FRAUDE E ESTELIONATO NA INTERNET: O REGIME JURÍDICO DO ESTELIONATO DIGITAL APÓS A LEI Nº 15.397/2026

Fraud and swindling on the internet: the legal regime of digital fraud after Law No. 15,397/2026

Oswaldo Prezotti[1]

RESUMO

O presente artigo analisa o regime jurídico-penal do estelionato digital no Brasil após a Lei nº 15.397, de 30 de abril de 2026, que promoveu ampla reforma dos crimes patrimoniais. Mediante pesquisa bibliográfica, documental e jurisprudencial, com conferência da redação vigente da legislação em fontes oficiais, reconstrói-se a trajetória legislativa iniciada com a Lei nº 14.155/2021 — criadora da fraude eletrônica (art. 171, § 2º-A, do Código Penal) e da regra de competência pelo domicílio da vítima (art. 70, § 4º, do Código de Processo Penal, interpretado pelo Superior Tribunal de Justiça no CC 185.983) — e examinam-se as inovações de 2026: a ampliação típica da fraude eletrônica, que passou a alcançar expressamente a duplicação de dispositivo eletrônico ou aplicação de internet; a incriminação da cessão de conta bancária para trânsito de recursos criminosos (conta laranja); as novas qualificadoras do furto de dispositivos eletrônicos; e a revogação do § 5º do art. 171, com o retorno do estelionato, em regra, à ação penal pública incondicionada — inovação mais gravosa e, portanto, irretroativa. Discute-se, ao final, a tensão central do debate contemporâneo: a aposta reiterada no endurecimento de penas contrasta com o diagnóstico criminológico e empírico de que a contenção da fraude digital depende primordialmente de capacidade investigativa, perícia e cooperação institucional. Conclui-se que a reforma moderniza o aparato típico, mas repete fórmula punitivista de eficácia preventiva duvidosa.

Palavras-chave: estelionato digital; fraude eletrônica; Lei nº 15.397/2026; conta laranja; ação penal.

ABSTRACT

This article analyzes the criminal law regime of digital fraud in Brazil after Law No. 15,397 of April 30, 2026, which carried out a broad reform of property crimes. Through bibliographic, documentary and case-law research, with verification of the current wording of the legislation in official sources, the paper retraces the legislative path initiated by Law No. 14,155/2021 — which created the offense of electronic fraud (article 171, § 2-A, of the Penal Code) and the venue rule based on the victim's domicile (article 70, § 4, of the Code of Criminal Procedure, as interpreted by the Superior Court of Justice in CC 185,983) — and examines the 2026 innovations: the typical expansion of electronic fraud, which now expressly covers the duplication of electronic devices or internet applications; the criminalization of ceding a bank account for the transit of criminal proceeds (money-mule accounts); the new qualified forms of theft of electronic devices; and the repeal of § 5 of article 171, with fraud returning, as a rule, to unconditional public prosecution — a more burdensome innovation and therefore non-retroactive. Finally, the paper discusses the central tension of the contemporary debate: the

[1]Graduando do Curso de Direito da Faculdade Aprendiz, Barbacena/MG. Pesquisa de forma independente temas de Direito Penal e Direito Digital, com foco em crimes cibernéticos. Este texto tem finalidade exclusivamente acadêmica e educativa e não constitui aconselhamento jurídico.

repeated reliance on harsher penalties contrasts with the criminological and empirical diagnosis that containing digital fraud depends primarily on investigative capacity, forensics and institutional cooperation. The article concludes that the reform modernizes the statutory framework but repeats a punitive formula of doubtful preventive effectiveness.

Keywords: *digital fraud; electronic fraud; Law No. 15,397/2026; money-mule accounts; criminal prosecution.*

1 INTRODUÇÃO

A fraude patrimonial tornou-se o crime característico da economia digitalizada brasileira. Os indicadores disponíveis em 2026 compõem um quadro expressivo: segundo levantamento da Check Point Research relativo a junho de 2026, cada organização brasileira sofreu, em média, 4.001 tentativas de ataque cibernético por semana — crescimento de 44% em um ano e patamar muito superior à média global de 2.270 (CONVERGÊNCIA DIGITAL, 2026); o relatório de ameaças ao setor financeiro da CrowdStrike de 2026 situou o Brasil entre os cinco países mais visados do mundo por ataques a instituições financeiras e destacou a atuação do grupo brasileiro identificado como PLUMP SPIDER, dedicado a fraudes contra entidades financeiras mediante engenharia social e ferramentas de acesso remoto (CROWDSTRIKE, 2026); e o Canal Nacional de Denúncias de Crimes Cibernéticos registrou 87.689 denúncias em 2025, alta de 28,4% (AGÊNCIA BRASIL, 2026). Do golpe do falso atendimento bancário à clonagem de aplicativos de mensagens, a fraude digital massificou-se como experiência cotidiana.

A resposta legislativa mais recente a esse cenário é a Lei nº 15.397, de 30 de abril de 2026, publicada em 4 de maio de 2026, que alterou profundamente o tratamento dos crimes patrimoniais no Código Penal: majorou penas de furto, roubo e receptação, criou qualificadoras para a subtração de dispositivos eletrônicos, redesenhou a fraude eletrônica, incriminou expressamente a cessão de contas bancárias a esquemas criminosos e revogou o § 5º do art. 171, devolvendo ao estelionato, em regra, a ação penal pública incondicionada (BRASIL, 2026).

O presente artigo tem por objetivo examinar o regime jurídico do estelionato digital resultante dessa reforma. A seção 2 reconstrói a construção legislativa anterior, centrada na Lei nº 14.155/2021; a seção 3 analisa as inovações de 2026 em matéria de fraude; a seção 4 discute a tensão entre o endurecimento sancionatório e a efetividade da persecução, incorporando as críticas doutrinárias à opção punitivista. Seguem-se as considerações finais. A pesquisa é bibliográfica, documental e jurisprudencial, e a redação vigente de todos os dispositivos citados foi conferida no Portal da Legislação da Presidência da República em julho de 2026.

2 A CONSTRUÇÃO LEGISLATIVA DA TUTELA PENAL CONTRA A FRAUDE DIGITAL

2.1 O estelionato clássico e as oscilações do legislador

O tipo básico do estelionato — obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento (art. 171, caput, do Código Penal) — demonstrou notável plasticidade diante das fraudes praticadas pela internet: phishing, páginas falsas, perfis fraudulentos e golpes de engenharia social sempre couberam, em princípio, na fórmula aberta de 1940. A percepção político-criminal, contudo, era de insuficiência, tanto pela pena — reclusão de um a cinco anos — quanto pelas dificuldades investigatórias e de fixação de competência próprias do ambiente digital.

A história recente do dispositivo é marcada por oscilações. A Lei nº 13.964/2019 (Pacote Anticrime) introduziu o § 5º, condicionando a ação penal, em regra, à representação da vítima — opção celebrada por parte da doutrina como racionalização da persecução (JORIO; BOLDT, 2021). Menos de dois anos depois, a Lei nº 14.155/2021 inaugurou o movimento inverso, de exasperação; e a Lei nº 15.397/2026, como se verá, completou-o, revogando o próprio § 5º. Em sete anos, o estelionato transitou da ação pública incondicionada à condicionada e de volta à incondicionada — instabilidade que, por si, já constitui dado relevante para a avaliação da racionalidade da política criminal brasileira.

2.2 A Lei nº 14.155/2021: fraude eletrônica e competência pelo domicílio da vítima

A Lei nº 14.155, de 27 de maio de 2021, tornou mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet (BRASIL, 2021). Sua principal criação foi a fraude eletrônica do art. 171, § 2º-A: pena de reclusão de quatro a oito anos quando a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento. Acresceram-se a majorante do servidor mantido fora do território nacional (§ 2º-B) e a do crime praticado contra idoso ou vulnerável (§ 4º).

A doutrina recebeu a novidade com reservas. Jorio e Boldt (2021), em comentário sistemático à lei, reconhecem a oportunidade político-criminal da tipificação específica, mas denunciam o exagero sancionatório: a pena mínima da fraude eletrônica é quatro vezes superior

à do estelionato comum, sem que exista diferença de reprovabilidade material entre o engodo praticado por correio eletrônico e o praticado presencialmente com documento falso — desproporção que, ademais, praticamente inviabiliza a substituição da pena privativa de liberdade por restritivas de direitos. Os autores criticam, ainda, a fronteira imprecisa entre a fraude eletrônica e o furto mediante fraude eletrônica (art. 155, § 4º-B), fonte de insegurança na qualificação de transferências obtidas por invasão de contas.

No plano processual, a lei acrescentou o § 4º ao art. 70 do Código de Processo Penal: nos estelionatos praticados mediante depósito, emissão de cheques sem provisão ou com pagamento frustrado, ou mediante transferência de valores, a competência define-se pelo domicílio da vítima, firmando-se pela prevenção em caso de pluralidade de vítimas (BRASIL, 2021). A regra respondeu à peregrinação processual imposta às vítimas de golpes praticados a distância. Seu alcance foi delimitado pelo Superior Tribunal de Justiça: no CC 185.983, relatado pelo ministro Joel Ilan Paciornik, a Terceira Seção assentou que a competência pelo domicílio da vítima restringe-se às modalidades expressamente indicadas no dispositivo, permanecendo, nas demais hipóteses, a regra geral do local da obtenção da vantagem (BRASIL, 2022).

Completou o quadro anterior à reforma de 2026 a Lei nº 14.478/2022, que, ao disciplinar os ativos virtuais, acrescentou ao Código Penal o art. 171-A: organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações que envolvam ativos virtuais, valores mobiliários ou quaisquer ativos financeiros com o fim de obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento, com pena de reclusão de quatro a oito anos e multa (BRASIL, 1940). A figura respondeu à proliferação de pirâmides financeiras travestidas de investimento em criptomoedas e evidencia a tendência de especialização típica: o gênero estelionato desdobra-se em espécies definidas pelo instrumento — a rede social, o dispositivo, o ativo virtual — em detrimento da unidade conceitual da fraude.

3 A LEI Nº 15.397/2026 E O NOVO DESENHO DA REPRESSÃO À FRAUDE DIGITAL

3.1 Panorama da reforma e as qualificadoras patrimoniais digitais

Originária do Projeto de Lei nº 3.780/2023, de autoria do deputado Kim Kataguiri e relatado no Senado Federal pelo senador Efraim Filho, a Lei nº 15.397/2026 promoveu a mais ampla revisão dos crimes patrimoniais das últimas décadas. Registre-se, como indício da própria desproporção que a doutrina viria a denunciar, que o texto aprovado foi parcialmente

vetado: caiu o dispositivo que elevaria a pena do roubo qualificado pelo resultado lesão corporal grave, sob a justificativa de que a pena mínima resultante superaria a do homicídio qualificado (SENADO FEDERAL, 2026) — veto que o Planalto registra no art. 157, § 3º, I, do Código Penal (BRASIL, 2026). No furto, elevou a pena básica para reclusão de um a seis anos, remodelou o furto mediante fraude eletrônica (art. 155, § 4º-B, com pena de quatro a dez anos) e criou qualificadora específica para a subtração de aparelho de telefonia celular, de computador, inclusive portátil ou do tipo prancheta, ou de qualquer dispositivo eletrônico ou informático semelhante (art. 155, § 6º, II), igualmente apenada com reclusão de quatro a dez anos; no roubo, incluiu causa de aumento paralela (art. 157, § 2º, IX) (BRASIL, 2026). O legislador reconheceu, nessas figuras, que o dispositivo móvel é hoje porta de acesso ao patrimônio financeiro integral da vítima: o celular subtraído vale menos pelo hardware do que pelas credenciais bancárias que carrega.

No estelionato, o caput recebeu redação atualizada, mantido o intervalo de reclusão de um a cinco anos e multa. O endurecimento operou-se, portanto, não na pena básica, mas na arquitetura das figuras derivadas e no regime processual — técnica que concentra o rigor nas modalidades organizadas e digitais da fraude.

A reforma alcançou, ainda, a infraestrutura digital coletiva: o crime de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (art. 266) passou a ser apenado com reclusão de dois a quatro anos e multa, com pena em dobro quando o crime é cometido por ocasião de calamidade pública ou mediante subtração, dano ou destruição de equipamento instalado em estrutura utilizada para a prestação de serviços de telecomunicações (BRASIL, 2026). A par disso, o furto de fios, cabos e equipamentos de energia, telefonia e transferência de dados recebeu qualificadora própria (art. 155, § 8º) — resposta ao vandalismo patrimonial que, ao subtrair componentes de baixo valor venal, produz apagões de conectividade com dano social desproporcional.

3.2 A fraude eletrônica ampliada

A reforma reescreveu o § 2º-A do art. 171, mantendo a pena de quatro a oito anos, mas alargando o alcance típico:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos, envio de correio eletrônico fraudulento, duplicação de dispositivo eletrônico ou aplicação de internet, ou por qualquer outro meio fraudulento análogo (BRASIL, 1940, com a redação dada pela Lei nº 15.397/2026).

A inclusão da duplicação de dispositivo eletrônico ou aplicação de internet incorpora expressamente ao tipo as técnicas de clonagem de chips (SIM swap), o espelhamento de aplicativos de mensagens e a replicação fraudulenta de aplicações bancárias — modalidades que, sob a redação de 2021, dependiam da cláusula analógica final. A alteração reduz o espaço de controvérsia sobre a subsunção dos golpes mais frequentes da prática brasileira, como a clonagem de contas de aplicativos de mensagens seguida de pedidos de transferência a contatos da vítima.

3.3 A cessão de conta laranja

Inovação de relevo é a figura do art. 171, § 2º, VII: incorre nas penas do estelionato quem cede, gratuita ou onerosamente, conta bancária para que nela transitem recursos destinados ao financiamento de atividade criminosa ou que dela sejam fruto (BRASIL, 2026). O dispositivo ataca a infraestrutura financeira dos esquemas de fraude — a rede de contas de passagem que pulveriza os valores subtraídos e frustra o rastreamento e o bloqueio —, dispensando a demonstração de participação do cedente na fraude antecedente: a cessão consciente da conta passa a ser conduta típica autônoma, equiparada ao estelionato (COSTA; ENALDO; BRETZ, 2026). A doutrina adverte, porém, para o desafio probatório do elemento subjetivo — distinguir o colaborador consciente da pessoa vulnerável aliciada ou enganada para abrir contas —, ponto em que a aplicação judicial definirá o alcance real da incriminação (SANTOS, R., 2026).

3.4 A revogação do § 5º e o direito intertemporal

A mudança de maior impacto processual é a revogação integral do § 5º do art. 171: o estelionato voltou a ser, em regra, crime de ação penal pública incondicionada, dispensada a representação da vítima. A justificativa declarada é operacional: nas fraudes digitais massificadas, com centenas ou milhares de vítimas pulverizadas pelo território nacional, a exigência de representação individual fragmentava a persecução e inviabilizava a visão de conjunto dos esquemas criminosos; a ação incondicionada devolve ao Ministério Público a possibilidade de persecução unificada e de atuação de ofício sobre organizações especializadas (SANTOS, M. A. F., 2026).

No plano intertemporal, a alteração é inovação mais gravosa: a condição de procedibilidade integra o estatuto de garantia do acusado, de modo que a nova disciplina não retroage para alcançar fatos praticados antes de 4 de maio de 2026 — em relação a eles, subsiste

a exigência de representação no prazo decadencial (COSTA; ENALDO; BRETZ, 2026). Trata-se de aplicação do princípio da irretroatividade da lei penal mais severa (art. 5º, XL, da Constituição), que a doutrina estende às normas processuais de conteúdo material, categoria na qual a doutrina majoritária situa a disciplina da ação penal.

4 ENDURECIMENTO DE PENA VERSUS EFETIVIDADE INVESTIGATIVA

4.1 A crítica de proporcionalidade e de populismo penal

A recepção doutrinária da Lei nº 15.397/2026 reproduziu, ampliada, a controvérsia de 2021. Yarochewsky (2026) qualifica o diploma como lei desarranjada: editada sem verificação empírica prévia de impactos, equipara, no plano sancionatório, crimes patrimoniais sem violência a delitos contra a vida — o furto de um celular pode alcançar pena de quatro a dez anos, intervalo equivalente ao do roubo na disciplina anterior —, agravando a inflação legislativa e alimentando o encarceramento em massa, que recai seletivamente sobre réus jovens, negros e pobres. Na mesma direção, especialistas ouvidos pela imprensa especializada apontaram a reiteração de um modelo de exasperação de penas sem eficácia demonstrada na redução da criminalidade patrimonial, com risco adicional de alcançar, na figura da conta laranja, pessoas vulneráveis aliciadas pelos esquemas (SANTOS, R., 2026). A crítica conecta-se à advertência formulada por Jorio e Boldt (2021) já quanto à lei de 2021: a distância valorativa que o legislador enxerga entre a fraude digital e a fraude analógica não encontra correspondência na reprovabilidade material das condutas.

Sob a ótica dos institutos despenalizadores, o endurecimento produz efeitos em cadeia: penas mínimas iguais ou superiores a quatro anos afastam o acordo de não persecução penal e dificultam a substituição por restritivas de direitos e a fixação de regimes iniciais brandos, deslocando para o cárcere condutas de lesividade heterogênea (COSTA; ENALDO; BRETZ, 2026). O paradoxo apontado pela crítica é conhecido: quanto mais a resposta se concentra na cominação abstrata, menos ela discrimina entre o operador profissional do esquema e o partícipe marginal.

4.2 O argumento da efetividade e seus limites

O contraponto favorável à reforma não se apoia primordialmente nas penas, mas nos instrumentos: a ação penal incondicionada, a tipificação autônoma da conta laranja e a ampliação típica da fraude eletrônica removem obstáculos reais à persecução das fraudes

organizadas, permitindo a formação de casos estruturais a partir de vítimas dispersas (SANTOS, M. A. F., 2026). O próprio contexto empírico reforça a plausibilidade do argumento: diante de adversários profissionalizados como os documentados pela CrowdStrike (2026) no setor financeiro brasileiro, a exigência de representação individual constituía assimetria evidente entre a escala da criminalidade e a escala da resposta estatal.

O consenso possível entre as posições, todavia, é significativo: nenhuma corrente sustenta que a majoração de penas, por si, reduza a fraude digital. A contenção do fenômeno depende de perícia digital, cooperação com instituições financeiras e provedores, rastreamento de ativos e integração investigativa — capacidades cuja construção não se decreta (SANTOS, M. A. F., 2026). A eficácia da Lei nº 15.397/2026 será medida, portanto, menos pelas penas cominadas e mais pelo uso que órgãos de persecução fizerem dos novos instrumentos processuais e típicos.

5 CONSIDERAÇÕES FINAIS

O percurso realizado permite sintetizar o novo regime do estelionato digital brasileiro. A Lei nº 15.397/2026 completou o movimento iniciado em 2021: a fraude eletrônica consolidou-se como figura central, agora com alcance típico que incorpora expressamente a duplicação de dispositivos e aplicações; a infraestrutura financeira dos esquemas foi atacada pela incriminação da cessão de conta laranja; o patrimônio informático da vítima recebeu tutela qualificada no furto e no roubo; e a persecução foi desobstruída pelo retorno à ação penal pública incondicionada, irretroativa por mais gravosa.

A avaliação crítica da reforma, contudo, deve distinguir seus dois vetores. O vetor instrumental — ação penal, competência, tipificação de condutas de suporte — responde a deficiências reais e documentadas da persecução da fraude massificada, e nele reside o potencial de efetividade da lei. O vetor sancionatório — a escalada das penas cominadas — repete fórmula cuja ineficácia preventiva a criminologia vem apontando há décadas, ao custo de desproporções internas que a doutrina já qualificou como desarranjo sistemático. A experiência dirá se os novos instrumentos serão utilizados para desmontar organizações ou se a lei se somará ao acervo do direito penal simbólico.

Como agenda de pesquisa futura, sugere-se o acompanhamento empírico da aplicação da figura da conta laranja — em especial do tratamento judicial dos cedentes vulneráveis —, a avaliação do impacto da ação incondicionada sobre o volume e a qualidade das persecuções por fraude digital e o estudo da interação entre a nova disciplina penal e os mecanismos regulatórios

de prevenção a fraudes do sistema financeiro, campo em que a resposta ao estelionato digital será, necessariamente, interinstitucional.

REFERÊNCIAS

AGÊNCIA BRASIL. Denúncias de crimes cibernéticos crescem 28% em 2025, mostra Safernet. Brasília, DF: Empresa Brasil de Comunicação, fev. 2026. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2026-02/denuncias-de-crimes-ciberneticos-crescem-28-em-2025-mostra-safernet. Acesso em: 21 jul. 2026.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 jul. 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Rio de Janeiro, RJ: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 jul. 2026.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet [...]. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 21 jul. 2026.

BRASIL. Lei nº 14.478, de 21 de dezembro de 2022. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais [...]. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14478.htm. Acesso em: 21 jul. 2026.

BRASIL. Lei nº 15.397, de 30 de abril de 2026. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), a fim de majorar as penas previstas para os crimes de furto, roubo, estelionato, receptação [...]. Brasília, DF: Presidência da República, 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/L15397.htm. Acesso em: 21 jul. 2026.

BRASIL. Superior Tribunal de Justiça. Conflito de Competência 185.983. Relator: Min. Joel Ilan Paciornik. Terceira Seção. Julgado em 2022. (2022).

CONVERGÊNCIA DIGITAL. Ataques hackers crescem 44% em junho e Brasil ultrapassa 4 mil ciberataques semanais por empresa. Jul. 2026. Disponível em: https://convergenciadigital.com.br/mercado/ataques-hackers-crescem-44-em-junho-e-brasil-ultrapassa-4-mil-ciberataques-semanais-por-empresa/. Acesso em: 21 jul. 2026.

COSTA, Adriano Sousa; ENALDO, Francisco; BRETZ, William. Considerações práticas sobre a Lei 15.397/2026. Meu Site Jurídico, Editora JusPodivm, 13 maio 2026. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2026/05/13/consideracoes-praticas-sobre-a-lei-15-397-2026/. Acesso em: 21 jul. 2026.

CROWDSTRIKE. CrowdStrike 2026 Financial Services Threat Landscape Report. Austin, 2026. Disponível em: https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-financial-services-threat-landscape-report/. Acesso em: 21 jul. 2026.

JORIO, Israel Domingos; BOLDT, Raphael. Comentários à Lei 14.155/2021 (III): as alterações no art. 171, §§ 2º-A e 2º-B do CP (fraude eletrônica). Empório do Direito, 21 ago. 2021. Disponível em: https://emporiododireito.com.br/leitura/comentarios-a-lei-14-155-2021-iii-as-alteracoes-no-art-171-2-a-e-2-b-do-cp-fraude-eletronica. Acesso em: 21 jul. 2026.

SANTOS, Marco Aurelio Fernandes dos. Estelionato digital: o novo protagonismo do MP na Lei 15.397/26. Migalhas, 8 maio 2026. Disponível em: https://www.migalhas.com.br/depeso/455295/estelionato-digital-o-novo-protagonismo-do-mp-na-lei-15-397-26. Acesso em: 21 jul. 2026.

SANTOS, Rafa. Lei de crimes patrimoniais traz avanços, mas repete punitivismo. Consultor Jurídico, São Paulo, 6 maio 2026. Disponível em: https://www.conjur.com.br/2026-mai-06/lei-de-crimes-patrimoniais-moderniza-tipos-penais-mas-repete-punitivismo/. Acesso em: 21 jul. 2026.

SENADO FEDERAL. Sancionado aumento de penas para furto, roubo e receptação. Agência Senado, Brasília, DF, 4 maio 2026. Disponível em: https://www12.senado.leg.br/noticias/materias/2026/05/04/sancionado-aumento-de-penas-para-furto-roubo-e-receptacao. Acesso em: 21 jul. 2026.

YAROCHEWSKY, Leonardo Isaac. Lei 15.397/2026: uma lei desarranjada. Jornal de Ciências Criminais — IBCCRIM, São Paulo, 4 maio 2026. Disponível em: https://jcc.ibccrim.org.br/colunistas/lei-15-397-2026-uma-lei-desarranjada/. Acesso em: 21 jul. 2026.