XIII SEMPAD
Seminário de Pesquisa em Administração UNIFACS

FRAUDE DIGITAL E TRANSFORMAÇÕES ECONÔMICAS: UM BREVE ENTRELACE ENTRE CULTURA, TECNOLOGIA E GOVERNANÇA

Debora Coutinho Silva[1]
Alberto da Silva Dultra Junior[2]
Hélder Uzêda Castro[3]

RESUMO
O presente artigo tem por objetivo fomentar o debate acadêmico e prático acerca da cultura da fraude no ambiente digital, analisando as novas modalidades de crimes surgidas com o avanço das tecnologias da informação e comunicação, bem como a forma como os marcos normativos brasileiros vêm sendo atualizados para enfrentar essas transformações. Com o aumento exponencial do comércio eletrônico, dos serviços digitais e da circulação massiva de dados, observa-se a intensificação de práticas fraudulentas como golpes financeiros, falsificação de identidades digitais e estelionatos eletrônicos. A pesquisa adota uma abordagem qualitativa e exploratória, sustentada por revisão bibliográfica e análise documental de dados secundários provenientes de fontes jurídicas, técnicas e estatísticas nacionais e internacionais. Utiliza-se, ainda, a análise de conteúdo orientada por Bardin (2016), visando identificar padrões e estratégias recorrentes no cenário brasileiro. Os resultados indicam que, embora haja avanços legislativos, a exemplo da Lei nº 14.155/2021 e a vigência da Lei Geral de Proteção de dados LGPD, a resposta normativa ainda é insuficiente diante da sofisticação tecnológica dos crimes digitais. Conclui-se que o enfrentamento eficaz da cultura da fraude requer ações integradas, que articulem repressão penal, investimento em tecnologia, educação digital e mudança cultural. O artigo propõe a superação de uma visão meramente punitiva, com o fortalecimento da governança digital e o engajamento de múltiplos atores sociais para construção de uma cultura de integridade.

Palavras-chave: Fraude digital; Governança digital; Cultura; Cibersegurança; Direito digital.

ABSTRACT
This article aims to foster the academic and practical debate about the culture of fraud in the digital environment, analyzing the new forms of crimes that have emerged with the advancement of information and communication technologies, as well as the way in which Brazilian normative frameworks have been updated to face these transformations. With the exponential increase in e-commerce, digital services and massive circulation of data, there is

[1] Acadêmica no Curso de Direito da Universidade São Judas Tadeu (USJT, Brasil). Estudante de Iniciação Científica pelo Instituto Ânima de Educação – ProCiência 2025. E-mail:deboracoutinho2002@gmail.com
[2] Mestrando em Direito, Governança e Políticas Públicas pela Universidade Salvador (UNIFACS, Brasil). Mentor de Iniciação Científica pelo Instituto Ânima de Educação – ProCiência 2025. E-mail: asdultra@gmail.com
[3] Orientador do trabalho. Pesquisador e Professor Titular nos Programas de Pós-graduação em Administração (PPGA) e em Direito, Governança e Políticas Públicas (PPGDGPP) da Universidade Salvador (UNIFACS, Brasil). E-mail: helderuzeda@gmail.com

an intensification of fraudulent practices such as financial scams, falsification of digital identities and electronic scam. The research adopts a qualitative and exploratory approach, supported by literature review and documentary analysis of secondary data from national and international legal, technical and statistical sources. It is also used the content analysis guided by Bardin (2016), in order to identify recurring patterns and strategies in the Brazilian scenario. The results indicate that, although there are legislative advances, such as Law no 14.155/2021 and the validity of the LGPD General Data Protection Law, the normative response is still insufficient in view of the technological sophistication of digital crimes. It is concluded that the effective fight against the culture of fraud requires integrated actions, which articulate criminal repression, investment in technology, digital education and cultural change. The article proposes to overcome a merely punitive vision, with the strengthening of digital governance and the engagement of multiple social actors to build a culture of integrity.

Keywords: Digital fraud; Digital governance; Culture; Cybersecurity; Digital law.

1. INTRODUÇÃO

A intensificação da digitalização econômica tem promovido transformações estruturais profundas nos modelos de interação entre indivíduos, organizações e governos, instaurando novas dinâmicas de mercado e redesenhando a arquitetura das transações comerciais. A incorporação acelerada de tecnologias digitais, tais como plataformas online, sistemas automatizados e soluções baseadas em inteligência artificial, amplia de modo exponencial as oportunidades de negócios e a integração entre mercados. Contudo, esse mesmo ambiente, caracterizado pela inovação permanente, mostra-se igualmente propenso à disseminação de práticas fraudulentas, crimes cibernéticos e condutas oportunistas que tensionam a capacidade institucional de regulação, fiscalização e resposta tempestiva.

No contexto brasileiro, os indicadores revelam a magnitude do problema. Segundo levantamento da Visa (2023), o país ocupa o segundo lugar no ranking global de fraudes, com índice de risco de 14,24% em um universo de mais de 2,7 bilhões de transações processadas, totalizando US$ 381 bilhões, situando-se logo atrás da China (14,93%). Tal cenário reflete não apenas a elevada exposição do sistema digital brasileiro a condutas ilícitas, mas também a emergência de uma verdadeira “cultura da fraude”, sustentada por brechas tecnológicas, baixa maturidade em governança digital e lacunas institucionais na gestão de riscos cibernéticos.

O comércio eletrônico, em particular, constitui terreno fértil para a evolução de esquemas fraudulentos cada vez mais sofisticados. De acordo com o Relatório do Laboratório de Inteligência e Ameaças da FortiGuard Labs (2022), o Brasil registrou 31,5 bilhões de tentativas de ataques cibernéticos, um incremento de 94% em relação ao ano anterior. Entre as

práticas mais recorrentes destacam-se *chargebacks*[4] fraudulentos, técnicas de *phishing*[5], "fraudes amigáveis" (perpetradas por pessoas do convívio da vítima) e "auto-fraudes" (realizadas pelos próprios titulares dos dados de forma deliberada).

Esses fenômenos se expandem em ritmo equiparável ao da própria evolução tecnológica, impondo desafios concretos aos mecanismos de regulação e controle institucional. O ciclo de inovação digital, contínuo e acelerado, dificulta a atualização tempestiva de normas, mecanismos de *compliance* e barreiras técnicas de segurança. Nesse contexto, torna-se imperativa a realização de investigações acadêmicas que examinem criticamente, de forma interdisciplinar e prospectiva, os contornos dessa problemática.

É nesse cenário que se insere o presente estudo, desenvolvido no âmbito do Projeto de Iniciação Científica "Governança, Controladoria e Inovação: um estudo sobre fraudes corporativas", fomentado pelo Instituto Ânima, por meio do Programa ProCiência. O objetivo deste texto é compreender a constituição e os impactos da "cultura da fraude" na economia digital brasileira, articulando dimensões comportamentais, institucionais e tecnológicas que concorrem para sua reprodução.

O percurso metodológico adotado fundamenta-se em uma abordagem qualitativa, de caráter exploratório e descritivo, orientada pela busca de compreensão aprofundada do fenômeno estudado. Para tanto, articula-se uma revisão sistemática da literatura com uma análise documental criteriosa, de modo a integrar diferentes perspectivas teóricas e evidências empíricas. Essa estratégia visa não apenas mapear e sintetizar o estado da arte sobre fraudes digitais e governança corporativa, mas também identificar padrões, lacunas e tendências emergentes que possam subsidiar interpretações críticas e formulações teóricas mais robustas. O levantamento teórico será realizado com base em estudos nacionais e internacionais sobre fraudes digitais, governança corporativa, proteção de dados e direito digital, utilizando bases como Scielo, Google Scholar, SSRN e Web of Science.

A análise documental abrangerá relatórios estatísticos e técnicos produzidos por instituições como o CERT.br, a Federação Brasileira de Bancos (Febraban), a Visa e empresas

[4] Processo em que um cliente contesta uma compra feita com cartão de crédito ou débito junto à operadora, solicitando o estorno do valor.
[5] Espécie de ataque cibernético que usa e-mails, mensagens de texto, telefonemas ou sites fraudulentos para enganar as pessoas a compartilhar dados confidenciais, baixar malware ou se expor a crimes cibernéticos de outras formas.

de cibersegurança como Fortinet[6] e Kaspersky[7]. O tratamento dos dados seguirá a técnica de categorização temática proposta por Bardin (2016), visando identificar padrões recorrentes de conduta e estratégias fraudulentas utilizadas no ambiente digital brasileiro.

Espera-se, ao final, que este trabalho contribua para o avanço do debate teórico e empírico acerca dos riscos cibernéticos no contexto da economia digital, fornecendo subsídios para a formulação de ações preventivas e mecanismos de contenção mais eficazes. Almeja-se, igualmente, fomentar uma reflexão interdisciplinar acerca dos limites da inovação tecnológica diante da fragilidade dos controles institucionais, problematizando os rumos da segurança digital em sociedades cada vez mais conectadas.

2. FRAUDE DIGITAL: CONCEITO JURÍDICO, ELEMENTOS E DESAFIOS REGULATÓRIOS

2.1 Conceito Jurídico Clássico de Fraude

No âmbito do Direito, a fraude é tradicionalmente compreendida como uma conduta dolosa caracterizada pela má-fé do agente, que, mediante engano ou ardil, busca obter vantagem indevida em prejuízo de terceiros. Bitencourt (2020) define a fraude como um ato enganoso voltado ao benefício próprio, capaz de gerar danos a indivíduos ou empresas. Nessa mesma linha, Venosa (2011, p. 213) conceitua a fraude como o uso de meios escusos para contornar normas legais ou cláusulas contratuais, mesmo que ainda não plenamente constituídas. Complementarmente, Silva (2016, p. 645) enfatiza a imprescindibilidade da intenção danosa e a exterioridade em relação à relação jurídica diretamente envolvida.

De acordo com Monteiro de Barros (2009, p. 245), a caracterização da fraude exige a presença de um terceiro efetivamente lesado pelo ato fraudulento, sendo essencial que a conduta não se restrinja a mera violação contratual entre as partes. O sistema de justiça brasileiro, portanto, identifica como elementos centrais da fraude a astúcia, a má-fé e a intenção deliberada de induzir alguém ao erro com o propósito de obter vantagem ilícita.

[6] Fundada há mais de 20 anos em Sunnyvale, Califórnia, a Fortinet atua na área da segurança cibernética e na convergência de rede e segurança.
[7] Empresa de Pesquisa e Análise Global, formada por um grupo de especialistas em cibersegurança, especializados em ataques APT, espionagem cibernética e tendências globais de cibercrime.

2.2 Inovação Tecnológica e Novas Modalidades de Fraude

Com a transformação digital da economia, a fraude passou a assumir contornos mais sofisticados, alavancada pelas possibilidades tecnológicas contemporâneas. O ambiente digital, marcado pela interconectividade, pelo anonimato relativo e pela velocidade das transações, ampliou o espectro de atuação dos agentes fraudulentos. Nesse novo contexto, proliferam técnicas como *phishing*, falsificação de identidades digitais, engenharia social e exploração de falhas em sistemas informatizados, que desafiam os mecanismos tradicionais de prevenção e repressão.

Além disso, o dolo nas fraudes digitais manifesta-se não apenas pela intenção de obter lucro ilícito, mas também pelo domínio técnico sobre sistemas de informação e pelo conhecimento sobre suas vulnerabilidades. Os meios digitais permitem o disfarce da autoria, a internacionalização dos ataques e o emprego de automações, tornando o combate a essas condutas mais complexo e desafiador.

2.3 Avanços Normativos no Ordenamento Jurídico Brasileiro

Diante da proliferação das fraudes digitais, o ordenamento jurídico brasileiro buscou se adaptar, ainda que de forma gradual, aos novos desafios. Um marco importante foi a promulgação da Lei nº 14.155/2021, que alterou dispositivos do Código Penal e do Código de Processo Penal para incluir a criminalização de condutas fraudulentas praticadas por meios eletrônicos. A principal inovação foi a inclusão do § 2º-A ao artigo 171 do Código Penal, que agrava a pena de crimes como estelionato, furto e invasão de dispositivos informáticos quando praticados por meio digital ou pela internet.

Essa legislação permitiu tipificar com maior precisão crimes cometidos em ambientes digitais, abrangendo fraudes bancárias eletrônicas, golpes via redes sociais, clonagem de aplicativos e outras formas contemporâneas de estelionato digital. Contudo, mesmo com esse avanço, persistem lacunas normativas em relação a práticas emergentes, como fraudes em plataformas de *streaming*, aplicativos de mensagens instantâneas e ambientes descentralizados.

2.4 Desafios Regulatórios e Necessidade de Abordagens Interdisciplinares

Embora o arcabouço legal tenha evoluído, ainda há significativa dificuldade em acompanhar a velocidade com que as tecnologias e os métodos de fraude se transformam. Muitos atos fraudulentos permanecem à margem da tipificação penal convencional, gerando insegurança jurídica e entraves à responsabilização eficaz dos infratores. Isso evidencia a

urgência de uma doutrina mais especializada e moderna, capaz de oferecer fundamentos teóricos e normativos adaptáveis à complexidade digital.

Adicionalmente, é preciso reconhecer que o enfrentamento da fraude digital ultrapassa o campo estritamente jurídico. Exige-se uma abordagem interdisciplinar, integrando áreas como ciência da computação, governança de dados, segurança da informação e educação digital. A prevenção eficaz dependerá não apenas de dispositivos legais punitivos, mas também da implementação de sistemas tecnológicos preventivos, da capacitação institucional e da promoção de uma cultura de integridade digital.

3. TECNOLOGIAS DE PREVENÇÃO À FRAUDE DIGITAL: MECANISMOS, DESAFIOS E EDUCAÇÃO DO USUÁRIO

3.1 Chargebacks e Estratégias de Mitigação

Os *chargebacks* constituem um dos principais desafios enfrentados por empresas no comércio digital. Embora representem instrumentos legítimos de proteção ao consumidor, quando utilizados de forma indevida ou fraudulenta convertem-se em fonte expressiva de prejuízos financeiros e instabilidade contratual.

Para mitigar esse problema, destaca-se o monitoramento em tempo real das transações financeiras. Sistemas baseados em aprendizado de máquina (*machine learning*) analisam o comportamento do usuário a partir de dados históricos, construindo perfis comportamentais que permitem identificar desvios anômalos. Segundo Schneier (2012), tais sistemas detectam padrões fora do comportamento habitual do cliente, possibilitando ações corretivas imediatas antes da efetivação da fraude.

A autenticação multifatorial (MFA) também se consolidou como medida eficaz para a redução de transações não autorizadas. Por meio do envio de códigos temporários via SMS, e-mail ou aplicativos autenticadores, estabelece-se uma segunda camada de verificação da identidade do usuário. Embora a MFA não elimine integralmente os *chargebacks* decorrentes de fraudes amigáveis, reduz de modo significativo os riscos associados a acessos indevidos (Krebs, 2024).

Adicionalmente, a verificação biométrica e documental, aliada a sistemas de criptografia ponta a ponta, acrescenta camadas complementares de segurança. Esses recursos diminuem o risco de interceptação de dados e fortalecem a rastreabilidade das transações financeiras.

3.2 Prevenção ao *Phishing*: Tecnologias e Educação

O *phishing* constitui uma das modalidades mais recorrentes de fraude digital, caracterizando-se como técnica de engenharia social que visa à obtenção indevida de dados sensíveis por meio da manipulação psicológica dos usuários. A prevenção eficaz desse tipo de ameaça requer uma combinação de soluções tecnológicas e estratégias educativas contínuas. Entre as medidas técnicas mais utilizadas destacam-se:

- sistemas de filtragem de e-mails, capazes de identificar e bloquear mensagens maliciosas com base em palavras-chave, links suspeitos e remetentes desconhecidos;
- verificação de reputação de sites, por meio de listas negras e ferramentas de inspeção de segurança digital;
- uso obrigatório de HTTPS e certificados digitais válidos, conferindo maior confiabilidade às plataformas transacionais;
- MFA como barreira adicional, mesmo quando as credenciais do usuário são comprometidas;
- softwares antivírus e antiphishing, com detecção proativa de ameaças; e
- sistemas de resposta a incidentes, que permitem a contenção imediata de ataques e a comunicação ágil com usuários afetados (Symantec, 2024).

Contudo, a literatura especializada evidencia que a tecnologia, isoladamente, é insuficiente. Mitnick (2003) e Schneier (2004) ressaltam que a educação do usuário constitui elemento central da prevenção, uma vez que as fraudes de *phishing* exploram lapsos de atenção e desconhecimento sobre ameaças digitais. Treinamentos regulares, simulações de ataques e campanhas de conscientização figuram, nesse sentido, como estratégias altamente recomendadas (ENISA, 2023).

3.3 Barreiras Econômicas e Desigualdade Tecnológica

Apesar da existência de soluções tecnológicas robustas, seu custo de implementação ainda representa um entrave para pequenos e médios negócios. Tais empresas, mais vulneráveis a perdas, frequentemente não dispõem de infraestrutura técnica ou financeira para adotar sistemas avançados de prevenção, o que acentua a desigualdade digital e mantém parcela significativa do comércio eletrônico em situação de risco permanente.

Esse contexto reforça a urgência do fortalecimento de políticas públicas voltadas à segurança digital, com ênfase em:

- linhas de crédito específicas para investimentos em proteção de dados e cibersegurança;
- programas de capacitação técnica direcionados a empreendedores; e
- apoio ao desenvolvimento de soluções escaláveis e acessíveis a microempresas.

3.4 A Dinâmica do Ciclo Fraude - Contramedida

Um dos aspectos mais desafiadores no enfrentamento da fraude digital é a velocidade com que os fraudadores adaptam suas estratégias diante de novas tecnologias. A dinâmica entre inovação criminosa e resposta institucional configura um ciclo contínuo de ação e reação, no qual a eficácia de uma tecnologia tende a ser temporária.

Isaca (2022) e ENISA (2023) destacam que a verdadeira robustez da prevenção reside na capacidade de detecção preditiva de riscos aliada à gestão integrada de incidentes. Por isso, as empresas devem ir além da simples aquisição de softwares, incorporando uma cultura organizacional orientada à segurança da informação, com governança, protocolos de resposta e investimento constante em inovação.

4. CULTURA DA FRAUDE NO BRASIL VS ENFRENTAMENTO LEGISLATIVO

O antropólogo norte-americano Melville Herskovits (1963) conceitua a cultura como a parcela do ambiente moldada pelo ser humano, resultante dos padrões comuns que cada grupo social desenvolve para assegurar sua sobrevivência. Esses padrões manifestam-se em estruturas de parentesco, formas de associação e sistemas de significação que dão sentido à vida coletiva. Para o autor, cada grupo social apresenta características originais que possibilitam as diferenciações culturais entre comunidades distintas.

Na mesma linha, Edward B. Tylor (1871) define cultura ou civilização, em seu sentido etnográfico mais amplo, como esse todo complexo que inclui conhecimentos, crenças, arte, moral, leis, costumes e quaisquer outras capacidades e hábitos adquiridos pelo homem enquanto membro da sociedade. Tal concepção permite compreender a cultura nas interações entre indivíduos, bem como seu uso como instrumento de diferenciação e, potencialmente, de discriminação social, econômica e política.

A cultura da fraude não é fenômeno recente. Nesse sentido, (Faoro, 2001, p.127):

> Os estadistas do Segundo Reinado - a herança coube à República - pretendiam matar a fraude, a violência e a corrupção eleitorais mediantes novas leis e novos sistemas. As tentativas se alinham: a lei dos círculos de 1855, a circunscrição de três deputados em 1860, a lei dos terços de 1875 e a eleição direta de 1881(Lei Saraiva). Cada uma das reformas provocava uma onda de euforia, logo desmentida pelas práticas viciosas, que sobrenadavam à lei.

A fraude no Brasil, em suas múltiplas expressões, revela um fenômeno social de raízes profundas. Presente tanto nos altos escalões do poder quanto nas práticas cotidianas do cidadão comum, esse padrão de comportamento, frequentemente denominado “cultura da fraude”, manifesta-se como um elemento historicamente tolerado ou relativizado. Tal cultura desafia não apenas os mecanismos formais de controle e punição, mas também os valores que sustentam a convivência social e o pacto civilizatório democrático.

Para Souza (2017), a desigualdade estrutural e a concentração de poder econômico e político constituem os verdadeiros propulsores das micro e macrofraudes existentes no país. A corrupção, segundo o autor, não se reduz a um problema moral ou individual, mas expressa as desigualdades sociopolíticas e socioculturais, que extrapolam as dimensões estritamente econômicas. O patrimonialismo, nessa perspectiva, traduz-se na “vibração” do frêmito fraudulento e na naturalização de uma “mentalidade rentista” intrinsecamente corrompida em sua essência.

Nesse sentido, a cultura da fraude não configura um traço isolado, mas um fator estruturante das relações sociais e econômicas. Sua presença é identificável em múltiplas práticas, como os recorrentes casos de sonegação fiscal, a apresentação de atestados médicos falsos e o favorecimento indevido em licitações públicas. Esse cenário tem exigido, e continua a exigir, revisões normativas que enfrentem as novas modalidades de fraude, especialmente aquelas que se sofisticam com os avanços tecnológicos. Exemplo disso é a Lei nº 14.155/2021, que alterou o Código Penal e agravou as penas para estelionatos cometidos por meios digitais.

As mudanças legislativas, embora importantes, configuram respostas parciais à proliferação de fraudes eletrônicas, a exemplo do *phishing*, golpes em redes sociais, clonagem de aplicativos de mensagens e uso indevido de dados pessoais para transações financeiras. Leis como a Lei Carolina Dieckmann (Lei nº 12.737/2012), ao tipificar a invasão de dispositivos informáticos, e o Marco Civil da Internet (Lei nº 12.965/2014), ao estabelecer princípios como proteção à privacidade, responsabilidade civil e neutralidade da rede, são marcos relevantes na regulação do ambiente digital. Ainda assim, apenas legislar é insuficiente para enfrentar um problema de natureza cultural.

O combate eficaz à fraude requer não apenas o fortalecimento institucional, mas também uma mudança de mentalidade coletiva. A promoção de uma educação cidadã e digital emerge como instrumento fundamental para conscientizar a população acerca dos danos sociais provocados pela fraude, prevenindo, reconhecendo e desestimulando condutas ilícitas. É

igualmente necessário compreender que a "cultura da fraude" não é um fenômeno periférico, mas uma prática profundamente arraigada no cotidiano brasileiro, desde infrações sofisticadas até pequenos desvios, muitas vezes normalizados sob o rótulo do "jeitinho brasileiro". Essa banalização da transgressão fragiliza os esforços de controle legal e reforça a sensação de impunidade.

Além das alterações legislativas, impõe-se o aprimoramento de mecanismos institucionais de fiscalização mais eficazes e autônomos, incluindo auditorias automatizadas, canais de denúncia protegidos (*whistleblowing*) e maior atuação das autoridades reguladoras. A efetividade das normas depende, em larga medida, da sua aplicação rigorosa, imparcial e transparente.

Por fim, a ampliação da participação da sociedade civil no combate à fraude é indispensável. Iniciativas de monitoramento cidadão, campanhas educativas e o fortalecimento de uma cultura de integridade e conformidade devem ser incentivados, pois a luta contra a fraude não se limita aos tribunais: ela se materializa nas escolhas cotidianas e nas práticas sociais que valorizam a honestidade.

5. GOVERNANÇA DIGITAL E RESPONSABILIDADE COMPARTILHADA

A crescente complexidade e descentralização do ecossistema digital impõem a necessidade de um novo modelo de governança no qual o enfrentamento à fraude deixe de ser responsabilidade exclusiva do Estado, tornando-se um compromisso compartilhado entre governo, setor privado, sociedade civil e usuários da tecnologia.

Nesse contexto, a governança digital – compreendida como o conjunto de políticas, mecanismos de controle, tecnologias e estruturas institucionais voltadas à integridade e à segurança da informação nas interações digitais – desponta como elemento essencial no combate às fraudes. Mais do que um aparato técnico, ela configura um espaço normativo e ético capaz de articular diferentes atores e interesses em prol de um ambiente confiável. Esse movimento envolve a consolidação de boas práticas de *compliance* digital, sistemas de gestão de riscos cibernéticos e políticas internas corporativas que orientem o uso ético da tecnologia. As empresas que operam no ambiente digital devem assumir protagonismo na busca por integridade sistêmica, investindo em protocolos robustos de detecção e resposta a fraudes.

Outro aspecto crucial é o papel das plataformas tecnológicas na prevenção e detecção de ilícitos. Redes sociais, instituições financeiras e marketplaces online funcionam como

"*gatekeepers*"[8] do ambiente digital, devendo responder não apenas pela reparação de danos aos usuários, mas também pela adoção de medidas preventivas. Isso inclui a criação de políticas de uso transparentes, mecanismos eficazes de denúncia e exclusão de perfis falsos, auditoria de algoritmos, proteção dos dados dos consumidores e disponibilização de informações claras sobre práticas de segurança. A ausência dessas medidas perpetua a vulnerabilidade sistêmica e reforça a cultura da impunidade.

A construção de uma governança digital robusta pressupõe também a consolidação institucional de órgãos reguladores e fiscalizadores, como Banco Central, Ministério Público e Polícia Federal. Integrar e modernizar essas instituições, com aporte de recursos tecnológicos, pode resultar em sistemas de monitoramento mais ágeis, responsivos e preditivos. Ademais, parcerias público-privadas voltadas ao desenvolvimento de soluções tecnológicas, como rastreabilidade de transações, certificação de identidade digital e criptografia avançada, ampliam a eficiência do combate à fraude e fomentam um ambiente de confiança propício à inovação e ao desenvolvimento sustentável da economia digital.

Nesta altura, é indispensável o fortalecimento da cidadania digital. Capacitar a população para compreender seus direitos, deveres e riscos no ambiente virtual deve ser premissa de políticas públicas e programas corporativos. A governança digital, para ser efetiva, deve combinar transparência, interoperabilidade e *accountability* nos sistemas públicos e privados, podendo materializar-se em iniciativas como observatórios nacionais e regionais de fraudes digitais, abertura de dados sobre crimes cibernéticos e auditoria de algoritmos de decisão automatizada.

CONSIDERAÇÕES FINAIS

A análise realizada evidencia que a fraude no Brasil não é um fenômeno episódico ou restrito ao comportamento individual, mas uma realidade complexa e multifacetada, enraizada na história social e institucional do país. Embora a legislação e a jurisprudência – como decisões do Superior Tribunal de Justiça (HC 285.587/SP, 2016) – façam uso recorrente do termo "fraude", sua definição técnica permanece fluida e, em muitos casos, indeterminada.

[8] Um gatekeeper pode ser entendido como o "guardião da informação", ou seja, aquele que controla o fluxo de mensagens, dados ou conteúdos em um determinado contexto. O termo é usado, sobretudo, para designar pessoas, instituições ou mecanismos que selecionam, filtram e direcionam o que será transmitido ou acessado por um público.

Essa imprecisão dificulta a uniformização de entendimentos e a formulação de políticas públicas eficazes.

Os achados de Venosa (2011) e Monteiro de Barros (2009) reforçam que a fraude não se limita ao engano, mas implica a intenção de causar prejuízo a terceiros. Tal compreensão, embora consolidada na doutrina, enfrenta desafios práticos diante da generalidade do conceito em sede judicial. Ao mesmo tempo, a literatura aponta que a corrupção e a fraude resultam menos de desvios morais isolados e mais de estruturas patrimonialistas e desiguais que moldam as práticas sociais (Souza, 2017).

Esse diagnóstico reforça a necessidade de um enfrentamento sistêmico: fortalecer leis anticorrupção, ampliar mecanismos independentes de auditoria e canais protegidos de denúncia (*whistleblowing*), promover transparência em todos os níveis e investir na formação ética e digital da sociedade. Tecnologias de prevenção, como autenticação multifatorial, tokenização e criptografia avançada (Schneier, 2012; Krebs, 2023), devem ser combinadas a estratégias educativas, pois, como salientam Mitnick (2003) e Schneier (2004), a consciência do usuário é determinante na mitigação de riscos como phishing, chargebacks e fraudes em redes sociais.

Entretanto, a efetividade dessas medidas não é apenas tecnológica. Treinamentos contínuos, definição de políticas claras de devolução e suporte proativo ao consumidor (Serasa, 2025) são fatores preponderantes para reduzir estornos e litígios. Ao mesmo tempo, a criação de observatórios e bases de dados nacionais sobre fraude digital pode alimentar pesquisas empíricas e fortalecer a tomada de decisão baseada em evidências.

Em termos de contribuição, este estudo ilumina a interdependência entre tecnologia, governança e cultura social no enfrentamento da fraude, oferecendo um panorama integrado que pode subsidiar gestores públicos, empresas e legisladores.

Para estudos posteriores, recomenda-se investigar casos aplicados, por exemplo: experiências de bancos digitais, *marketplaces* e órgãos reguladores que já adotaram sistemas de monitoramento em tempo real, ou políticas de educação digital para consumidores; de modo a identificar práticas exitosas, barreiras e lições aprendidas. Pesquisas comparativas entre diferentes setores econômicos e países também podem oferecer insights valiosos para políticas públicas e estratégias corporativas.

Consolidar uma cultura de integridade e corresponsabilidade demanda mais do que reformas pontuais: exige uma transformação profunda na relação entre Estado, mercado e sociedade civil. Somente com engajamento conjunto e abordagem interdisciplinar,

combinando tecnologia, educação e governança democrática, será possível transformar o combate à fraude em um verdadeiro pilar de reconstrução ética, cidadã e institucional no Brasil.

REFERÊNCIAS

BARDIN, Laurence. **Análise de conteúdo.** São Paulo: Edições 70, 2016.

BALTAZAR Júnior, José Paulo. **Crimes Federais.** Porto Alegre: Livraria do Advogado Editora, 2011.

BARBOSA, Daniel Cunha. Conscientização em cibersegurança: aprenda a criar uma campanha eficaz. **We Live Security,** 26 fev. 2021. Disponível em: <https://www.welivesecurity.com/br/2021/02/26/conscientizacao-em-ciberseguranca-aprenda-a-criar-uma-campanha-eficaz/>. Acesso em: 10 set. 2024.

BITENCOURT, Cezar Roberto. **Direito Penal: Parte Especial.** 22. ed. São Paulo: Saraiva, 2020.

ISACA. **Cybersecurity Culture: A How-to Guide. Schaumburg: Information Systems Audit and Control Association,** 2022. Disponível em: https:<//www.isaca.org/resources>. Acesso em: 2 jul. 2025.

EUROPEAN UNION AGENCY FOR CYBERSECURITY – ENISA. **ENISA Threat Landscape.** 2023. Disponível em: < https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023> Acesso em: 1 out. 2024.

FAORO, Raymundo. **Machado de Assis: a pirâmide e o trapézio.** 4.ª ed. rev. São Paulo: Globo, 2001.

FORTIGUARD LABS. **Relatório de ameaças cibernéticas 2022: tentativas de ataques e tipos de fraudes.** 2022. Disponível em: https:<//www.fortinet.com/resources/fortiguard-labs/cybersecurity-threat-report-2022>. Acesso em: 1 out. 2024.

HERSKOVITS, Melville J. **Antropologia Cultural.** São Paulo: Mestre Jou, 1963.

OLIVEIRA, Andressa Jarletti Gonçalves de. **A proteção dos consumidores contra fraudes bancárias e digitais.** CONJUR, 2023. Disponível em: https:<//www.conjur.com.br/2023/05/17/protecao-consumidores-fraudes-bancarias-digital>. Acesso em: 1 set. 2024.

KREBS, Brian. Ransomware Attacks: How to Protect Yourself. **KREBS ON SECURITY**, 2023. Disponível em: https:< https://krebsonsecurity.com/2023/06/why-malware-crypting-services-deserve-more-scrutiny/>. Acesso em: 28 set. 2024.

MITNICK, Kevin; SIMON, William L. **A arte de enganar:** como hackers invadem a mente das pessoas. São Paulo: Campus, 2003.

MONTEIRO, Washington de Barros. **Curso de Direito Civil 1**. 42. ed. São Paulo: Saraiva, 2009.

SCHNEIER, Bruce. **Secrets and Lies:** Digital Security in a Networked World. New York: Wiley, 2004.

SCHNEIER, Bruce. **Liars and Outliers: Enabling the Trust that Society Needs to Thrive.** New Jersey: Wiley, 2012.

SERASA EXPERIAN. **Maiores tendências em fraudes e crimes financeiros em 2025**. Disponível em:< https://www.serasaexperian.com.br/conteudos/as-5-maiores-tendencias-em-fraudes-e-crimes-financeiros-da-atualidade/>. Acesso em: 9 fev. 2025.

SILVA, De Plácido. **Vocabulário jurídico.** 32. ed. Rio de Janeiro: Forense, 2016.

SOUZA, Jessé. **A elite do atraso:** da escravidão à Lava Jato. São Paulo: Editora Leya, 2017.
SYMANTEC. Internet Security Threat Report 2024. Disponível em: <https://www.broadcom.com/company/newsroom/press-releases?filtr=2024>. Acesso em: 1 out. 2024.

TYLOR, Edward B**. Primitive culture:** Researches into the development of mythology, philosophy, religion, language, art, and custom. Vols. 1–2. London: John Murray, 1871.

VENOSA, Silvio de Salvo. **Direito civil:** parte geral. 11. ed. São Paulo: Atlas, 2011.

VISA. Para Visa, o Brasil tem o 2º maior índice de fraudes no mundo. **Valor Econômico**, 2024. Disponível em: https:<//www.valor.com.br/empresas/para-visa-o-brasil-tem-o-2-maior-indice-de-fraudes-no-mundo>. Acesso em: 1 jul. 2024.

VISA. Relatório de fraudes globais 2023: índices de risco e ranking de países. 2023. Disponível em: https:<//www.visa.com.br/relatorios/fraudes-global-2023>. Acesso em: 1 out. 2024.