmente previa reclusão de 1 a 4 anos e multa, passou a prever reclusão de 1 a 6 anos e multa. O impacto prático dessa modificação não se limita à dosimetria da pena. A ampliação do máximo abstrato repercute em prazos prescricionais, avaliação de gravidade concreta, política de acordos penais, medidas cautelares e percepção institucional do delito. Trata-se, contudo, de endurecimento geral, não propriamente digital.

No furto praticado durante o repouso noturno, a reforma também aumentou a resposta penal, substituindo a fração de um terço por aumento de metade. Embora essa alteração não esteja

diretamente ligada aos golpes digitais, ela revela o movimento amplo de recrudescimento dos crimes patrimoniais. A crítica é que, ao elevar penas de modo generalizado, o legislador corre o risco de tratar com a mesma intensidade situações muito distintas, desde furtos de baixa complexidade até delitos integrados a cadeias criminosas sofisticadas.

A mudança mais relevante para a criminalidade digital aparece no furto mediante fraude eletrônica. A Lei nº 14.155/2021 já havia criado a figura do art. 155, §4º-B, com pena de reclusão de 4 a 8 anos e multa para o furto mediante fraude cometido por dispositivo eletrônico ou informático, conectado ou não à rede de computadores. A Lei nº 15.397/2026 elevou essa pena para 4 a 10 anos e multa. A alteração reforça a tutela penal diante de fraudes digitais, mas não resolve, por si só, a dificuldade central desses delitos: identificar autores, rastrear valores, obter dados técnicos, preservar provas digitais e recuperar ativos antes de sua dispersão.

A nova qualificadora relativa à subtração de aparelho de telefonia celular, computador, tablet ou dispositivo eletrônico semelhante é um dos pontos mais expressivos da reforma. Antes da Lei nº 15.397/2026, não havia previsão específica no art. 155, §6º, voltada à subtração desses dispositivos. Com a nova redação, tais bens passam a receber pena de reclusão de 4 a 10 anos e multa. A justificativa político-criminal é compreensível: o celular contemporâneo não é apenas bem móvel de valor econômico; ele concentra identidade digital, aplicativos bancários, autenticações, contatos, mensagens, documentos e dados pessoais. Ainda assim, a aplicação da qualificadora exige proporcionalidade concreta, sob pena de transformar qualquer furto de celular, independentemente do contexto, em infração de altíssima gravidade abstrata.

No roubo, a Lei nº 15.397/2026 aumentou a pena do caput de 4 a 10 anos para 6 a 10 anos de reclusão e multa. Além disso, inseriu majorante específica quando a subtração envolver aparelho celular, computador, tablet ou dispositivo eletrônico semelhante. A opção legislativa reconhece que o roubo de dispositivo eletrônico pode gerar danos subsequentes, como invasão de contas, transferências indevidas, extorsões digitais e exploração de dados pessoais. O problema é que o aumento da pena mínima do roubo atinge todo o tipo penal, inclusive situações sem conexão com criminalidade digital, o que confirma a tendência de endurecimento geral da resposta patrimonial.

No estelionato, a inovação mais relevante é a figura da cessão de conta bancária, conhecida como conta laranja. O novo art. 171, §2º, VII, pune quem cede, gratuita ou onerosamente, conta bancária para que nela transitem recursos destinados ao financiamento de atividade criminosa ou que dela sejam fruto. A importância dessa previsão está em deslocar a persecução penal para a infraestrutura financeira dos golpes. A fraude digital depende de comunicação enganosa, mas também depende de contas aptas a receber, fracionar, sacar ou transferir valores. A conta laranja é, nesse contexto, elo funcional entre a vítima e os beneficiários finais do crime.

A criminalização da cessão de conta bancária, entretanto, exige interpretação constitucionalmente controlada. O tipo não autoriza punição automática do titular da conta. A prova deve demonstrar cessão consciente, vínculo subjetivo com a finalidade criminosa ou, ao menos, assunção consciente do risco em circunstâncias objetivamente reveladoras da origem ilícita ou da destinação criminosa dos valores. Sem essa exigência, a figura típica pode converter vulneráveis econômicos, pessoas enganadas ou titulares instrumentalizados em responsáveis penais objetivos por crimes praticados por terceiros.

Na fraude eletrônica, a Lei nº 15.397/2026 ampliou a redação do art. 171, §2º-A, para alcançar, além das hipóteses já previstas pela Lei nº 14.155/2021, condutas envolvendo duplicação de dispositivo eletrônico ou aplicação de internet. A atualização é tecnicamente relevante, porque aproxima o tipo penal de golpes por clonagem de aplicativos de mensagem, falsos ambientes digitais, simulação de interface bancária, duplicação de acesso e manipulação de aplicações. A abertura da expressão “meio fraudulento análogo”, contudo, deve ser lida com cautela, para não permitir analogia penal em prejuízo do acusado.

A reforma também revogou o art. 171, §5º, que havia tornado o estelionato, em regra, crime de ação penal pública condicionada à representação. Com a revogação, a tendência é de retorno da ação penal pública incondicionada. Essa mudança pode favorecer a persecução de golpes massivos, nos quais há múltiplas vítimas, dificuldade de identificação da autoria, vergonha da vítima em relatar o fato e baixa compreensão sobre a necessidade de representação. Ainda assim, por afetar o exercício da pretensão punitiva de modo prejudicial ao acusado, a alteração deve respeitar a irretroatividade em relação a fatos anteriores.

Na receptação, a pena do caput do art. 180 foi elevada para reclusão de 2 a 6 anos e multa. Embora pareça alteração lateral, ela é relevante para a economia dos crimes digitais, especialmente em relação a celulares furtados ou roubados. O mercado de receptação viabiliza revenda irregular, desmontagem, desbloqueio, retirada de peças, exportação informal e exploração de dados. Ao endurecer a receptação, o legislador tenta atacar a demanda econômica que estimula a subtração inicial. O êxito dessa medida, porém, depende de investigação sobre a cadeia de circulação dos aparelhos, e não apenas da punição do receptor encontrado em flagrante com o objeto.

A análise comparativa revela, portanto, que a Lei nº 15.397/2026 atua em duas frentes. A primeira é o endurecimento geral dos crimes patrimoniais, com aumento de penas em figuras clássicas como furto, roubo, estelionato e receptação. A segunda é a tentativa de aproximar o Código Penal da realidade dos golpes digitais, especialmente ao reconhecer a relevância penal dos dispositivos eletrônicos, da fraude por aplicações de internet e das contas bancárias utilizadas para circulação de valores ilícitos. A crítica central é que a reforma identifica corretamente pontos sensíveis da cadeia

criminosa, mas continua concentrada na elevação abstrata de penas, quando a criminalidade patrimonial digital exige também prevenção, rastreabilidade financeira, bloqueio célere de ativos, investigação tecnológica e recuperação efetiva dos valores subtraídos.

7 DADOS EMPÍRICOS E EFICÁCIA DA RESPOSTA PENAL

A pergunta sobre a eficácia da Lei nº 15.397/2026 não pode ser respondida apenas pela comparação de penas. É necessário confrontar a estrutura normativa com os dados disponíveis sobre criminalidade patrimonial digital.

O primeiro dado relevante é a massificação da vitimização. Quando o DataSenado indica que 24% dos brasileiros com mais de 16 anos perderam dinheiro em crimes cibernéticos no período de 12 meses, a questão deixa de ser episódica. Trata-se de fenômeno de massa, com vítimas distribuídas por diferentes perfis socioeconômicos (Senado Federal, 2024). Se não há perfil claro de vítima, a política criminal não pode se limitar a alertas genéricos de “cuidado na internet”. A prevenção deve envolver arquitetura segura de plataformas, autenticação robusta, educação digital e resposta institucional rápida.

O segundo dado é a inversão da criminalidade patrimonial. O Anuário Brasileiro de Segurança Pública registra que, em 2024, houve 745.333 roubos e 2.166.552 estelionatos. O relatório afirma que a inversão entre roubos e estelionatos ocorreu em 2020 e se acentuou desde então, consolidando tendência de reorganização dos crimes patrimoniais (Fórum Brasileiro de Segurança Pública, 2025). Logo, a criminalidade patrimonial se desloca parcialmente da violência física para a fraude, sem que isso signifique menor dano social.

O terceiro dado é a expansão do estelionato eletrônico. O crescimento de 17% dos registros de estelionato por meio eletrônico em 2024 indica que a fraude digital cresce em ritmo superior ao estelionato total (Fórum Brasileiro de Segurança Pública, 2025). Isso reforça a tese de que o problema não é apenas o estelionato como categoria clássica, mas a digitalização da fraude como modelo escalável de criminalidade.

O quarto dado envolve celulares. Mesmo com queda no total de roubos e furtos de celulares em 2024, o volume de 917.748 aparelhos subtraídos permanece expressivo. Além disso, o Anuário mostra que roubos de celulares caíram 33,2% entre 2018 e 2024, enquanto furtos desses equipamentos subiram 9,5% no mesmo período (Fórum Brasileiro de Segurança Pública, 2025). A mudança sugere adaptação racional da criminalidade: menos exposição ao confronto violento e maior exploração de oportunidades de subtração discreta.

O quinto dado é bancário. A Febraban demonstra que os canais digitais concentram a maior parte da dinâmica bancária contemporânea e que o Pix continua crescendo nas movimentações financeiras. Em 2025, o Pix com movimentação pelo mobile banking atingiu 29,419 bilhões de transações, aumento de 19% em relação a 2024 (FEBRABAN; Deloitte, 2026). O Banco Central define o Mecanismo Especial de Devolução como mecanismo exclusivo do Pix criado para facilitar devoluções em caso de fraude, golpe ou crime, aumentando as possibilidades de a vítima reaver os recursos (Banco Central do Brasil, 2025a).

Esses dados apontam para uma conclusão: a pena mais alta pode ter função expressiva e retributiva, mas sua capacidade preventiva depende de certeza de detecção, velocidade de bloqueio e recuperação de ativos. Golpes digitais são crimes de oportunidade tecnológica e financeira. Se o valor transita por múltiplas contas em minutos, a ameaça de pena futura perde força preventiva quando a investigação é lenta, fragmentada ou incapaz de reconstruir o fluxo financeiro.

Portanto, a eficácia da Lei nº 15.397/2026 dependerá de sua articulação com políticas não penais e processuais: integração entre bancos e persecução penal, uso adequado do Mecanismo Especial de Devolução, compartilhamento seguro de indícios de fraude, fortalecimento de delegacias especializadas, cooperação com provedores, educação digital, bloqueio de IMEI, rastreamento de receptação, recuperação de ativos e atendimento às vítimas.

8 ANÁLISE POLÍTICO-CRIMINAL: EFICÁCIA OU DIREITO PENAL SIMBÓLICO?

O Direito Penal simbólico ocorre quando a lei penal é utilizada para produzir sensação de resposta estatal sem correspondência suficiente em eficácia material. Não significa que toda majoração de pena seja simbólica. O problema surge quando o legislador elege a elevação abstrata da sanção como substituto de políticas públicas, investigação e prevenção.

A Lei nº 15.397/2026 não é puramente simbólica. Ela identifica corretamente pontos estruturais da criminalidade patrimonial digital: o celular como chave de acesso, a conta bancária cedida como infraestrutura financeira, a fraude eletrônica como modalidade intensificada de estelionato e a receptação como motor econômico da subtração de aparelhos. Esses elementos justificam atualização normativa.

Entretanto, a lei revela traços de Direito Penal de emergência. A resposta legislativa concentra-se no aumento de penas, mesmo quando os dados indicam que o problema central é a capacidade de investigação, prevenção e recuperação. O Anuário Brasileiro de Segurança Pública é expressivo ao afirmar que o crime mudou muito nos últimos anos e que a forma de enfrentá-lo

também precisa mudar (Fórum Brasileiro de Segurança Pública, 2025). Essa mudança não se resume à dosimetria penal.

A experiência dos golpes digitais mostra que a prevenção depende mais de arquitetura institucional do que de ameaça penal abstrata. O fraudador atua pela expectativa de anonimato, rapidez e baixa recuperação dos valores. Se a conta bancária intermediária é usada com facilidade, se a movimentação atípica não é detectada, se o bloqueio demora, se a vítima não sabe acionar o Mecanismo Especial de Devolução, se as informações bancárias não chegam adequadamente à investigação e se a polícia não possui estrutura tecnológica, o aumento de pena terá efeito limitado.

Além disso, há risco de seletividade. Os operadores mais sofisticados podem permanecer ocultos, enquanto titulares vulneráveis de contas, pequenos receptadores ou agentes de baixa hierarquia se tornam os alvos mais visíveis da persecução. A criminalização da conta laranja só será legítima se alcançar a infraestrutura dolosa do golpe, e não se funcionar como atalho para punir quem está mais próximo documentalmente da transação.

A tese defendida é, portanto, intermediária e crítica: a Lei nº 15.397/2026 possui utilidade dogmática e pode reforçar a resposta penal em casos graves, mas sua eficácia preventiva dependerá de política criminal integrada. O aumento de pena é insuficiente quando desacompanhado de inteligência financeira, cooperação interinstitucional, rastreamento de ativos, repressão à receptação, proteção de dados, regulação bancária preventiva e educação digital.

9 LIMITES CONSTITUCIONAIS DA NOVA REPRESSÃO PENAL

A repressão penal aos golpes digitais deve observar os princípios da legalidade, taxatividade, culpabilidade, proporcionalidade, intervenção mínima, subsidiariedade e responsabilidade penal subjetiva. A gravidade social dos golpes digitais não autoriza flexibilização de garantias.

O princípio da legalidade exige que as condutas sejam descritas de forma suficientemente determinada. Termos como “dispositivo eletrônico”, “aplicação de internet” e “meio fraudulento análogo” permitem adaptação tecnológica, mas devem ser interpretados restritivamente para evitar ampliação ilimitada do tipo penal. A abertura semântica é compreensível em crimes digitais, porque a tecnologia muda rapidamente; contudo, a analogia não pode operar em prejuízo do acusado.

A culpabilidade impede responsabilização objetiva. Esse limite é especialmente importante na conta laranja. O art. 171, §2º, VII, exige cessão de conta bancária para trânsito de recursos destinados ao financiamento de atividade criminosa ou que dela sejam fruto. A conduta típica não é simplesmente ter conta usada por criminoso, mas ceder a conta com vínculo subjetivo com a finalidade criminosa ou com a origem ilícita dos recursos.

A proporcionalidade também impõe controle. A pena de 4 a 10 anos para furto de celular pode ser adequada em contextos de organização criminosa, exploração de dados, reiteração, prejuízo elevado ou integração com fraudes bancárias. Mas sua aplicação automática a todo furto de aparelho, sem análise concreta, pode gerar desproporção. A individualização da pena deve funcionar como correção constitucional da severidade abstrata.

A intervenção mínima exige que o Direito Penal seja *última ratio*. No campo digital, isso não significa afastar a repressão penal, mas reconhecer que ela não substitui mecanismos de segurança bancária, proteção de dados, bloqueio tecnológico, prevenção por design, educação digital e regulação administrativa. O Direito Penal chega tarde quando a vítima já perdeu o dinheiro e o ativo já foi disperso.

A presunção de inocência e o devido processo legal também devem orientar a produção probatória. Em crimes digitais patrimoniais, a prova frequentemente envolve registros bancários, IPs, logs, geolocalização, dados cadastrais, registros de dispositivos, imagens, conversas e perícia em aparelhos. A complexidade probatória não permite condenações baseadas em inferências frágeis. O nexó entre agente, conduta, dolo e vantagem ilícita deve ser demonstrado com segurança.

10 COMPETÊNCIA, CONCURSO DE CRIMES E AÇÃO PENAL

A competência nos crimes patrimoniais digitais exige distinção entre modalidades típicas. No estelionato praticado mediante depósito, cheque ou transferência de valores, o art. 70, §4º, do Código de Processo Penal fixa a competência pelo domicílio da vítima, com prevenção em caso de pluralidade de vítimas (Brasil, 1941).

No furto mediante fraude eletrônica, entretanto, a lógica pode ser diversa. Quando a fraude é usada para burlar sistema bancário e movimentar valores sem entrega voluntária da vítima, a consumação tende a ocorrer no local em que a coisa sai da esfera de disponibilidade da vítima ou da instituição lesada. Em casos envolvendo violação de sistema de segurança bancário, a definição da competência dependerá da instituição atingida, da titularidade do bem jurídico e da presença de interesse federal.

O concurso de crimes também merece atenção. Um mesmo contexto pode envolver furto ou roubo de celular, invasão de dispositivo, estelionato eletrônico, receptação, falsidade documental, associação criminosa, organização criminosa ou lavagem de capitais. A definição dependerá da autonomia das condutas, da existência de desígnios independentes, da estabilidade do grupo e dos atos de ocultação ou dissimulação de valores.

A conta laranja pode funcionar como participação, crime equiparado ao estelionato ou etapa de lavagem, a depender do caso. Se o titular cede a conta antes ou durante a fraude, sabendo que ela

receberá valores ilícitos, a conduta pode se enquadrar no art. 171, §2º, VII. Se, posteriormente, pratica atos autônomos de ocultação ou dissimulação para dar aparência lícita ao produto do crime, pode haver discussão sobre lavagem de capitais. A capitulação não deve ser cumulativa de forma automática, sob pena de bis in idem.

Quanto à ação penal, a revogação do art. 171, §5º, pela Lei nº 15.397/2026 tende a restabelecer a ação penal pública incondicionada para o estelionato. Essa alteração pode melhorar a persecução de golpes massivos, nos quais muitas vítimas deixam de representar por desconhecimento, medo, vergonha ou baixa confiança institucional. Contudo, a aplicação temporal deve respeitar a irretroatividade de norma prejudicial ao acusado, por possuir reflexos materiais na persecução penal.

11 CONSIDERAÇÕES FINAIS

O aumento de pena nos crimes patrimoniais digitais, por si só, não é medida suficiente para enfrentar golpes digitais, fraudes bancárias, contas laranja, receptação de celulares e subtrações de dispositivos eletrônicos. A Lei nº 15.397/2026 representa atualização normativa relevante, mas sua eficácia depende de estrutura institucional que ultrapassa o texto penal.

A hipótese da pesquisa foi confirmada com ajustes. A nova lei não pode ser reduzida a Direito Penal simbólico, porque identifica corretamente elementos centrais da criminalidade patrimonial contemporânea: dispositivos eletrônicos, fraude digital, contas intermediárias e circulação econômica dos bens subtraídos. No entanto, a lei revela traços simbólicos quando aposta prioritariamente no endurecimento penal e não enfrenta, no mesmo plano, as condições que tornam os golpes digitais rentáveis e de difícil apuração.

Os dados empíricos demonstram que a criminalidade patrimonial mudou de eixo. O crescimento dos estelionatos, a expansão dos estelionatos eletrônicos, a massificação das transações digitais, o volume de celulares subtraídos e a baixa recuperação de aparelhos indicam que o problema é sistêmico. O Estado não enfrenta esse cenário apenas com pena maior. Precisa de investigação tecnológica, cooperação bancária, rastreabilidade de valores, bloqueio rápido de ativos, uso eficiente do Mecanismo Especial de Devolução, integração de bases de dados, repressão à receptação e proteção informacional das vítimas.

Dogmaticamente, a Lei nº 15.397/2026 exige interpretação cuidadosa. A cessão de conta bancária é avanço importante, mas não autoriza presunção automática de dolo. A subtração de celulares merece tratamento diferenciado, mas a pena deve ser individualizada conforme a gravidade concreta. A fraude eletrônica precisa ser aplicada com respeito à taxatividade. A revogação da

representação no estelionato pode ampliar a efetividade persecutória, mas deve respeitar a irretroatividade da norma prejudicial.

Assim, a conclusão central é que a Lei nº 15.397/2026 é necessária, mas insuficiente. Ela atualiza a linguagem penal diante dos golpes digitais, porém não substitui política pública. O enfrentamento eficaz dos crimes patrimoniais digitais exige menos confiança retórica no aumento de pena e mais compromisso institucional com prevenção, tecnologia, inteligência financeira, recuperação de ativos e garantias constitucionais.

REFERÊNCIAS

BANCO CENTRAL DO BRASIL. **FAQ sobre o Mecanismo Especial de Devolução (MED)**. Brasília: Banco Central do Brasil, 2025a. Disponível em: <https://www.bcb.gov.br/meubc/faqs/p/o-que-e-e-como-funciona-o-mecanismo-especial-de-devolucao-med>. Acesso em: 4 jul. 2026.

BANCO CENTRAL DO BRASIL. **BC aprimora o Mecanismo Especial de Devolução do Pix**. Brasília: Banco Central do Brasil, 2025b. Disponível em: <https://www.bcb.gov.br/detalhenoticia/20817/nota>. Acesso em: 4 jul. 2026.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, 1940. Versão compilada consultada em 2026.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, DF: Presidência da República, 1941. Versão compilada consultada em 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Versão compilada consultada em 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Versão compilada consultada em 2026.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Código Penal para tornar mais graves crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet e altera o Código de Processo Penal para definir competência em modalidades de estelionato. Brasília, DF: Presidência da República, 2021.

BRASIL. **Lei nº 15.397, de 30 de abril de 2026**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, a fim de majorar penas de crimes contra o patrimônio e tipificar crimes relacionados à receptação de animal doméstico e fraude bancária. Brasília, DF: Presidência da República, 2026.

CADERNOS SISTEMATIZADOS. **Direito Penal**: Parte Geral. Edição 2026.1. [S. l.]: Cadernos Sistematizados, 2026a.

CADERNOS SISTEMATIZADOS. **Direito Processual Penal 1**. Edição 2026.1. [S. l.]: Cadernos Sistematizados, 2026b.

CADERNOS SISTEMATIZADOS. **Direito Processual Penal 2**. Edição 2026.1. [S. l.]: Cadernos Sistematizados, 2026c.

FEBRABAN; DELOITTE. **Pesquisa Febraban de Tecnologia Bancária 2026**: 34ª edição. São Paulo: Febraban; Deloitte, 2026.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **19º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2025.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Manual de Direito Penal**: Parte Geral: arts. 1º a 120 do CP. 37. ed. Indaiatuba, SP: Editora Foco, 2025a.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Manual de Direito Penal**: Parte Especial: arts. 121 a 234-B do CP. 38. ed. Indaiatuba, SP: Editora Foco, 2025b.

SENADO FEDERAL. **Golpes digitais atingem 24% da população brasileira, revela DataSenado**. Brasília: Agência Senado, 1 out. 2024.