A CRIAÇÃO DE UM BANCO DE DADOS DE CONDENADOS POR FRAUDES DIGITAIS: UMA MEDIDA NECESSÁRIA PARA O COMBATE À CRIMINALIDADE DIGITAL

THE CREATION OF A DATABASE OF INDIVIDUALS CONVICTED OF ELECTRONIC FRAUD: A NECESSARY MEASURE TO COMBAT DIGITAL CRIME

João Carlos Ermelindo Bernardo[1]

DATA DE RECEBIMENTO: 12/10/2024
DATA DE APROVAÇÃO: 19/12/2025

RESUMO: Este artigo analisa a migração da criminalidade para o ambiente digital, com ênfase no crescimento exponencial das fraudes eletrônicas nas últimas décadas. Examina-se a evolução normativa no Brasil, especialmente a Lei nº 14.155/2021, que tipificou o furto mediante fraude eletrônica e o estelionato eletrônico, bem como as medidas internacionais decorrentes da Convenção de Budapeste sobre o Crime Cibernético. A pesquisa evidencia que as fraudes digitais apresentam características próprias, marcadas por modus operandi sofisticados e pela reincidência dos agentes, impulsionada pela sensação de impunidade. Destaca-se, ainda, a vulnerabilidade das vítimas e a complexidade investigativa desses delitos. Com base em experiências estrangeiras, defende-se a criação de um banco de dados nacional de condenados por fraudes digitais como instrumento essencial para a prevenção e repressão desses crimes, o que reforça a atuação investigativa, reduzindo a reincidência e afasta a percepção de impunidade.

PALAVRAS-CHAVE: Fraudes digitais; estelionato eletrônico; furto mediante fraude eletrônica; Lei nº 14.155/2021; Convenção de Budapeste; banco de dados criminal.

ABSTRACT: This article analyzes the migration of crime into the digital environment, focusing on the exponential growth of electronic fraud in recent decades. It examines the legal developments in Brazil, particularly Law No. 14.155/2021, which criminalized electronic fraud and online scam offenses, as well as the international measures arising from the Budapest Convention on Cybercrime. The study demonstrates that digital fraud has distinctive features, characterized by sophisticated modus operandi and the offenders' tendency to recidivism, often encouraged by the perception of impunity. It also highlights the vulnerability of victims and the investigative challenges posed by such crimes. Drawing on foreign experiences, the paper argues for the creation of a national database of individuals convicted of digital fraud as an essential tool for preventing and repressing these offenses, strengthening investigative work, reducing recidivism, and countering the perception of impunity.

[1] Aluno da graduação da Faculdade de Direito de São Bernardo do Campo. Contato: joao.c.bernardo@direitosbc.br

KEYWORDS: Digital fraud; online scam; electronic fraud theft; Law No. 14.155/2021; Budapest Convention; criminal database.

1 DAS NOVAS TECNOLOGIAS E SEU IMPACTO QUANTO ÀS FRAUDES DIGITAIS

Desde os primórdios, a busca pela interação e pela troca de conhecimento entre os seres humanos já evidenciava um caráter curioso e obstinado no desejo de dinamizar e aproximar as relações sociais, que ao longo dos séculos se aprofundou até alcançar um marco decisivo com a criação da Internet, hoje reconhecida como ferramenta indispensável na era moderna. Tal invenção possibilitou inúmeros avanços e benefícios nas esferas pessoal, profissional, cultural e econômica da vida dos cidadãos, impulsionada pela vontade de expansão das diversas áreas de interesse social. Contudo, também abriu espaço para o surgimento de novas formas de criminalidade, uma vez que a ambição humana e os meios utilizados para alcançar determinados resultados nem sempre se alinham ao que é admitido pela ordem estabelecida.

Com efeito, o cenário internacional revela números alarmantes no tocante ao avanço das fraudes eletrônicas. Apenas em 2024, a Índia registrou aproximadamente 3,6 milhões de incidentes de fraudes financeiras, que resultaram em prejuízos estimados em mais de ₹22.845 crore. Esse montante representa um crescimento de 206% em relação ao ano de 2023, quando as perdas totalizaram cerca de ₹7.465 crore. Os dados demonstram não apenas a dimensão econômica do problema, mas também a velocidade com que esse tipo de criminalidade tem se expandido em países emergentes, impulsionada pela massificação dos meios digitais de pagamento e a crescente conectividade da população[2].

No Reino Unido, um recente relatório da UK Finance revela um expressivo aumento nas fraudes do tipo *remote purchase*, forma na qual criminosos utilizam dados de cartões roubados para efetuar compras online, por telefone ou via correio,

[2] "India's cyber fraud epidemic: Rs 22,845 crore lost in 2024; 206% jump from previous year, says government." *Times of India*, 22 jul. 2025. Disponível em: https://timesofindia.indiatimes.com/business/cybersecurity/indias-cyber-fraud-epidemic-rs-22845-crore-lost-in-just-a-year-206-jump-from-previous-year-says-government/articleshow/122840099.cms. Acesso em: 29 set. 2025.

muitas vezes de modo a induzir as vítimas a fornecer códigos de uso único (OTPs). Em 2024, os casos dessa modalidade fraudulenta cresceram 22% e alcançaram quase 2,6 milhões de incidentes, enquanto as perdas aumentaram 11% e totalizaram aproximadamente £400 milhões. Essa escalada contribuiu substancialmente para que o montante total de fraudes não autorizadas no país atingisse £722 milhões, com 3,13 milhões de ocorrências – evolução de 14% em relação ao ano anterior[3].

Nessa mesma esteira, um estudo intitulado *"Which countries are most affected by online fraud?"* apontou que os Estados Unidos ocupam a liderança entre os países mais afetados por fraudes online, seguidos por França, Reino Unido, Irlanda e Dinamarca. O levantamento demonstra que, embora a ameaça seja global, certas regiões apresentam maior vulnerabilidade, seja pela amplitude do mercado digital, seja pela atratividade econômica para criminosos. A constatação reforça a necessidade de medidas preventivas e políticas de cibersegurança mais robustas, sobretudo em países desenvolvidos, nos quais o grande volume de transações eletrônicas amplia o risco e a exposição a ataques fraudulentos[4].

Em âmbito nacional, dados recentes apontam um crescimento substancial da criminalidade digital. Em 2024, fraudes financeiras em canais eletrônicos e cartões aumentaram 17%, saltando de R$ 8,6 bilhões para R$ 10,1 bilhões em perdas, segundo dados da Febraban, sendo que golpes via PIX foram responsáveis por R$ 2,7 bilhões dessas perdas, o que representa um aumento de 43%[5]. Na mesma toada, o Indicador de Tentativas de Fraude da Serasa Experian registrou que, em janeiro de 2025, foram evitadas 1.242.093 tentativas de golpe — um volume recorde — o que representa um crescimento de 41,6% em comparação a janeiro de 2024[6].

Nessa toada, de acordo com dados coletados por meio da Lei de Acesso à Informação, constatou-se um aumento de aproximadamente 800% nos registros de

---

[3] "Remote purchase' fraud in UK surges as customers tricked into disclosing passcodes." *The Guardian*, 28 mai. 2025. Disponível em: https://www.theguardian.com/money/2025/may/28/remote-purchase-fraud-uk-surges-customers-tricked-passcodes. Acesso em: 29 set. 2025.

[4] MONSTERSGAME. *Which countries are most affected by online fraud? Study reveals*. Disponível em: https://www.monstersgame.co.uk/technology/which-countries-are-most-affected-by-online-fraud-study-reveals/. Acesso em: 29 set. 2025.

[5] "Fraudes em canais eletrônicos crescem 17% e golpes via Pix aumentam 43% em um ano." *Sindicato dos Empregados em Estabelecimentos Bancários – Tubarão*, 11 mar. 2025. Disponível em: https://www.bancariostb.com.br/noticia/fraudes-em-canais-eletronicos-crescem-17-e-golpes-via-pix-aumentam-43-em-um-ano/. Acesso em: 29 set. 2025.

[6] Brasil tem recorde nas tentativas de fraude registradas em janeiro, aponta Serasa Experian." *Serasa Experian*, 17 abr. 2025. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/indicadores/brasil-tem-recorde-nas-tentativas-de-fraude-registradas-em-janeiro-aponta-serasa-experian/. Acesso em: 29 set. 2025.

crimes digitais no Brasil entre os anos de 2020 e 2025. Entre as condutas mais recorrentes figuram o estelionato digital, o furto mediante fraude eletrônica e a invasão de dispositivos informáticos, fenômeno que evidencia não apenas a sofisticação das práticas ilícitas em ambiente virtual, mas também a urgência de uma resposta normativa e repressiva compatível com a gravidade do risco social envolvido[7].

Consigne-se que em razão das transformações tecnológicas e sociais das últimas décadas, o que se observa, em nível global, é uma clara migração da criminalidade para o uso de recursos eletrônicos e informáticos como instrumentos de perpetuação da delinquência, tendo a fraude como principal mecanismo nesse processo. Como ressalta o estudo *Responding to victimisation in a digital world: a case study of fraud and computer misuse reported in Wales*, os avanços digitais não apenas facilitaram a comunicação e o acesso à informação, mas também ampliaram as oportunidades de atuação criminosa, o que permitiu a consolidação de golpes e esquemas fraudulentos em escala global[8].

Diante desse cenário, impõe-se a necessidade de uma análise acerca da adoção de políticas públicas voltadas ao combate das fraudes eletrônicas, sobretudo em razão de seu crescimento exacerbado. Tal reflexão mostra-se essencial não apenas para avaliar a eficácia das medidas já implementadas, mas também para identificar lacunas normativas e operacionais que permitam a expansão dessas práticas ilícitas.

2 DAS FRAUDES DIGITAIS

Com as alterações promovidas pela Lei nº 14.155/2021, o Código Penal passou a tipificar, de forma específica, duas modalidades centrais de fraude eletrônica: o furto mediante fraude cometido por meio eletrônico (art. 155, § 4º-B) e o estelionato eletrônico (art. 171, § 2º-A).

---

[7] BAGUETE. *Crimes digitais crescem 800% em cinco anos*. Disponível em:https://www.baguete.com.br/noticias/crimes-digitais-crescem-800-em-cinco-anos?utm. Acesso em: 1 out. 2025.

[8] CORREIA, Sara Giro. *Responding to victimisation in a digital world: a case study of fraud and computer misuse reported in Wales*. Crime Science, v. 8, art. 4, 2019. Disponível em: https://doi.org/10.1186/s40163-019-0099-7. Acesso em: 1 out. 2025.

Quanto à primeira figura, trata-se da forma qualificada do furto cometido mediante fraude. Nessa modalidade, o agente subtrai coisa alheia móvel, para si ou para outrem, por meio de dispositivo eletrônico ou informático, esteja conectado ou não à rede de computadores, independentemente da violação de mecanismos de segurança ou do uso de programas maliciosos[9].

No que se refere à segunda figura, a qualificadora incide quando o agente obtém, para si ou para outrem, vantagem ilícita em prejuízo de terceiro, mediante fraude baseada em informações fornecidas pela própria vítima ou por outra pessoa induzida em erro, seja por meio de redes sociais, contatos telefônicos, correio eletrônico ou qualquer outro mecanismo fraudulento equivalente[10].

Bitencourt obtempera que a semelhança entre os delitos reside principalmente na utilização de fraude e de meios tecnológicos como *modus operandi* para a sua prática[11].

Nessa trilha, conforme o magistério de Mirabete, a fraude é o expediente utilizado para levar alguém ao erro, a fim de que este atue com uma falsa representação da realidade. A fraude pode se manifestar pelo artifício, de natureza predominantemente material, ardil, de natureza predominantemente moral, ou por qualquer outro ato insidioso, clandestino ou enganoso[12].

Por outro turno, o termo dispositivo designa qualquer equipamento, mecanismo ou componente concebido para o desempenho de uma função específica, enquanto a informática corresponde à ciência dedicada ao tratamento de informações

---

[9] "Art. 155 – Subtrair, para si ou para outrem, coisa alheia móvel:
Pena – reclusão, de um a quatro anos, e multa.
§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo." (BRASIL. Código Penal. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 29 set. 2025).

[10] "Art. 171 – 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:
Pena – reclusão, de um a cinco anos, e multa.
§ 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 ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo." (BRASIL. Código Penal. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 29 set. 2025).

[11] BITENCOURT, Cezar Roberto. *Furto mediante uso de dispositivo eletrônico ou informático*. Consultor Jurídico, 14 jun. 2021. Disponível em: https://www.conjur.com.br/2021-jun-14/bitencourt-furto-mediante-uso-dispositivo-eletronico-ou-informatico/. Acesso em: 30 set. 2025.

[12] MIRABETE, Julio Fabbrini; FABBRINI, Renato N. *Manual de direito penal: parte especial arts. 121 a 234-B do CP*. 37. ed. Indaiatuba: Editora Foco, 2024, p. 92.

por meio de computadores ou outros aparelhos de processamento de dados. Assim, entende-se por dispositivo eletrônico ou informático todo sistema ou aparelho apto a viabilizar eletronicamente o armazenamento, o processamento ou a transmissão de dados e informações, abrangendo computadores de diferentes espécies (desktops, notebooks, tablets, servidores), seus componentes e periféricos, bem como outros equipamentos que permitam tais operações, ainda que possam desempenhar funções diversas[13].

É salutar destacar que a diferença central entre essas duas figuras típicas está no verbo núcleo do tipo. No furto mediante fraude eletrônica, o agente subtrai a coisa alheia móvel — isto é, toma o bem sem a anuência da vítima. Já no estelionato eletrônico, a própria vítima entrega a vantagem indevida, induzida em erro, uma vez que sua manifestação de vontade encontra-se viciada pelo meio fraudulento empregado[14]. Para além disso, no primeiro delito a fraude é utilizada para burlar a vigilância da vítima e permitir a subtração, enquanto no estelionato o agente falsifica a realidade para fazer com que a vítima realize a entrega, de modo espontâneo, da vantagem indevida desejada pelo sujeito ativo.

No que tange aos sujeitos ativos nos crimes de furto mediante fraude eletrônica e estelionato eletrônico, evidenciam-se características comuns que remontam a perfis com conhecimento tecnológico acima da média e tendência à reincidência. Estudos como *s* mostram que muitos agentes desses crimes dominam ferramentas digitais, têm familiaridade com redes, sistemas de pagamento online ou engenharia social, o que facilita a concepção e execução de fraudes complexas[15]. Além disso, pesquisas comparativas indicam que não são hábitos isolados de atuação criminal: esses agentes frequentemente repetem a prática, impulsionados pela percepção de que o risco de identificação é baixo, pela sensação de impunidade e pelo retorno financeiro rápido. Esse padrão reforça que, para eles, cometer um golpe não é um ato único, mas parte de uma trajetória criminosa sustentada, estimulada

[13] MIRABETE; FABBRINI, *Manual de direito penal*, p. 459.

[14] CONTIERI, Nichollas Flávio. *O fundamento da diferença entre furto mediante fraude e estelionato*. Escola da Magistratura do Paraná – EMAP, 2019. Disponível em: https://www.emap.com.br/wp-content/uploads/2019/11/NICHOLLAS-FLAVIO-CONTIERI.pdf. Acesso em: 29 set. 2025.

[15] ANDEREZ, Dario Ortega; KANJO, Eiman; ANWAR, Amna; JOHNSON, Shane D.; LUCY, David. *The Rise of Technology in Crime Prevention: Opportunities, Challenges and Practitioners' Perspectives*. Preprint, 26 jan. 2021. Disponível em: https://doi.org/10.48550/arXiv.2102.04204. Acesso em: 01 out. 2025.

pelas possibilidades que os meios eletrônicos oferecem — anonimato, escala, baixa supervisão — bem como pela ausência de consequências efetivas[16].

De outro vértice, as vítimas de fraudes digitais frequentemente pertencem a perfis de vulnerabilidade: idosos, pessoas com menor familiaridade com recursos tecnológicos, pouca informação sobre segurança digital, e com maior confiança nas relações interpessoais. Estudos apontam que idosos (especialmente acima de 75 anos) enfrentam perdas financeiras maiores e têm maior probabilidade de vitimização repetida, embora relatem menos os incidentes[17]. Fatores como declínio cognitivo, confiança excessiva, solidão, sair pouco de casa ou morar sozinho, e desconhecimento técnico são frequentemente mencionados como elementos que facilitam a ação fraudulenta. Esse perfil vulnerável não é apenas passivo: os golpes exploram precisamente essas fragilidades, induzem ao erro, manipulam emoções ou criam sensação de urgência, o que, em última análise, possibilita a consumação dos ilícitos — seja pela subtração direta praticada pelo agente, seja pela obtenção da vantagem indevida a partir da própria vítima[18].

Por sua vez, os métodos de execução das fraudes digitais revelam constante inventividade e adaptação às tecnologias disponíveis. Os agentes utilizam a engenharia social para elaborar narrativas críveis que reduzem a cautela das vítimas, valem-se de técnicas tradicionais como *phishing*, *smishing* e *vishing* para capturar credenciais, recorrem a expedientes como *SIM swap* e *account takeover* para assumir o controle de contas, além de empregarem programas maliciosos, *keyloggers* e páginas falsas destinadas à obtenção automatizada de dados. Mais recentemente, exploram recursos como *deepfakes*, robôs virtuais e anúncios fraudulentos em plataformas de comércio eletrônico, o que confere aparência de legitimidade às práticas ilícitas. Tais condutas, frequentemente organizadas em etapas de reconhecimento, contato, exploração e lavagem, aproveitam-se de redes sociais,

---

[16] MISRA, Gaurav; JUNGER, Marianne; MONTOYA, Lorena. *A Cross-National Study on Cybercrime: Incident, Suspect and Victim Characteristics for Digital and Traditional Fraud in the Netherlands and Kolkata, India*. *Journal of Forensic Sciences & Criminal Investigation*, v. 10, n. 5, 2018. Disponível em: https://juniperpublishers.com/jfsci/JFSCI.MS.ID.555634.php?utm. Acesso em: 01 out. 2025.

[17] HAVERS, Benjamin; TRIPATHI, Kartikeya; BURTON, Alexandra; McMANUS, Sally; COOPER, Claudia. *Cybercrime victimisation among older adults: A probability sample survey in England and Wales*. *International Journal of Law and Psychiatry*, 2023. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC11654966/?utm.Acesso em: 01 out. 2025.

[18] SHANG, Yuxi; WU, Zhongxian; DU, Xiaoyu; JIANG, Yanbin; MA, Beibei; CHI, Meihong. *The psychology of the internet fraud victimization of older adults: A systematic review*. *Frontiers in Psychology*, 5 set. 2022. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC9484557/?utm. Acesso em: 01 out. 2025

aplicativos de mensagens e serviços de pagamento instantâneo para ampliar o alcance e a velocidade da execução. A multiplicidade de meios evidencia não apenas a sofisticação das fraudes, mas também a dificuldade de identificação dos autores e de reparação dos danos[19]. Neste sentido, a Corte Bandeirante possui precedentes que demonstram a diversidade de formas na prática dessas fraudes (grifos nossos):

> DIREITO PENAL. APELAÇÃO. ESTELIONATO ELETRÔNICO. RECURSO PARCIALMENTE PROVIDO. I. Caso em Exame **O apelante foi condenado por estelionato eletrônico, praticado por meio de envio de comprovantes falsos de pagamento via pix, visando enganar a vítima, proprietário de uma lanchonete, em quatro ocasiões.** A pena inicial foi de cinco anos de reclusão em regime semiaberto e pagamento de doze dias-multa. II. Questão em Discussão 2. A questão em discussão consiste em: (i) possibilidade de reconhecimento da insignificância; (ii) aplicação da atenuante da confissão; (iii) aplicação do estelionato privilegiado; (iv) redução da pena e substituição por pena restritiva de direitos; (v) fixação de regime aberto; (vi) isenção de custas. III. Razões de Decidir 3. A palavra da vítima, corroborada por testemunha policial, foi considerada válida e suficiente para embasar a condenação, não havendo incongruências ou interesses que desvirtuem os depoimentos. 4. O valor do prejuízo, superior a 1/10 do salário-mínimo, afasta a aplicação do princípio da insignificância. A reiteração delitiva e o modus operandi indicam alta reprovabilidade da conduta. IV. Dispositivo e Tese 5. Recurso parcialmente provido para aplicar o estelionato privilegiado, substituindo a reclusão por detenção, mantendo-se o regime semiaberto e a condenação em custas, com pagamento suspenso até que o condenado tenha condições de realizá-lo sem prejuízo do sustento próprio ou da família. Tese de julgamento: 1. A palavra da vítima pode embasar condenação quando firme e harmônica com demais provas. 2. O princípio da insignificância não se aplica a valores superiores a 1/10 do salário-mínimo e a condutas de alta reprovabilidade. Legislação Citada: Código Penal, art. 171, caput e §2º-A; art. 71, caput. Código de Processo Penal, art. 202, 206, 207, 156. Código de Processo Civil, art. 98, §1º, inciso I, §3º. Jurisprudência Citada: STJ, AgRg no AREsp nº 143.681/SP, Rel. Min. Arnaldo Esteves Lima, Quinta Turma, DJe 2.8.2010. STF, RHC nº 114966, Rel. Min. Rosa Weber, DJ de 08.05.13. STF, HC nº 84.412/SP, Rel. Min. Celso de Mello. (TJSP; Apelação Criminal 1500840-87.2023.8.26.0079; Relator (a): Mens de Mello; Órgão Julgador: 7ª Câmara de Direito Criminal; Foro de Botucatu - 1ª Vara Criminal; Data do Julgamento: 02/07/2025; Data de Registro: 02/07/2025)[20].

> APELAÇÃO CRIMINAL – FURTO SIMPLES E FURTO MEDIANTE FRAUDE ELETRÔNICA – **Ré que subtrai o celular da vítima e se vale da senha nele instalada, na galeria do aparelho, para contrair despesas junto a estabelecimentos comerciais** – Materialidade delitiva e autoria demonstradas – Penas redimensionadas – Circunstâncias judiciais desfavoráveis que autorizam a majoração da pena-base – Fração de 1/6 mais consentânea – Continuidade delitiva – Reconhecida com inclusão também do furto simples, mantida a fração de 1/4.– Regime prisional semiaberto – Subsistência. Recurso parcialmente provido. (TJSP; Apelação Criminal 1502813-04.2023.8.26.0168; Relator (a): Antonio B. Morello; Órgão Julgador:

[19] ZHANG, Chuo Jun; GILL, Asif Q.; LIU, Bo; ANWAR, Memoona J. *AI-based identity fraud detection: a systematic review*. 2025. Disponível em:https://arxiv.org/abs/2501.09239?utm. Acesso em: 1 out. 2025.
[20] TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Acórdão nº 19.421.308. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=19421308&cdForo=0. Acesso em: 1 out. 2025.

> 10ª Câmara de Direito Criminal; Foro de Dracena - 3ª Vara; Data do Julgamento: 21/03/2025; Data de Registro: 21/03/2025)[21].
>
> DIREITO PENAL. APELAÇÃO CRIMINAL. FURTO QUALIFICADO. PARCIAL PROVIMENTO. I. Caso em Exame 1. **Réus condenados por furto qualificado em caixas eletrônicos, com manipulação indevida de terminais para acessar contas de vítimas.** Apelação busca desclassificação para furto simples e readequação da dosimetria penal. II. Questão em Discussão 2. A questão em discussão consiste em determinar se a conduta dos réus pode ser desclassificada para furto simples e se a dosimetria penal foi adequadamente aplicada. III. Razões de Decidir 3. A conduta dos réus foi praticada com manipulação indevida de terminais eletrônicos, caracterizando furto qualificado. 4. A dosimetria penal foi reavaliada em benefício dos indigitados, considerando a culpabilidade exacerbada e as circunstâncias judiciais desfavoráveis. IV. Dispositivo e Tese 5. Recurso parcialmente provido para readequar a dosimetria penal. Tese de julgamento: 1. A manipulação indevida de terminais eletrônicos caracteriza furto qualificado. 2. A dosimetria penal deve considerar a culpabilidade e circunstâncias judiciais desfavoráveis. _____ Legislação Citada: Código Penal, art. 155, § 4º-B e § 4º-C, inciso II; art. 14, inciso II; art. 29, caput; art. 33, § 2º e § 3º; art. 44, I, II, III; art. 77, caput, I e II. Jurisprudência Citada: STJ, AgRg no AgRg nos EDcl no AREsp 1617439 PR. STF, HC 174749 AgR, Rel. Min. Alexandre de Moraes, Primeira Turma, j. 20.09.2019. (TJSP; Apelação Criminal 1500252-58.2024.8.26.0560; Relator (a): J. E. S. Bittencourt Rodrigues; Órgão Julgador: 13ª Câmara de Direito Criminal; Foro de Votuporanga - 2ª Vara Criminal e Da Infância e Juventude; Data do Julgamento: 28/08/2025; Data de Registro: 28/08/2025)[22].

Com efeito, as diversas formas de execução das fraudes digitais não apenas obscurecem a identificação dos infratores, como também apontam para padrões específicos no *modus operandi* de cada agente. Ao empregar diferentes artifícios, o delinquente evidencia uma adaptação estratégica ao ambiente digital e às características das vítimas. Essa multiplicidade de formas permite que o agente alterne entre técnicas mais visíveis e outras mais sutis, de modo a evitar detecção policial ou judicial, o que revela também suas "assinaturas" particulares, tais como a escolha de plataformas, horários específicos, tipos de mensagens ou apelos persuasivos[23].

---

[21] TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Acórdão nº 19.016.309. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=19016309&cdForo=0. Acesso em: 01 out. 2025.

[22] TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Acórdão nº 19.639.856. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=19639856&cdForo=0. Acesso em: 01 out. 2025.

[23] EZE, Thomas Chukwuma; OKONKWO, Patrick; AMADI, Chinedu. *Cybercrime Modus Operandi: Computer Misuses*. American Journal of Research in Computer Science, v. 7, n. 1, 2025. Disponível em: https://sdiopr.s3.ap-south-1.amazonaws.com/2025/JANUARY/14_Jan_2025/2024_AJRCOS_128138/Rev_AJRCOS_128138_Eze_A.pdf?utm. Acesso em: 01 out. 2025.

Nesse quadro, revela-se imprescindível a formulação e implementação de políticas criminais adequadas, capazes de acompanhar a dinamicidade das condutas delitivas em ambiente digital.

3 DAS POLÍTICAS CRIMINAIS DE COMBATE A FRAUDES DIGITAIS

Cumpre consignar, *ab initio*, que o marco pioneiro no ordenamento jurídico brasileiro quanto às fraudes digitais consiste na Lei nº 14.155/2021, responsável pela tipificação dos delitos de furto mediante fraude praticado por meio eletrônico ou informático, bem como do estelionato eletrônico. Antes de sua vigência, já se encontravam em vigor diplomas normativos que disciplinam condutas relacionadas aos crimes cibernéticos, estabelecem diretrizes para o uso responsável da internet e preveem medidas de proteção aos dados dos utentes dos sistemas tecnológicos, *ad exemplum*, a Lei nº 12.737/2012 ("Lei Carolina Dieckmann"), a Lei nº 12.965/2014 (Marco Civil da Internet) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD). Todavia, nenhuma das referidas normas, embora de inegável relevância para a tutela do ambiente digital, tipificou o delito de fraude digital.

Nesse sentido, a Lei nº 14.155 de 2021 culminou pena de reclusão de quatro a oito anos e multa aos crimes de estelionato eletrônico e furto mediante fraude cometido por meio eletrônico ou informático[24]. Cuida-se de *lex gravior*, o escopo do legislador foi exasperar o tratamento dado aos delinquentes que praticarem as fraudes por meio digital[25].

[24] BRASIL. Lei nº 14.155, de 27 de maio de 2021. "Art. 155. Subtrair, para si ou para outrem, coisa alheia móvel: [...] § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo."
"Art. 171. 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: [...]
§ 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 ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo."

[25] COSTA, Adriano Sousa; GUIMARÃES, Gustavo Ribeiro Costa Rigo; TORRES, Thiago. Questões práticas sobre o estelionato após as Leis 13.964/2019 e 14.155/2021. *Consultor Jurídico (ConJur)*, São Paulo, 28 set. 2021. Disponível em: https://www.conjur.com.br/2021-set-28/academia-policia-questoes-praticas-estelionato-leis-139642019-141552021. Acesso em: 1 out. 2025

Para além disso, a lei mencionada também trouxe majorante caso a fraude digital seja cometida mediante a utilização de servidor mantido fora do território nacional ou contra idoso ou pessoa vulnerável, considerada, em ambos os casos, a relevância do resultado gravoso[26].

Em âmbito processual, a Lei nº 14.155/2021 alterou o Código de Processo Penal e estabeleceu que, nos casos em que o estelionato seja praticado mediante emissão de cheques sem provisão de fundos em poder do sacado, com pagamento frustrado ou por meio de transferência de valores, a competência será definida pelo domicílio da vítima e, em caso de pluralidade de vítimas, pela prevenção[27].

Na mesma toada, a Convenção sobre o Crime Cibernético, assinada em Budapeste, aprovada pelo Decreto Legislativo nº 37/2021 e promulgada pelo Decreto nº 11.491/2023, estabelece medidas destinadas ao combate da criminalidade digital[28]. Seu artigo 8, b, estabelece que os Estados-partes devem tipificar, em sua legislação interna, condutas dolosas e não autorizadas que causem prejuízo a terceiros por meio de qualquer interferência no funcionamento de um computador ou de um sistema de computadores, realizada com a intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita[29]. Na mesma linha, o artigo 13, 1 da Convenção prevê a

---

[26] BRASIL. Lei nº 14.155, de 27 de maio de 2021. "Art. 155. [...]
§ 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável."
"Art. 171. [...]
§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
§ 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.".

[27] BRASIL. Lei nº 14.155, de 27 de maio de 2021. "Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
§ 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.".

[28] CONVENÇÃO SOBRE O CRIME CIBERNÉTICO (Budapeste, 23 de novembro de 2001). Promulgada no Brasil pelo Decreto nº 11.491, de 12 de abril de 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 30 set. 2025.

[29] CONVENÇÃO SOBRE O CRIME CIBERNÉTICO (Budapeste, 23 de novembro de 2001). Art. 8 – Fraude informática: "Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, a conduta de quem causar, de forma dolosa e não autorizada, prejuízo patrimonial a outrem por meio de: a) qualquer inserção, alteração, apagamento ou supressão de dados de computador; b) qualquer interferência no funcionamento de um computador ou de um sistema de computadores, realizada com a intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita.".

adoção de sanções criminais eficazes, adequadas e dissuasivas, dentre as quais a privação de liberdade[30].

Nada obstante relevantes as mudanças trazidas, não foram suficientes para a mitigação das ocorrências de fraudes digitais, que, vale dizer, continuam em ascensão[31].

De outro vértice, algumas nações contam com bancos de dados que reúnem informações relativas aos condenados por fraudes digitais, com descrição pormenorizada dos agentes e das condutas criminosas praticadas, medida que, *a priori*, mostra-se eficiente no combate às fraudes digitais.

Um exemplo é o *Internet Crime Complaint Center* (IC3) do FBI, entidade norte-americana especializada no recebimento e análise de denúncias relacionadas a crimes cibernéticos, especialmente fraudes digitais, roubos de identidade e golpes que utilizam a internet como meio ou instrumento. As vítimas submetem queixas por meio de portal eletrônico, no qual se coletam dados como o tipo de transação, valores perdidos, informações do autor (quando disponíveis) e os dispositivos usados no golpe[32]. A efetividade do sistema se evidencia na capacidade do IC3 não só de contabilizar ocorrências mas de possibilitar rastreamento e recuperação de ativos com sucesso. No relatório anual de 2020, por exemplo, o IC3 identificou 791.790 denúncias, com perdas superiores a US$ 4,1 bilhões, e, por meio do *Recovery Asset Team* (RAT), foram congelados aproximadamente US$ 380 milhões de um total de perdas reportadas de US$ 462 milhões — uma taxa de sucesso de quase 82% na recuperação de fundos[33]. Em 2023, o RAT iniciou 3.008 casos de *Financial Fraud Kill Chains*, com perdas estimadas em US$ 758,05 milhões, dos quais foram retidos cerca de US$ 538,39 milhões — o que equivale a aproximadamente 71% de êxito. Esse mecanismo inclusive auxilia no trabalho investigativo, pois os registros de queixas

[30] CONVENÇÃO SOBRE O CRIME CIBERNÉTICO (Budapeste, 23 de novembro de 2001). Art. 13 – Sanções e medidas: "Cada Parte adotará medidas legislativas e outras providências necessárias para assegurar que os crimes tipificados de acordo com os Artigos de 2 a 11 sejam punidos por meio de sanções criminais eficazes, adequadas e dissuasivas, que incluam a privação de liberdade.".

[31] BAGUETE. *Crimes digitais crescem 800% em cinco anos*. Disponível em: https://www.baguete.com.br/noticias/crimes-digitais-crescem-800-em-cinco-anos?utm. Acesso em: 1 out. 2025.

[32] *About – Internet Crime Complaint Center (IC3)*. Disponível em: https://www.ic3.gov/Home/About?utm. Acesso em: 1 out. 2025.

[33] *Internet Crime Complaint Center – 2020 Annual Report*. IC3 recebeu 791.790 queixas, com perdas reportadas superiores a US$ 4,1 bilhões. O *Recovery Asset Team* (RAT) conseguiu congelar cerca de US$ 380 milhões de um total de US$ 462 milhões, o que corresponde a uma taxa de sucesso de aproximadamente 82%. Disponível em: https://www.ic3.gov/AnnualReport/Reports/2020_ic3report.pdf?utm. Acesso em: 1 out. 2025.

permitem correlações entre casos semelhantes, facilitam a identificação do *modus operandi* dos infratores, possibilitam alertas a instituições financeiras e favorecem a cooperação entre jurisdições internacionais[34].

No Reino Unido, o *National Fraud Database* (NFD), mantido pela Cifas, constitui o principal mecanismo de prevenção e repressão a fraudes, ao centralizar informações relativas a práticas fraudulentas confirmadas ou tentadas[35]. Seu funcionamento baseia-se no compartilhamento de dados entre instituições financeiras, seguradoras, empresas de telecomunicações e órgãos públicos, que registram ocorrências de fraude e, em contrapartida, acessam o banco para verificar novos pedidos ou movimentações suspeitas. Tal dinâmica confere ao NFD caráter preventivo, pois permite identificar padrões de fraude, proteger potenciais vítimas e mitigar riscos antes que os ilícitos se consolidem[36]. A eficácia do sistema demonstra-se nos resultados práticos: apenas em 2024 foram registrados mais de 421 mil casos, sobretudo de fraudes de identidade, e estima-se que o uso compartilhado do banco de dados evitou perdas superiores a £ 2,1 bilhões[37].

Nesse sentido, a adoção de um sistema unificado de identificação de condenados por fraudes digitais revela-se instrumento essencial no enfrentamento dessa criminalidade. Cada fraudador deixa uma verdadeira impressão digital do crime, correspondente a um *modus operandi* singular, o que permite às autoridades reconhecer padrões e antecipar estratégias de investigação e prevenção. Por se tratar de práticas que exigem conhecimento técnico especializado, a existência de um cadastro centralizado reduz a reincidência ao facilitar a identificação de infratores já condenados e, por conseguinte, afasta a sensação de impunidade, o que reforça o caráter dissuasório das sanções. Ademais, esse banco de dados fornece parâmetros concretos para subsidiar investigações futuras e orientar a atuação estatal diante de

[34] *FBI Internet Crime Report 2023*. Disponível em: https://pt.scribd.com/document/835838296/FBI-Internet-Crime-Report-2023-1710798294-1?utm. Acesso em: 1 out. 2025.
[35] *Using data analytics to tackle fraud and error*. National Audit Office (Reino Unido). Disponível em: https://www.nao.org.uk/wp-content/uploads/2025/07/using-data-analytics-to-tackle-fraud-and-error.pdf?utm_. Acesso em: 1 out. 2025.
[36] *National Fraud Database – Cifas*. Disponível em: https://www.cifas.org.uk/fraud-prevention-community/combined-threat-protect/national-fraud-database?utm. Acesso em: 1 out. 2025.
[37] *Fraudscape 2025: record fraud levels – Cifas*. Disponível em: https://www.cifas.org.uk/newsroom/fraudscape-2025-record-fraud-levels?utm. Acesso em: 1 out. 2025.

novas modalidades de fraude digital, tal mecanismo eleva a eficácia das respostas repressivas e preventivas[38].

Com efeito, a sofisticação e a plasticidade dos métodos empregados pelos agentes tornam ineficazes respostas tradicionais de persecução penal, exigindo estratégias integradas que combinem prevenção, repressão e cooperação transnacional. Nesse sentido, a atuação estatal deve ser pautada não apenas pela atualização normativa, mas também pelo fortalecimento de mecanismos investigativos, tecnológicos e institucionais, de modo a oferecer uma resposta proporcional à complexidade da criminalidade eletrônica[39].

CONCLUSÕES

A evolução tecnológica transformou profundamente a dinâmica social e as formas de interação humana, mas também possibilitou a migração da criminalidade para o meio digital. Esse deslocamento da prática delitiva representou um marco no cenário criminal contemporâneo, pois inaugurou novas modalidades ilícitas, dentre as quais se destacam as fraudes digitais. O aumento desses delitos ocorreu de maneira constante e progressiva, e alcançou índices alarmantes em âmbito nacional e internacional, o que revela não apenas a sofisticação das práticas ilícitas, mas também a insuficiência das respostas tradicionais do sistema penal.

Com efeito, as fraudes digitais apresentam características próprias que as diferenciam das formas convencionais de criminalidade. O sujeito ativo desses delitos geralmente possui elevado conhecimento tecnológico e atua de maneira reiterada. Adotam métodos que configuram um verdadeiro modus operandi, identificável como uma “assinatura criminosa”. A multiplicidade de técnicas empregadas – que vai desde o phishing, smishing e vishing até o uso de *deepfakes* e softwares maliciosos – demonstra a plasticidade e a inventividade dos agentes, dificultando sobremaneira a atuação das autoridades competentes. O resultado é a perpetuação de um ciclo de

[38] Anna Gekoski; Joanna R. Adler; Tim McSweeney. *Profiling the Fraudster: Findings from a Rapid Evidence Assessment*. *Policing and Society*. Disponível em: https://www.tandfonline.com/doi/full/10.1080/17440572.2022.2137670?utm. Acesso em: 2 out. 2025.

[39] Fran Casino; Claudia Pina; Pablo López-Aguilar; Edgar Batista; Agustí Solanas; Constantinos Patsakis. *SoK: Cross-border Criminal Investigations and Digital Evidence*. arXiv, 25 maio 2022. Disponível em: https://arxiv.org/abs/2205.12911?utm. Acesso em: 1 out. 2025.

reincidência, que se sustenta pela sensação de impunidade e pelo retorno financeiro rápido, fatores que incentivam a continuidade da conduta delitiva.

As vítimas, por sua vez, geralmente pertencem a grupos vulneráveis, como idosos ou pessoas com baixo nível de conhecimento tecnológico. Essa vulnerabilidade potencializa o êxito das práticas fraudulentas, pois os criminosos exploram fragilidades cognitivas, emocionais e sociais, manipulam sentimentos como urgência, medo ou confiança excessiva.

Nesse contexto, a Lei nº 14.155/2021 representou um avanço significativo, ao tipificar expressamente o furto mediante fraude eletrônica e o estelionato eletrônico, além de estabelecer penas mais severas para tais práticas. Essa legislação respondeu a uma necessidade premente da sociedade, ao reconhecer a gravidade dos delitos digitais. Todavia, o contínuo crescimento dos casos demonstra que a simples alteração normativa não se revelou suficiente para frear as fraudes digitais. A situação exige uma resposta mais ampla, que vá além do endurecimento punitivo, e inclua políticas integradas de prevenção e repressão.

Experiências estrangeiras mostram-se exitosas nesse sentido. Países como os Estados Unidos e o Reino Unido já implementaram sistemas de bancos de dados de condenados por crimes digitais, os quais centralizam informações sobre os agentes e seus métodos, possibilitando a identificação de padrões criminosos, a prevenção de novos ilícitos e a redução da reincidência. Esses mecanismos fortalecem a atuação investigativa, pois permitem correlações entre casos e fornecem subsídios para políticas públicas de segurança digital. Além disso, reforçam o caráter dissuasório das sanções, ao afastar a percepção de impunidade que atualmente permeia a criminalidade virtual.

Diante desse panorama, a criação de um banco de dados nacional de condenados por fraudes digitais revela-se não apenas uma medida recomendável, mas uma exigência diante da magnitude do problema. O Brasil, como signatário da Convenção de Budapeste sobre o Crime Cibernético, assumiu o compromisso internacional de adotar medidas eficazes contra a criminalidade digital. A implementação de um sistema unificado de dados atenderia a esse compromisso, ao mesmo tempo em que contribuiria para a modernização da persecução penal e para a proteção efetiva da sociedade brasileira.

Conclui-se, portanto, que a evolução da criminalidade para o meio digital impõe ao Estado brasileiro a necessidade de ir além da legislação existente, através da adoção de instrumentos inovadores de combate às fraudes eletrônicas. A criação de um banco de dados de condenados por fraudes digitais se mostra, *a priori,* como providência eficaz para a repressão e a prevenção desses delitos que, nos cinco últimos anos, tiveram crescimento exponencial.

REFERÊNCIAS

ANDEREZ, Dario Ortega; KANJO, Eiman; ANWAR, Amna; JOHNSON, Shane D.; LUCY, David. ***The Rise of Technology in Crime Prevention***: *Opportunities, Challenges and Practitioners' Perspectives*. Preprint, 26 jan. 2021. Disponível em: https://doi.org/10.48550/arXiv.2102.04204. Acesso em: 01 out. 2025.

BAGUETE. **Crimes digitais crescem 800% em cinco anos**. Disponível em: https://www.baguete.com.br/noticias/crimes-digitais-crescem-800-em-cinco-anos?utm. Acesso em: 1 out. 2025.

BITENCOURT, Cezar Roberto. Furto mediante uso de dispositivo eletrônico ou informático. *In:* **Consultor Jurídico**, 14 jun. 2021. Disponível em: https://www.conjur.com.br/2021-jun-14/bitencourt-furto-mediante-uso-dispositivo-eletronico-ou-informatico/. Acesso em: 30 set. 2025.

BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 29 set. 2025.

BRASIL. **Decreto nº 11.491**, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada em Budapeste em 23 de novembro de 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 30 set. 2025.

CASINO, Fran; PINA, Claudia; LÓPEZ-AGUILAR, Pablo; BATISTA, Edgar; SOLANAS, Agustí; PATSAKIS, Constantinos. ***SoK****: Cross-border Criminal Investigations and Digital Evidence*. arXiv, 25 maio 2022. Disponível em: https://arxiv.org/abs/2205.12911?utm. Acesso em: 1 out. 2025.

CIFAS. **Fraudscape** 2025: record fraud levels – Cifas. Londres: Cifas, 2025. Disponível em: https://www.cifas.org.uk/newsroom/fraudscape-2025-record-fraud-levels?utm. Acesso em: 1 out. 2025.

CIFAS. **National Fraud Database** – Cifas. Londres: Cifas. Disponível em: https://www.cifas.org.uk/fraud-prevention-community/combined-threat-protect/national-fraud-database?utm. Acesso em: 1 out. 2025.

CONTIERI, Nichollas Flávio. **O fundamento da diferença entre furto mediante fraude e estelionato**. Escola da Magistratura do Paraná – EMAP, 2019. Disponível

em: https://www.emap.com.br/wp-content/uploads/2019/11/NICHOLLAS-FLAVIO-CONTIERI.pdf. Acesso em: 29 set. 2025.

CORREIA, Sara Giro. **Responding to victimisation in a digital world**: a case study of fraud and computer misuse reported in Wales. Crime Science, v. 8, art. 4, 2019. Disponível em: https://doi.org/10.1186/s40163-019-0099-7. Acesso em: 1 out. 2025.

COSTA, Adriano Sousa; GUIMARÃES, Gustavo Ribeiro Costa Rigo; TORRES, Thiago. Questões práticas sobre o estelionato após as Leis 13.964/2019 e 14.155/2021. *In:* **Consultor Jurídico** (ConJur), São Paulo, 28 set. 2021. Disponível em: https://www.conjur.com.br/2021-set-28/academia-policia-questoes-praticas-estelionato-leis-139642019-141552021. Acesso em: 1 out. 2025.

EZE, Thomas Chukwuma; OKONKWO, Patrick; AMADI, Chinedu. ***Cybercrime Modus Operandi**: Computer Misuses. In: American Journal of Research in Computer Science*, v. 7, n. 1, 2025. Disponível em: https://sdiopr.s3.ap-south-1.amazonaws.com/2025/JANUARY/14_Jan_2025/2024_AJRCOS_128138/Rev_AJRCOS_128138_Eze_A.pdf?utm. Acesso em: 01 out. 2025.

GEKOSKI, Anna; ADLER, Joanna R.; McSWEENEY, Tim. *Profiling the Fraudster: Findings from a Rapid Evidence Assessment. In:* ***Policing and Society***, v. 33, n. 6, p. 739-757, 2022. Disponível em: https://www.tandfonline.com/doi/full/10.1080/17440572.2022.2137670?utm. Acesso em: 2 out. 2025.

HAVERS, Benjamin; TRIPATHI, Kartikeya; BURTON, Alexandra; McMANUS, Sally; COOPER, Claudia. *Cybercrime victimisation among older adults: A probability sample survey in England and Wales. In:* ***International Journal of Law and Psychiatry**, 2023*. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC11654966/?utm. Acesso em: 01 out. 2025.

MISRA, Gaurav; JUNGER, Marianne; MONTOYA, Lorena. *A Cross-National Study on Cybercrime: Incident, Suspect and Victim Characteristics for Digital and Traditional Fraud in the Netherlands and Kolkata, India. In:* ***Journal of Forensic Sciences & Criminal Investigation***, v. 10, n. 5, 2018. Disponível em: https://juniperpublishers.com/jfsci/JFSCI.MS.ID.555634.php?utm. Acesso em: 01 out. 2025.

MONSTERSGAME. *"Which countries are most affected by online fraud? Study reveals." In:* ***Monstersgame***, 27 mar. 2025. Disponível em: https://www.monstersgame.co.uk/technology/which-countries-are-most-affected-by-online-fraud-study-reveals/. Acesso em: 29 set. 2025.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Manual de direito penal**: parte especial arts. 121 a 234-B do CP. 37. ed. Indaiatuba: Editora Foco, 2024.

NATIONAL AUDIT OFFICE (Reino Unido). ***Using data analytics to tackle fraud and error***. Londres, 2025. Disponível em: https://www.nao.org.uk/wp-content/uploads/2025/07/using-data-analytics-to-tackle-fraud-and-error.pdf?utm_. Acesso em: 1 out. 2025.

SERASA EXPERIAN. Brasil tem recorde nas tentativas de fraude registradas em janeiro, aponta Serasa Experian. *In:* **Serasa Experian**, 17 abr. 2025. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/indicadores/brasil-tem-recorde-

nas-tentativas-de-fraude-registradas-em-janeiro-aponta-serasa-experian/. Acesso em: 29 set. 2025.

SHANG, Yuxi; WU, Zhongxian; DU, Xiaoyu; JIANG, Yanbin; MA, Beibei; CHI, Meihong. *The psychology of the internet fraud victimization of older adults: A systematic review. In:* ***Frontiers in Psychology***, 5 set. 2022. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC9484557/?utm. Acesso em: 01 out. 2025.

SINDICATO DOS EMPREGADOS EM ESTABELECIMENTOS BANCÁRIOS – TUBARÃO. **Fraudes em canais eletrônicos crescem 17% e golpes via Pix aumentam 43% em um ano**. 11 mar. 2025. Disponível em: https://www.bancariostb.com.br/noticia/fraudes-em-canais-eletronicos-crescem-17-e-golpes-via-pix-aumentam-43-em-um-ano/. Acesso em: 29 set. 2025.

THE GUARDIAN. *Remote purchase' fraud in UK surges as customers tricked into disclosing passcodes. In:* ***The Guardian***, 28 mai. 2025. Disponível em: https://www.theguardian.com/money/2025/may/28/remote-purchase-fraud-uk-surges-customers-tricked-passcodes. Acesso em: 29 set. 2025.

TIMES OF INDIA. *India's cyber fraud epidemic: Rs 22,845 crore lost in 2024; 206% jump from previous year, says government. In:* ***Times of India***, 22 jul. 2025. Disponível em: https://timesofindia.indiatimes.com/business/cybersecurity/indias-cyber-fraud-epidemic-rs-22845-crore-lost-in-just-a-year-206-jump-from-previous-year-says-government/articleshow/122840099.cms. Acesso em: 29 set. 2025.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. **Acórdão nº 19.016.309**. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=19016309&cdForo=0. Acesso em: 01 out. 2025.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. **Acórdão nº 19.421.308**. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=19421308&cdForo=0. Acesso em: 1 out. 2025.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. **Acórdão nº 19.639.856**. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=19639856&cdForo=0. Acesso em: 01 out. 2025.

UNITED STATES. Federal Bureau of Investigation. ***Internet Crime Complaint Center*** *(IC3) – About*. Disponível em: https://www.ic3.gov/Home/About?utm&utm. Acesso em: 1 out. 2025.

UNITED STATES. Federal Bureau of Investigation. ***Internet Crime Report 2020***. Washington, D.C.: FBI, 2021. Disponível em: https://www.ic3.gov/AnnualReport/Reports/2020_ic3report.pdf?utm. Acesso em: 1 out. 2025.

UNITED STATES. Federal Bureau of Investigation. ***Internet Crime Report 2023***. [S.l.]: FBI, 2023. Disponível em: https://pt.scribd.com/document/835838296/FBI-Internet-Crime-Report-2023-1710798294-1?utm. Acesso em: 1 out. 2025.

ZHANG, Chuo Jun; GILL, Asif Q.; LIU, Bo; ANWAR, Memoona J. ***AI-based identity fraud detection****: a systematic review*. 2025. Disponível em: https://arxiv.org/abs/2501.09239?utm. Acesso em: 1 out. 2025.