

A IDENTIDADE QUE O ALGORITMO FABRICOU: FRAUDES BANCÁRIAS COM PESSOAS SINTÉTICAS E DEVER DE SEGURANÇA

THE IDENTITY THE ALGORITHM FABRICATED: BANKING FRAUD WITH SYNTHETIC PERSONS AND THE DUTY OF SECURITY

Luiza Mércia Freire Corrêa¹

RESUMO: A inteligência artificial generativa alterou o custo e a qualidade da falsificação de sinais de identidade: documentos, rostos, vozes e comportamentos podem ser produzidos com alta coerência, e ataques de injeção inserem mídia forjada diretamente no fluxo de verificação. Este artigo investiga em que medida a fabricação algorítmica de identidades altera o conteúdo do dever de segurança bancária na abertura, validação e autenticação de contas e operações, e quais critérios técnicos e probatórios permitem distinguir o defeito do serviço, imputável à instituição como fortuito interno, da fraude externa sem nexo causal com a infraestrutura bancária. A pesquisa é qualitativa, exploratória e jurídico-dogmática, e combina análise normativa do Código de Defesa do Consumidor, da Lei Geral de Proteção de Dados Pessoais e da regulação do Conselho Monetário Nacional e do Banco Central do Brasil, exame de precedentes do Superior Tribunal de Justiça, revisão narrativa interdisciplinar da literatura de segurança da informação e de estudos sobre identificação, e uso de padrões técnicos estrangeiros como referência persuasiva, com corte em 9 de setembro de 2026. Os resultados indicam que a fraude sintética desloca o defeito da falsidade documental para a arquitetura de confiança, que a responsabilidade permanece objetiva nos limites do fortuito interno sem ser automática, e que o ordenamento já contém os elementos de um dever proporcional, dinâmico, sistêmico e demonstrável de segurança identitária. Como contribuição, propõem-se a cadeia de confiança identitária, a Matriz LACRE e o Pacote Mínimo de Evidência de Autenticidade.

Palavras-chave: Identidade sintética. Responsabilidade bancária. Dever de segurança. Verificação de identidade. Prova digital.

¹Especialista em Direito Bancário e Mercado Financeiro pela PUC-Minas, mestranda em Direito pela UNESA-RJ.

ABSTRACT: Generative artificial intelligence has changed the cost and quality of forging identity signals: documents, faces, voices and behaviours can be produced with high coherence, and injection attacks insert forged media directly into the verification flow. This article examines to what extent the algorithmic fabrication of identities alters the content of the banking duty of security in the opening, validation and authentication of accounts and transactions, and which technical and evidentiary criteria distinguish a service defect, attributable to the institution as internal fortuity, from external fraud lacking a causal link with the banking infrastructure. The research is qualitative, exploratory and legal-dogmatic, combining normative analysis of the Consumer Defence Code, the General Personal Data Protection Law and the regulation issued by the National Monetary Council and the Central Bank of Brazil, an examination of precedents of the Superior Court of Justice, a narrative interdisciplinary review of the information security literature and of identification studies, and the use of foreign technical standards as persuasive reference, with research closed on 9 September 2026. Results indicate that synthetic fraud shifts the defect from documentary falsity to the architecture of trust, that liability remains strict within the limits of internal fortuity without being automatic, and that the legal order already contains the elements of a proportionate, dynamic, systemic and demonstrable duty of identity security. As its contribution, the article proposes the identity trust chain, the LACRE Matrix and the Minimum Authenticity Evidence Package.

Keywords: Synthetic identity. Bank liability. Duty of security. Identity verification. Digital evidence.

1 INTRODUÇÃO

2

Uma conta é aberta em plataforma digital com documento legível, rosto que supera a prova de vida, telefone ativo, endereço plausível e histórico de uso que se torna coerente ao longo de semanas. Nenhum elemento, isoladamente, desperta suspeita. Meses depois, a conta é utilizada para receber valores de um golpe, ou o crédito acumulado em nome dessa persona é sacado e nunca pago, ou o número de inscrição fiscal de uma pessoa real aparece vinculado a dívidas que ela jamais contraiu. A pergunta que o caso impõe ao direito bancário não é apenas se algum documento era falso. É saber por que a composição de sinais foi aceita como identidade válida e a quem cabe suportar as consequências dessa aceitação.

O problema ganhou densidade nova com a inteligência artificial generativa. A digitalização da abertura de contas deslocou para sistemas automatizados a confiança antes depositada em presença física, documentos materiais e interação humana, e a síntese generativa alterou o custo e a qualidade da falsificação. Documentos, faces, vozes e comportamentos podem ser produzidos ou manipulados com alta coerência, ao passo que ataques de injeção inserem mídia forjada diretamente entre o dispositivo de captura e o sistema que a analisa. O ponto jurídico não é a constatação, já consolidada, de que a tecnologia sofisticou a fraude. É

determinar quando esse risco integra o serviço bancário e qual evidência permite atribuir o defeito à instituição.

A delimitação adotada recusa duas simplificações. A primeira sustenta que a inteligência artificial amplia as fraudes e, por isso, amplia automaticamente a responsabilidade dos bancos, formulação que a jurisprudência recente não autoriza. A segunda trata identidade sintética, impersonação e deepfake como sinônimos, quando designam fenômenos com objetos, vítimas e nexos de dano distintos. O recorte aqui proposto é localizar o defeito dentro da cadeia de produção de confiança da identidade bancária, isto é, no processo pelo qual a instituição converte sinais digitais em uma asserção de que existe um titular apto a contratar.

O problema de pesquisa pode ser assim formulado: em que medida a fabricação algorítmica de sinais de identidade altera o conteúdo do dever de segurança bancária na abertura, validação e autenticação de contas e operações, e quais critérios técnicos e probatórios permitem distinguir o fortuito interno e o defeito do serviço da fraude externa sem nexo causal com a infraestrutura bancária? O objetivo geral consiste em construir uma teoria jurídico-técnica brasileira do dever de segurança identitária. Quatro objetivos específicos o desdobram: fixar a taxonomia dos fenômenos; traduzir para o direito a mudança de superfície de ataque documentada pela literatura técnica; sistematizar as fontes normativas e jurisprudenciais desse dever; e propor instrumentos de análise e de prova aplicáveis ao litígio.

3

A hipótese central sustenta que, na era da inteligência artificial generativa, o dever de segurança bancária deve ser interpretado como abrangendo uma dimensão específica de segurança identitária: a instituição deve adotar controles proporcionais ao risco e tecnicamente atualizados para resolver a identidade, validar evidências, verificar o vínculo do requerente, preservar a integridade da captura e do canal, detectar vetores de falsificação conhecidos, monitorar inconsistências e manter trilhas de auditoria capazes de demonstrar a eficácia dos controles. A responsabilidade permanece objetiva quando o dano decorre de fortuito interno, mas não decorre automaticamente da ocorrência da fraude: o defeito e o nexo devem ser localizados na cadeia de confiança. Uma sub-hipótese acompanha o percurso: quanto mais decisivo o algoritmo na aprovação, mais relevante se torna a rastreabilidade das entradas, versões, limiares e exceções que explicam a asserção de identidade.

O artigo está organizado em cinco seções, incluída esta introdução. A segunda fixa a taxonomia da pessoa sintética e constrói o referencial teórico da identidade como representação

institucional. A terceira descreve a metodologia. A quarta expõe e discute os resultados em cinco movimentos: a superfície de ataque contemporânea, as fontes do dever de segurança identitária, a responsabilidade objetiva com localização técnica do defeito, a Matriz LACRE e o Pacote Mínimo de Evidência de Autenticidade. A quinta reúne as considerações finais, com limites e agenda de pesquisa.

2 A PESSOA SINTÉTICA E A PRODUÇÃO INSTITUCIONAL DE CONFIANÇA

A construção do argumento exige dois passos preliminares. O primeiro é terminológico, porque a imprecisão conceitual conduz a erros de qualificação jurídica. O segundo é teórico, e consiste em compreender a identidade bancária como representação que adquire eficácia institucional, o que permite formular com exatidão o que a fraude sintética inverte.

2.1 UMA TAXONOMIA NECESSÁRIA

A expressão identidade sintética não pode servir de rótulo para qualquer golpe que utilize inteligência artificial. Na definição consolidada pelo sistema da Reserva Federal norte-americana, a fraude por identidade sintética é o crime em que os perpetradores combinam informações fictícias e, por vezes, reais, como números de identificação e nomes, para criar identidades novas com o objetivo de fraudar instituições financeiras, órgãos públicos ou indivíduos (Federal Reserve Banks, 2019). A definição revela que o fenômeno antecede a atual onda generativa: a inteligência artificial amplia a escala e a verossimilhança das personas, mas não cria o problema do zero. A persona sintética clássica atravessa verificações cadastrais, constrói histórico de crédito e culmina no saque coordenado dos limites obtidos.

Ao lado dela situam-se fenômenos distintos, que o Quadro 1 organiza. A impersonação usa a identidade de uma pessoa real existente. O deepfake é mídia sintética, vetor de ataque, e não identidade em si. A tomada de conta atinge vínculo legítimo preexistente. A conta receptora, aberta ou mantida de modo irregular, funciona como infraestrutura de golpes praticados contra terceiros que jamais contrataram com a instituição. A separação tem consequência jurídica direta: em identidades integralmente fictícias, a instituição financeira pode ser a vítima econômica direta; em identidades híbridas, pode haver um titular de dado real prejudicado; em contas receptoras, a vítima pode ser um estranho ao contrato. Falar em ampliação de responsabilidade sem separar esses nexos de dano é falar de nada.

Quadro 1 - Taxonomia dos fenômenos de identidade fraudulenta no sistema financeiro

Fenômeno	Objeto	Local típico do risco
Impersonação	Pessoa real existente, cujos dados e face são usados por terceiro	Vínculo entre requerente e identidade; autenticação
Identidade sintética híbrida	Persona composta por atributos reais e fictícios com histórico construído	Resolução da identidade; validação cadastral; coerência entre fontes
Persona integralmente fabricada	Representação sem referente humano legítimo, com documento, face, voz e dispositivo coordenados	Toda a cadeia de comprovação de identidade
Deepfake e mídia sintética	Mídia, não identidade: vídeo facial ou voz clonada para cumprir prova de vida	Captura; detecção de injeção e de apresentação; autenticação
Tomada de conta	Conta legítima existente, acessada por engenharia social ou mídia sintética	Autenticação; recuperação de credenciais; monitoramento
Conta receptora	Conta de pessoa real ou de identidade irregular usada como infraestrutura do golpe	Abertura; conhecimento do cliente; monitoramento; resposta

Fonte: elaboração própria (2026), com base em Federal Reserve Banks (2019) e Financial Crimes Enforcement Network (2024).

2.2 DUPLOS DE DADOS, SUJEITOS DIGITAIS E A INVERSÃO FUNCIONAL

Haggerty e Ericson (2000) formularam o conceito de duplo de dados como resultado da abstração de corpos em fluxos de informação que são reagrupados em representações virtuais dotadas de vida social própria. A ideia foi aprofundada por trabalhos sobre sujeitos digitais e identificação. Goriunova (2019) mostra que sujeitos digitais são construídos por correspondência, correlação e modelagem e podem tornar-se capazes de produzir efeitos. Brensinger e Eyal (2021) descrevem a identificação pessoal como prática organizacional, e não como leitura de uma essência preexistente. Solove (2003), no plano jurídico, deslocou o furto de identidade da categoria de ato isolado do criminoso para a de problema de arquitetura, no qual a vulnerabilidade decorre do modo como as instituições coletam, agregam e utilizam informação para conceder acesso.

A literatura mais recente impede reivindicar originalidade excessiva. Gorichanaz (2024) aproxima expressamente os eus de dados, a inteligência artificial e o furto de identidade, e Lageson (2025) mostra que, diante de sistemas opacos de triagem, indivíduos podem construir e manipular seus próprios duplos de dados para obter acesso institucional. A noção de que representações digitais podem ser estrategicamente fabricadas para enganar organizações possui, portanto, antecedentes claros, e o passo conceitual que este artigo propõe é mais estreito. No modelo clássico, um sujeito preexistente produz rastros, esses rastros são agregados, e a

instituição passa a agir sobre o proxy. Na fraude sintética, o fraudador produz primeiro o proxy: atributos, documento, face, voz, dispositivo e comportamento são organizados para satisfazer os critérios da máquina. Quando a instituição aprova a abertura, o crédito ou a credencial, atribui eficácia institucional à representação. Não surge um novo sujeito de direito; surge uma identidade bancariamente operativa, representação que obtém capacidade de produzir efeitos porque a infraestrutura a reconheceu como legítima.

Essa inversão funcional do duplo de dados deve ser acompanhada de um limite teórico. Não é o algoritmo, isoladamente, que fabrica a pessoa. O sistema sociotécnico, composto por regras de negócio, modelos, fornecedores, bases externas, equipes de conformidade e decisões de risco, converte sinais em uma asserção institucional de identidade. A responsabilidade jurídica, por isso, não pode ser reduzida ao erro de um modelo biométrico; deve examinar a governança e a arquitetura que produziram a asserção. Uma selfie, um documento, um número de inscrição válido e um score facial não são a identidade: cada elemento é evidência, e a decisão de agregá-los e afirmar que existe um titular apto a contratar é o ponto em que a arquitetura bancária produz confiança.

3 METODOLOGIA

6

A pesquisa é de natureza qualitativa, com abordagem exploratória e descritiva e caráter jurídico-dogmático, e combina quatro procedimentos. O primeiro é a análise normativa do direito brasileiro aplicável, com leitura direta dos textos compilados do Código de Defesa do Consumidor, da Lei Geral de Proteção de Dados Pessoais e das normas do Conselho Monetário Nacional e do Banco Central do Brasil sobre abertura de contas, conhecimento do cliente, compartilhamento de indícios de fraude e segurança cibernética. O segundo é o exame de precedentes do Superior Tribunal de Justiça sobre responsabilidade por fraudes bancárias, com consulta aos acórdãos, informativos e notícias oficiais. O terceiro é a revisão narrativa interdisciplinar da literatura de segurança da informação sobre verificação facial, prova de vida e ataques de injeção, e dos estudos sociais sobre identificação e duplos de dados. O quarto é a utilização de documentos técnicos estrangeiros, em especial as diretrizes norte-americanas de comprovação de identidade, como referência persuasiva do que já é reconhecido como controle de garantia de identidade, sem convertê-los em norma brasileira. A delimitação temporal é expressa: a pesquisa foi encerrada em 9 de setembro de 2026.

O levantamento bibliográfico foi realizado em agosto e setembro de 2026, em português e em inglês, com combinações de descritores como identidade sintética, synthetic identity fraud, deepfake, liveness, injection attack, identity proofing, know your customer, dever de segurança, fortuito interno e responsabilidade bancária. A identificação da literatura combinou mecanismos acadêmicos de descoberta e indexação, busca por similaridade semântica e rastreamento de referências, complementados pela consulta direta às páginas dos periódicos, registros de DOI e fontes institucionais oficiais. Os resultados potencialmente relevantes foram confrontados individualmente quanto ao objeto, pertinência temática, natureza da publicação e aderência ao problema de pesquisa. A revisão permanece narrativa: não se executou protocolo de recuperação exaustiva, dupla triagem independente ou fluxograma de seleção, e a escolha das fontes seguiu critérios de pertinência teórica, com prioridade para estudos revisados por pares publicados em periódicos e conferências de referência e para documentos oficiais.

Quatro critérios de cautela orientaram a interpretação. Primeiro, resultados experimentais de segurança não são convertidos em taxas reais de fraude. Segundo, preprints são utilizados apenas para indicar a fronteira tecnológica e são identificados como tal. Terceiro, a expressão estado atual da tecnologia não é lida como obrigação de adotar qualquer novidade, e sim como critério de razoabilidade, proporcionalidade, maturidade e eficácia demonstrável. Quarto, a ausência de evidência técnica não é tratada como evidência de ausência de controle, embora a assimetria informacional torne a lacuna probatória relevante. A pesquisa não envolveu participantes humanos nem dados pessoais, razão pela qual não se submeteu a comitê de ética. Declara-se que ferramentas de inteligência artificial generativa foram utilizadas como apoio à organização e à redação do texto, permanecendo a autoria integralmente responsável pela seleção das fontes, pela análise e pelas conclusões.

4 RESULTADOS E DISCUSSÃO

Os resultados são apresentados em cinco movimentos: a mudança da superfície de ataque, do documento falso à subversão do fluxo de verificação; as fontes e os atributos do dever de segurança identitária; a responsabilidade objetiva com localização técnica do defeito; a Matriz LACRE como teste de suficiência por camadas; e o Pacote Mínimo de Evidência de Autenticidade como instrumento processual.

4.1 DO DOCUMENTO FALSO À SUBVERSÃO DO FLUXO DE VERIFICAÇÃO

A literatura técnica recente descreve uma mudança de capacidade que o direito precisa incorporar. As diretrizes de comprovação de identidade do instituto norte-americano de padrões, em sua quarta revisão, publicada em julho de 2025, decompõem o processo em resolução da identidade, validação da evidência e verificação do vínculo entre requerente e evidência, e reconhecem expressamente que muitos ataques emergentes combinam injeção digital com ferramentas generativas cada vez mais eficazes e acessíveis, inserindo mídia modificada ou forjada entre o ponto de captura e o elemento que realiza a comparação. O documento afirma que todas as formas de comprovação remota de identidade são, de algum modo, vulneráveis a esses ataques, que a comparação biométrica realizada com uma amostra capturada não os previne por si só, e exige controles que aumentem a confiança de que a mídia provém de sensor genuíno, análise da mídia submetida em busca de sinais de manipulação, testes contra artefatos de ataque conhecidos com documentação das taxas de falso negativo, canais protegidos e, quando cabível, revisão humana e atestação do dispositivo (National Institute of Standards and Technology, 2025). A unidade de inteligência financeira dos Estados Unidos, por sua vez, emitiu alerta em novembro de 2024 sobre esquemas de fraude com mídia sintética dirigidos a instituições financeiras, registrando que tais esquemas frequentemente envolvem a alteração ou criação de documentos de identidade fraudulentos para contornar métodos de verificação e autenticação (Financial Crimes Enforcement Network, 2024).

8

A evidência empírica revisada por pares confirma o diagnóstico. Li et al. (2022), em avaliação sistemática de plataformas comerciais de verificação facial de vida com um arcabouço de ataque baseado em deepfakes, verificaram que a maioria das interfaces avaliadas não empregava detecção específica de mídia sintética e que, mesmo entre as que a empregavam, a eficácia era preocupante, com defesas capazes de detectar vídeos sintéticos de alta qualidade e incapazes de detectar os de baixa qualidade. Zhang et al. (2023), em análise sistêmica de sistemas de verificação facial em aplicativos móveis, demonstraram que a maioria dos aplicativos examinados, incluídos alguns com bilhões de instalações, era vulnerável a ao menos um de quatro tipos de ataque cujos pré-requisitos eram facilmente obtidos, como uma única fotografia da vítima, e que a insegurança residia no desenho e na implementação do procedimento de verificação, e não apenas no modelo de aprendizado de máquina. O ponto juridicamente relevante não é generalizar percentuais, e sim derrubar a inferência de que, havendo prova de

vida, havia uma pessoa presente e consentindo: a prova de vida é sinal técnico cuja força probatória depende do desenho, do canal, do ataque considerado e do estado do sistema à época.

Um levantamento sistemático de 2026 sobre ataques a documentos de identidade, ainda em versão preliminar não revisada por pares, propõe modelo unificado de ameaça que reúne ataques de apresentação, injeção digital e síntese por modelos generativos, e identifica um descompasso persistente entre as condições dos conjuntos de referência e a operação real, com detectores que generalizam mal para documentos sintéticos não vistos (Das; C; Ramachandra, 2026). O trabalho é utilizado aqui apenas como indicador de fronteira. A conclusão que o conjunto autoriza é que o ataque contemporâneo é multimodal: a persona sintética é um conjunto coordenado de dados cadastrais, documento, biometria, telefone, dispositivo, endereço de rede, histórico transacional e conexões com outras identidades, o que explica a fragilidade de abordagens monomodais e conduz à decomposição da cadeia de confiança apresentada no Quadro 2. Bello et al. (2026), em revisão sobre verificação de identidade financeira, convergem ao integrar biometria, análise comportamental, explicabilidade e governança, e Sinigaglia et al. (2020), ao mapearem a autenticação multifator em serviços bancários reais, advertem contra a supervalorização de qualquer fator isolado.

Quadro 2 - Cadeia de confiança identitária: camadas, ataques, controles e evidência

Camada	Ataques relevantes	Controle esperado	defensivo	Evidência que deve existir
Resolução da identidade	Combinação de dados reais e fictícios; identidade duplicada; identificador usado em múltiplas personas	Consulta a fontes confiáveis; consistência entre atributos; detecção de vínculos anômalos		Bases consultadas, resultados, regras de resolução e alertas
Documento e evidência	Documento adulterado, sintético, recapturado ou injetado	Validação estrutural, semântica e criptográfica; captura ao vivo; análise de falsificação		Imagem original, metadados, resultado da validação e versão do motor
Vínculo pessoa e evidência	Troca de rosto, morfismo, deepfake, reapresentação	Comparação facial com detecção de apresentação e verificação cruzada		Escore, limiar, eventos do desafio e decisão
Integridade da captura	Câmera virtual, emulador, dispositivo comprometido, injeção de fluxo	Sensor genuíno, atestação do dispositivo, detecção de injeção		Telemetria do dispositivo, integridade do canal e alertas
Autenticação e recuperação	Clonagem de voz, deepfake, troca de chip, engenharia social	Autenticação adaptativa, elevação de fator, regras de recuperação		Fatores usados, mudanças de credencial e escore de risco

Camada	Ataques relevantes	Controle esperado	defensivo	Evidência que deve existir
Monitoramento	Saque coordenado de limites, conta receptora, transações incompatíveis	Análise comportamental, velocidade, rede, bloqueio e revisão		Alertas, perfil histórico, decisões e tempos de resposta

Fonte: elaboração própria (2026), com base em National Institute of Standards and Technology (2025) e nas fontes técnicas citadas.

4.2 O DEVER DE SEGURANÇA IDENTITÁRIA: FONTES E ATRIBUTOS

O ordenamento brasileiro já contém os elementos de um dever de segurança identitária, dispersos em três camadas normativas que a análise sistemática permite integrar. A primeira é consumerista. O art. 14 do Código de Defesa do Consumidor impõe ao fornecedor de serviços responsabilidade independente de culpa pelos danos causados por defeitos relativos à prestação, e seu § 1º define como defeituoso o serviço que não fornece a segurança que o consumidor dele pode esperar, consideradas as circunstâncias relevantes, entre as quais o modo de fornecimento, o resultado e os riscos que razoavelmente dele se esperam e a época em que foi fornecido. O § 2º acrescenta que o serviço não é considerado defeituoso pela adoção de novas técnicas, e o § 3º exonera o fornecedor apenas quando prove que o defeito inexistia ou a culpa exclusiva do consumidor ou de terceiro (Brasil, 1990). A referência à época do fornecimento é decisiva para o tema, porque converte a segurança esperada em padrão historicamente situado: o que era suficiente antes da difusão dos ataques de injeção pode não sê-lo depois.

A segunda camada é a proteção de dados. A Lei Geral de Proteção de Dados Pessoais consagra, no art. 6º, os princípios da segurança, da prevenção e da responsabilização e prestação de contas, este último definido como a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância das normas e, inclusive, a eficácia dessas medidas. O art. 46 exige medidas técnicas e administrativas aptas a proteger os dados pessoais, seu § 1º autoriza padrões mínimos que considerem a natureza das informações, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados sensíveis, e seu § 2º determina que essas medidas sejam observadas desde a fase de concepção do produto ou serviço até sua execução. O art. 45 preserva, nas relações de consumo, as regras de responsabilidade próprias (Brasil, 2018). A biometria facial empregada na verificação é dado sensível, o que confere dupla natureza jurídica ao controle: é simultaneamente medida de segurança e tratamento que exige salvaguardas.

A terceira camada é a regulação setorial, e ela é mais densa do que o debate costuma reconhecer. A Resolução CMN nº 4.753/2019, em seu art. 2º, exige das instituições, para a abertura de conta de depósitos, procedimentos e controles que permitam verificar e validar a identidade e a qualificação dos titulares e a autenticidade das informações fornecidas, inclusive mediante confrontação com bancos de dados de caráter público ou privado, e seu art. 8º impõe que os critérios de identificação e qualificação sejam formalizados em documento à disposição do regulador (Conselho Monetário Nacional, 2019). A Resolução BCB nº 96/2021 replica a exigência, em seu art. 4º, para as contas de pagamento (Banco Central do Brasil, 2021b). A Circular BCB nº 3.978/2020 estrutura os procedimentos destinados a conhecer o cliente, exige a verificação e a validação da autenticidade das informações de identificação e determina que a qualificação seja reavaliada de forma permanente, conforme a evolução da relação de negócio e do perfil de risco (Banco Central do Brasil, 2020). A Resolução Conjunta nº 6/2023 impõe o compartilhamento de dados sobre indícios de fraude entre instituições, com a finalidade de subsidiar seus controles preventivos, e seu art. 12 esclarece que o compartilhamento não exime a instituição da responsabilidade de efetuar os próprios procedimentos e controles de prevenção (Conselho Monetário Nacional; Banco Central do Brasil, 2023), e a Resolução BCB nº 343/2023 fixa o escopo mínimo desse compartilhamento, que abrange a abertura e a manutenção de

Dois desenvolvimentos recentes reforçam a lógica de defesa em profundidade. O primeiro é o sistema instituído pela Resolução BCB nº 475/2025, em funcionamento desde 1º de dezembro de 2025, que permite ao cidadão registrar restrição à abertura de contas em seu nome e cuja consulta prévia tornou-se obrigatória, por alterações nas Resoluções CMN nº 4.753/2019 e BCB nº 96/2021, antes da abertura de contas de depósitos, de poupança e de pagamento pré-pagas, permanecendo a decisão sob exclusiva responsabilidade da instituição (Banco Central do Brasil, 2025b; Conselho Monetário Nacional, 2019). O próprio regulador registrou, ao lançá-lo, que o sistema não substitui outras medidas de segurança, por se tratar de camada extra de proteção, e que as instituições devem continuar verificando a identidade dos clientes e a autenticidade das informações (Banco Central do Brasil, 2025a). O segundo é a atualização das normas de segurança cibernética. As Resoluções CMN nº 4.893/2021 e BCB nº 85/2021 exigem que a política de segurança contemple a capacidade de prevenir, detectar e reduzir a

vulnerabilidade a incidentes, controles de rastreabilidade da informação e procedimentos que abrangam, no mínimo, a autenticação, os mecanismos de rastreabilidade e a avaliação e correção de vulnerabilidades, e, em redação atualizada em dezembro de 2025, determinam trilhas de auditoria do processamento fim a fim dos dados, com registros que possibilitem identificar falhas ou comportamentos atípicos e retenção segura dessas trilhas (Conselho Monetário Nacional, 2021; Banco Central do Brasil, 2021a).

Da integração dessas camadas extrai-se a categoria proposta. O dever de segurança identitária é a dimensão do dever de segurança bancária que recai sobre o desenho, a operação, a atualização e a demonstração dos mecanismos pelos quais a instituição resolve, valida, verifica e mantém a confiança na identidade de quem ingressa ou atua no serviço financeiro. Trata-se de construção dogmática de sistematização, e não de dever novo criado sem fonte positiva. Quatro atributos o definem. Ele é proporcional ao risco, porque o nível de garantia não precisa ser idêntico para todas as relações, como reconhece a regulação ao vincular a qualificação ao perfil de risco. É dinâmico, porque técnicas de ataque e de defesa mudam, e tanto a época do fornecimento quanto o estado atual da tecnologia impedem julgar a suficiência do controle por uma fotografia congelada do mercado. É sistêmico, porque a segurança depende do fluxo completo e dos fornecedores, de modo que a terceirização da verificação não retira essa dimensão do serviço, ainda que a alocação interna entre banco e fornecedor seja questão distinta da análise perante o consumidor. É demonstrável, porque a prestação de contas e as trilhas de auditoria convertem a reconstrução da decisão de aceitar a identidade em ônus que recai sobre quem controla o sistema. A literatura comparada confirma essa direção: McGeeveran (2019) demonstra a convergência dos padrões de segurança de dados em torno da razoabilidade e da avaliação de risco, e não de regras tecnológicas fixas, e Shpachuk, Markova e Adamyk (2026), ao tratarem dos riscos jurídicos da fraude financeira impulsionada por inteligência artificial, defendem controles internos, testes contínuos e trilhas de auditoria como proteções institucionais.

Entre os antecedentes internacionais mais próximos, Delva Benavides, Leos Navarro e García Hernández (2026) propõem, para bancos digitais e fintechs, um modelo integrado de autenticidade, rastreabilidade e alocação de responsabilidade em fraudes com deepfakes, considerando fatores como capacidade de controle, previsibilidade do risco e capacidade probatória. A presente pesquisa não reivindica originalidade sobre esses vetores gerais de

imputação. Sua contribuição específica consiste em reconstruí-los no ordenamento brasileiro a partir da articulação entre proteção do consumidor, proteção de dados, regulação bancária e prova digital, distinguindo o juízo de responsabilidade da análise prévia de suficiência da própria segurança identitária e propondo instrumentos voltados à localização do defeito dentro da cadeia de confiança.

4.3 RESPONSABILIDADE OBJETIVA COM LOCALIZAÇÃO TÉCNICA DO DEFEITO

O ponto de partida jurisprudencial é conhecido. No Recurso Especial nº 1.197.929/PR, julgado pela Segunda Seção em 2011 sob o rito dos repetitivos, o Superior Tribunal de Justiça assentou que as instituições bancárias respondem objetivamente pelos danos causados por fraudes ou delitos praticados por terceiros, exemplificando com a abertura de conta-corrente ou o recebimento de empréstimos mediante fraude ou utilização de documentos falsos, porque tal responsabilidade decorre do risco do empreendimento e caracteriza fortuito interno (Superior Tribunal de Justiça, 2011). A tese foi cristalizada na Súmula nº 479 (Superior Tribunal de Justiça, 2012). Essa base acomoda, em princípio, versões tecnologicamente novas do mesmo risco, desde que o evento permaneça ligado à atividade e haja nexo causal.

13

A evolução posterior impede, contudo, a leitura automática. No Recurso Especial nº 2.052.228/DF, a Terceira Turma afirmou que o dever de segurança abrange a integridade patrimonial do consumidor, que a instituição que possibilita a contratação facilitada por aplicativos tem o dever de desenvolver mecanismos que identifiquem e obstem movimentações destoantes do perfil do consumidor, notadamente em valores, frequência e objeto, e que a ausência de procedimentos de verificação para transações atípicas corresponde a defeito na prestação do serviço (Superior Tribunal de Justiça, 2023). A segurança, portanto, é continuada e não se esgota na abertura da conta. No Recurso Especial nº 2.124.423/SP, julgado por maioria em 2024, a mesma Turma enfrentou a relação entre a vítima de um golpe e o banco no qual os estelionatários mantinham a conta receptora, do qual a vítima não era cliente. O acórdão afirmou que as instituições devem verificar e validar a identidade e a qualificação dos titulares e a autenticidade das informações, nos termos da Resolução CMN nº 4.753/2019, que a falta de demonstração dessas diligências configura falha no dever de segurança e que, comprovado o cumprimento, não há defeito que atraia a responsabilidade objetiva, ainda que a instituição atue exclusivamente em meio digital (Superior Tribunal de Justiça, 2024).

A linha subsequente confirma a estrutura bifronte. No Recurso Especial nº 2.222.175/SP, a Terceira Turma não conheceu do recurso da instituição e manteve a conclusão da origem de que a abertura de conta por terceiro fraudador, sem conferência da autenticidade dos documentos, configurara falha na prestação do serviço e viabilizara golpe contra terceiro (Superior Tribunal de Justiça, 2025). No Agravo em Recurso Especial nº 3.193.758/SP, a Quarta Turma assentou que, constatada a falha na abertura de conta em plataforma digital e nas transações subsequentes, impõe-se a responsabilidade objetiva das fornecedoras, em linha com o regime consumerista e com o risco do empreendimento (Superior Tribunal de Justiça, 2026a). Em sentido complementar, no Recurso Especial nº 2.209.868, a Terceira Turma afirmou que a responsabilidade por prejuízos decorrentes do golpe da falsa central de atendimento não é automática, dependendo da demonstração de falha na prestação do serviço, como a não identificação de operações incompatíveis com o perfil, a insuficiência dos mecanismos de segurança ou outro elemento que vincule a fraude ao risco da atividade, e reconheceu, no caso, culpa exclusiva da vítima e de terceiros, com rompimento do nexo causal nos termos do art. 14, § 3º, II, do Código de Defesa do Consumidor (Superior Tribunal de Justiça, 2026b).

Lidos em conjunto, esses precedentes autorizam denominar o regime vigente de responsabilidade objetiva com localização técnica do defeito. A instituição responde independentemente de culpa, mas o defeito e o nexo precisam ser demonstrados, e a prova da diligência exonera. A contribuição que este artigo propõe incide precisamente sobre o conteúdo dessa prova em 2026. Em um ambiente no qual a injeção de mídia e o deepfake são riscos documentados e reconhecidos por padrões técnicos e alertas oficiais, a demonstração de diligência não se esgota na apresentação de documentos pessoais nem na afirmação de que houve biometria. A pergunta passa a ser quais controles foram efetivamente utilizados, contra qual classe de ataque foram testados e qual trilha permite reconstruir a decisão de aceitar a identidade. Essa mudança é compatível com a jurisprudência que exige defeito e nexo, porque melhora a qualidade da prova em vez de presumir responsabilidade, e converge com a preocupação de Kjørven (2020) de que a digitalização não desloque excessivamente para o consumidor o risco da fraude que a arquitetura do serviço tornou possível. A literatura brasileira recente sobre responsabilidade civil por falhas de segurança e violação dos deveres de conhecimento do cliente (Bitelli; Marques, 2026) confirma a consolidação da tese geral, e sua

lacuna específica, relativa à inteligência artificial generativa e ao fluxo de verificação, é a que este trabalho procura ocupar.

A tipologia de vítimas completa a análise do nexó. O cliente legítimo impersonado exige que se pergunte se a falha ocorreu na autenticação, na recuperação de credenciais ou no monitoramento do próprio vínculo. O titular de dado real usado em persona híbrida, que não é cliente, exige que se pergunte se a instituição falhou em resolver e validar a identidade e, com isso, causou negativação, cobrança ou exposição. O terceiro defraudado por conta receptora exige que se pergunte se a falta de diligência na abertura ou na manutenção da conta foi condição causal relevante para o golpe, e é exatamente nesse ponto que a jurisprudência ora reconhece, ora afasta a responsabilidade conforme a prova concreta das diligências. A instituição financeira vítima de persona integralmente fictícia, por fim, enfrenta problema de perda interna e gestão de risco, e não de responsabilidade consumerista perante um indivíduo. A divergência aparente entre os precedentes sobre contas receptoras reforça a necessidade de análise probatória concreta da cadeia de identidade, que os dois instrumentos seguintes procuram operacionalizar.

4.4 A MATRIZ LACRE

A cadeia de confiança identitária permite localizar tecnicamente o defeito ao decompor a abertura e a autenticação em pontos de confiança sucessivos: a resolução da identidade, a validação da evidência, a verificação do vínculo entre requerente e evidência, a integridade da captura e do canal, a emissão e o uso de credenciais e a continuidade do monitoramento. A Matriz LACRE traduz essas etapas em cinco perguntas jurídicas de suficiência. Ela é apresentada como heurística analítica para a doutrina, para a conformidade e para a prova judicial, e não como padrão normativo oficial nem como reivindicação de prioridade absoluta, pois modelos de comprovação de identidade existem na literatura técnica e critérios de controle, previsibilidade e auditabilidade já aparecem em propostas jurídicas comparadas. Sua especificidade está na tradução brasileira integrada, que testa a qualidade da própria segurança identitária antes de perguntar quem controlava a camada, se o risco era previsível, se a medida era razoavelmente disponível e se a falha contribuiu causalmente para o dano. O Quadro 3 formula a matriz.

Os cinco eixos não resultam de seleção meramente nominal. O lastro identitário decorre dos deveres de identificação, qualificação e validação de informações presentes na regulação

bancária; a autenticidade da captura traduz os riscos de apresentação e injeção reconhecidos pela literatura técnica e pelos padrões de identity proofing; a coerência cruzada corresponde à necessidade de não avaliar isoladamente sinais cadastrais, biométricos, contextuais e comportamentais; a rastreabilidade e a revisibilidade decorrem dos deveres de prestação de contas, documentação e trilhas de auditoria; e a evolução do risco resulta da conjugação entre a época do fornecimento do serviço, o estado atual da tecnologia, a avaliação de vulnerabilidades e a atualização permanente dos controles. A Matriz LACRE é, assim, uma síntese funcional desses vetores normativos e técnicos, e não a criação autônoma de um padrão de segurança.

Quadro 3 - Matriz LACRE de segurança identitária

Camada	Pergunta de suficiência	Indicadores
Lastro identitário	A representação possui lastro verificável em fontes confiáveis e não apresenta conflitos de unicidade ou coerência?	Bases oficiais e privadas; identificador fiscal; sistema de restrição do regulador; duplicidades; vínculos entre telefone, endereço e dispositivo
Autenticidade da captura	Há confiança razoável de que documento, face ou voz foram capturados de fonte genuína e não injetados?	Captura ao vivo; detecção de apresentação; detecção de câmera virtual; atestação do dispositivo; canal protegido
Coerência cruzada	Os diversos sinais convergem entre si e com o comportamento esperado?	Documento e face; dados e bureau; dispositivo e geografia; velocidade; análise de rede; capacidade econômico-financeira
Rastreabilidade e revisibilidade	É possível reconstruir por que a identidade foi aceita e revisar a decisão?	Registros; versão do modelo; escore e limiar; regras; alertas; revisão humana; fornecedor
Evolução do risco	Os controles foram avaliados e atualizados diante de ameaças conhecidas e de mudanças do estado tecnológico?	Inteligência de ameaças; testes adversariais; taxas de falsa aceitação e rejeição; correções; monitoramento de desvio; revisão periódica

Fonte: elaboração própria (2026).

A matriz opera de modo cumulativo, e suas duas últimas camadas têm natureza distinta das três primeiras. Lastro, autenticidade e coerência dizem respeito ao caso concreto: perguntam se aquela identidade foi aceita com base em sinais suficientes. Rastreabilidade e evolução dizem respeito à governança: perguntam se a instituição consegue demonstrar o que fez e se manteve seus controles atualizados. A distinção importa para o nexos. Uma falha nas três primeiras camadas tende a ser diretamente causal, porque foi ela que permitiu à representação adquirir eficácia bancária. Uma falha nas duas últimas atua sobretudo no plano probatório: a instituição

que não consegue reconstruir sua decisão, ou que ignorou ameaças documentadas, dificilmente conseguirá provar que o defeito inexistiu, como lhe exige o art. 14, § 3º, I, do Código de Defesa do Consumidor.

4.5 O PACOTE MÍNIMO DE EVIDÊNCIA DE AUTENTICIDADE

A contribuição processual do artigo consiste em estabelecer quais evidências devem ser buscadas quando a autenticidade da abertura de conta ou da contratação é contestada. O objetivo não é impor, por via doutrinária, lista rígida aplicável a todos os casos, e sim oferecer um roteiro probatório proporcional ao risco e à arquitetura efetivamente utilizada, que dialogue com o princípio da prestação de contas da Lei Geral de Proteção de Dados Pessoais e com as trilhas de auditoria fim a fim exigidas pela regulação de segurança cibernética. O Quadro 4 apresenta o Pacote Mínimo de Evidência de Autenticidade.

Quadro 4 - Pacote Mínimo de Evidência de Autenticidade

Grupo	Elementos mínimos a buscar	Questão que responde
Sessão	Identificador da sessão, data e hora, duração, sequência de etapas e eventos de exceção	O que aconteceu e em que ordem?
Documento	Arquivo original, método de captura, metadados, zona de leitura mecânica e resultado da validação estrutural, semântica e criptográfica	A evidência era autêntica e estava presente?
Biometria	Imagem ou vídeo original preservado quando lícito, escore, limiar, detecção de apresentação, desafio e sinalizações	O sistema ligou corretamente requerente e identidade?
Integridade da captura	Detecção de câmera virtual, emulador ou dispositivo comprometido, atestação, integridade do componente e do canal	A mídia veio de sensor genuíno?
Modelo e fornecedor	Nome e versão do componente, data de implantação, configuração, mudanças e prestador	Qual tecnologia tomou a decisão?
Dispositivo e rede	Impressão do dispositivo, endereço de rede, localização quando pertinente, linha telefônica, velocidade e correlações	Havia sinais contextuais de inconsistência?
Bases e conhecimento do cliente	Fontes consultadas, resultados, consulta ao sistema de restrição, alertas compartilhados, qualificação e escore de risco	O lastro foi efetivamente verificado?
Decisão	Regra ou modelo acionado, escore final, exceções, sobreposição manual e revisão humana	Por que a identidade foi aceita?
Pós-abertura	Primeiras operações, elevação de limites, crédito, transferências, perfil, alertas e bloqueios	O risco emergiu depois e foi monitorado?
Governança	Testes contra ataques conhecidos, desempenho, revisão de vulnerabilidades e incidentes semelhantes	O controle era adequado ao estado do risco?

Fonte: elaboração própria (2026).

O pacote enfrenta uma assimetria processual característica desses litígios: a instituição detém os elementos técnicos decisivos, enquanto o consumidor ou o terceiro dispõe apenas do resultado, isto é, do contrato, do débito ou da conta que nega ter criado. A regra analítica que decorre do conjunto é que a ausência de registros que deveriam existir não prova, por si, que houve defeito, mas enfraquece de modo relevante a capacidade da instituição de demonstrar a adequação do serviço em matéria sob sua esfera técnica e informacional. Aplicado ao caso da introdução, o pacote conduz a perguntas verificáveis: se a persona foi confrontada com bases confiáveis e com o sistema de restrição do regulador; se a captura passou por detecção de injeção ou apenas por comparação facial; se os sinais de dispositivo, rede e comportamento eram coerentes; e se a instituição consegue reconstruir, com registros datados, por que aceitou aquela identidade. As respostas distinguem a diligência efetiva da diligência apenas alegada.

5 CONSIDERAÇÕES FINAIS

Este artigo perguntou em que medida a fabricação algorítmica de sinais de identidade altera o conteúdo do dever de segurança bancária, e quais critérios técnicos e probatórios permitem distinguir o fortuito interno e o defeito do serviço da fraude externa sem nexo causal com a infraestrutura bancária. A resposta construída articula três camadas.

18

A primeira é conceitual. Identidade sintética, impersonação, deepfake, tomada de conta e conta receptora não são sinônimos, e a separação dos nexos de dano precede qualquer juízo de responsabilidade. A inteligência artificial generativa não cria novo regime de responsabilidade bancária; altera a superfície técnica sobre a qual os deveres existentes incidem. A fraude sintética inverte funcionalmente o duplo de dados: o proxy é fabricado antes do sujeito, e a instituição, ao aceitá-lo, atribui-lhe eficácia bancária. Identidade é uma asserção institucional, e não um escore biométrico.

A segunda é dogmática, e confirma a hipótese central. O ordenamento brasileiro já contém os elementos de um dever de segurança identitária, integrado a partir da segurança esperada e da época do fornecimento no Código de Defesa do Consumidor, dos princípios de segurança, prevenção e prestação de contas e do estado atual da tecnologia na Lei Geral de Proteção de Dados Pessoais, e dos deveres setoriais de verificar identidade, conhecer o cliente, compartilhar indícios de fraude e manter rastreabilidade e trilhas de auditoria. Esse dever é proporcional, dinâmico, sistêmico e demonstrável. A responsabilidade permanece objetiva nos

limites do fortuito interno, mas não é automática: a jurisprudência recente exige defeito e nexo demonstráveis, admite a prova da diligência como exoneração e reconhece a culpa exclusiva como rompimento do nexo. O que muda é o conteúdo da prova de diligência, que não se esgota em documentos pessoais nem na afirmação de que houve biometria.

A terceira é propositiva. A cadeia de confiança identitária explica onde o sistema produz a identidade; a Matriz LACRE testa a suficiência da segurança por camadas, separando as falhas diretamente causais das falhas de governança que operam no plano probatório; e o Pacote Mínimo de Evidência de Autenticidade torna o debate judicialmente verificável, ao enumerar o que deve ser buscado quando a autenticidade é contestada. Os três instrumentos são contribuições heurística e probatória ancoradas em normas existentes, sem reivindicação de prioridade absoluta, e sua utilidade está em converter o debate abstrato sobre inteligência artificial em critérios concretos de defeito, nexo, prova e alocação de risco.

As limitações são explícitas. A pesquisa foi encerrada em 9 de setembro de 2026, com parte da literatura ainda em versão preliminar; a evidência técnica provém de contextos experimentais e estrangeiros, e sua transferência ao mercado brasileiro é inferencial; os padrões norte-americanos foram utilizados como referência persuasiva, e não como norma; e os instrumentos propostos são ferramentas analíticas sujeitas a refinamento pela prática regulatória e judicial. Dessas limitações decorre a agenda: examinar decisões estaduais sobre deepfakes e biometria; estudar a responsabilidade regressiva entre instituições e fornecedores de verificação; investigar a prova pericial de injeção em processos reais; e avaliar a convergência entre proteção de dados, prevenção à lavagem e proteção do consumidor em modelos integrados de garantia de identidade.

A conclusão que o estudo autoriza é sóbria. Quando a instituição transforma sinais digitais em uma asserção de identidade capaz de abrir conta, obter crédito, recuperar acesso ou movimentar recursos, o dever de segurança deve abranger a confiabilidade dessa transformação. Em fraudes sintéticas, o defeito não precisa residir em um documento isolado: pode estar na resolução da identidade, na validação da evidência, no vínculo biométrico, na integridade da captura, na autenticação ou no monitoramento. A responsabilidade objetiva será sustentável quando essa falha integrar o risco da atividade e contribuir causalmente para o dano, sem que culpa exclusiva ou fortuito externo rompam o nexo. A identidade que o algoritmo fabricou só

se torna bancariamente operativa porque uma arquitetura a aceitou, e é sobre a qualidade demonstrável dessa aceitação que o direito deve incidir.

REFERÊNCIAS

BANCO CENTRAL DO BRASIL. Circular nº 3.978, de 23 de janeiro de 2020. Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de “lavagem” ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016. Brasília, DF: BCB, 2020. Texto consolidado.

BANCO CENTRAL DO BRASIL. Resolução BCB nº 85, de 8 de abril de 2021. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. Brasília, DF: BCB, 2021a. Texto consolidado.

BANCO CENTRAL DO BRASIL. Resolução BCB nº 96, de 19 de maio de 2021. Dispõe sobre a abertura, a manutenção e o encerramento de contas de pagamento. Brasília, DF: BCB, 2021b. Texto consolidado.

BANCO CENTRAL DO BRASIL. Resolução BCB nº 343, de 4 de outubro de 2023. Dispõe sobre as medidas necessárias à execução do compartilhamento de dados e informações sobre indícios de fraudes de que trata a Resolução Conjunta nº 6, de 23 de maio de 2023. Brasília, DF: BCB, 2023. Texto consolidado.

BANCO CENTRAL DO BRASIL. **Banco Central lança o BC Protege+**. Brasília, DF: BCB, 1 dez. 2025a. Disponível em: <https://www.bcb.gov.br/detalhenoticia/20953/noticia>. Acesso em: 9 set. 2026.

BANCO CENTRAL DO BRASIL. Resolução BCB nº 475, de 26 de maio de 2025. Dispõe sobre sistema de comunicação de restrição a contratações no Sistema Financeiro Nacional. Brasília, DF: BCB, 2025b.

BELLO, Ahmed; UZOMA, Charles; ATADOGA, Simon; DEHUMO, Ayanrinno Peter; AKINTOLA, Akinyemi Sadeeq. Responsible AI in financial identity verification and risk mitigation. **Discover Sustainability**, v. 7, n. 1, artigo 1080, 2026. DOI: <https://doi.org/10.1007/s43621-026-03208-7>.

BITELLI, João Pedro Monteiro; MARQUES, Fernando de Oliveira. Aspectos contemporâneos da responsabilidade civil de instituições financeiras: falhas de segurança no serviço bancário e violação às obrigações legais de know your customer e customer due diligence. **Revista DCS**, v. 23, n. 92, artigo e6137, 2026. DOI: <https://doi.org/10.54899/dcs.v23i92.6137>.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**: Brasília, DF, 12 set. 1990. Texto compilado.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: Brasília, DF, 15 ago. 2018. Texto compilado.

BRENSINGER, Jordan; EYAL, Gil. The sociology of personal identification. **Sociological Theory**, v. 39, n. 4, p. 265-292, 2021. DOI: <https://doi.org/10.1177/07352751211055771>.

CONSELHO MONETÁRIO NACIONAL. Resolução CMN nº 4.753, de 26 de setembro de 2019. Dispõe sobre a abertura, a manutenção e o encerramento de conta de depósitos. Brasília, DF: BCB, 2019. Texto consolidado.

CONSELHO MONETÁRIO NACIONAL. Resolução CMN nº 4.893, de 26 de fevereiro de 2021. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. Brasília, DF: BCB, 2021. Texto consolidado.

CONSELHO MONETÁRIO NACIONAL; BANCO CENTRAL DO BRASIL. Resolução Conjunta nº 6, de 23 de maio de 2023. Dispõe sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Brasília, DF: BCB, 2023.

DAS, Gourab; C, Pavan Kumar; RAMACHANDRA, Raghavendra. **From forgeries to foundation models: a systematic survey of identity document attack and detection**. arXiv, 2026. Preprint não revisado por pares. Disponível em: <https://arxiv.org/abs/2607.01442>. Acesso em: 9 set. 2026.

21

DELVA BENAVIDES, Juan Emmanuel; LEOS NAVARRO, Jorge Antonio; GARCÍA HERNÁNDEZ, Alejandro Paul. Deepfakes in onboarding, KYC, and financial fraud: authenticity standards and liability framework for digital banks and FinTech. **Journal of FinTech and Sustainable Finance**, v. 2, p. 1-9, 2026. DOI: <https://doi.org/10.31875/2755-8398.2026.02.01>.

FEDERAL RESERVE BANKS. **Synthetic identity fraud in the U.S. payment system: a review of causes and contributing factors**. [S. l.]: Federal Reserve System, 2019. (Payments Fraud Insights). Disponível em: <https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf>. Acesso em: 9 set. 2026.

FINANCIAL CRIMES ENFORCEMENT NETWORK. **FinCEN alert on fraud schemes involving deepfake media targeting financial institutions**: FIN-2024-Alert004. Washington, DC: FinCEN, 13 nov. 2024. Disponível em: <https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf>. Acesso em: 9 set. 2026.

GORICHANAZ, Tim. Data selves and identity theft in the age of AI. In: ELLIOTT, Anthony (ed.). **The De Gruyter handbook of artificial intelligence, identity and technology studies**. Berlin: De Gruyter, 2024. p. 181-196. DOI: <https://doi.org/10.1515/9783110721751-010>.

GORIUNOVA, Olga. The digital subject: people as data as persons. **Theory, Culture & Society**, v. 36, n. 6, p. 125-145, 2019. DOI: <https://doi.org/10.1177/0263276419840409>.

HAGGERTY, Kevin D.; ERICSON, Richard V. The surveillant assemblage. **The British Journal of Sociology**, v. 51, n. 4, p. 605-622, 2000. DOI: <https://doi.org/10.1080/00071310020015280>.

KJØRVEN, Marte Eidsand. Who pays when things go wrong? Online financial fraud and consumer protection in Scandinavia and Europe. **European Business Law Review**, v. 31, n. 1, p. 77-109, 2020. DOI: <https://doi.org/10.54648/EULR2020004>.

LAGESON, Sarah. The artificially unintelligent data double. **Surveillance & Society**, v. 23, n. 4, p. 491-497, 2025. DOI: <https://doi.org/10.24908/ss.v23i4.20062>.

LI, Changjiang; WANG, Li; JI, Shouling; ZHANG, Xuhong; XI, Zhaohan; GUO, Shanqing; WANG, Ting. Seeing is living? Rethinking the security of facial liveness verification in the deepfake era. In: **USENIX SECURITY SYMPOSIUM**, 31., 2022, Boston. **Proceedings [...]**. Berkeley: USENIX Association, 2022. p. 2673-2690. Disponível em: <https://www.usenix.org/conference/usenixsecurity22/presentation/li-changjiang>. Acesso em: 9 set. 2026.

MCGEVERAN, William. The duty of data security. **Minnesota Law Review**, v. 103, n. 3, p. 1135-1208, 2019. DOI: <https://doi.org/10.24926/265535.971>.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Digital identity guidelines: identity proofing and enrollment**. NIST Special Publication 800-63A-4. Gaithersburg: NIST, 2025. DOI: <https://doi.org/10.6028/NIST.SP.800-63A-4>.

SHPACHUK, Vitaliy; MARKOVA, Olena; ADAMYK, Bogdan. AI-driven financial fraud: key risks and legal protections for financial institutions. **Journal of Banking Regulation**, v. 27, n. 1, artigo 6, 2026. DOI: <https://doi.org/10.1057/s41261-025-00304-y>.

SINIGAGLIA, Federico; CARBONE, Roberto; COSTA, Gabriele; ZANNONE, Nicola. A survey on multi-factor authentication for online banking in the wild. **Computers & Security**, v. 95, artigo 101745, 2020. DOI: <https://doi.org/10.1016/j.cose.2020.101745>.

SOLOVE, Daniel J. Identity theft, privacy, and the architecture of vulnerability. **Hastings Law Journal**, v. 54, n. 4, p. 1227-1276, 2003.

SUPERIOR TRIBUNAL DE JUSTIÇA (Brasil). **Recurso Especial nº 1.197.929/PR**: recurso repetitivo, Tema nº 466. Relator: Min. Luis Felipe Salomão. Segunda Seção. Julgado em 24 ago. 2011. **Diário da Justiça Eletrônico**: Brasília, DF, 12 set. 2011.

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

SUPERIOR TRIBUNAL DE JUSTIÇA (Brasil). **Recurso Especial nº 2.052.228/DF**. Relatora: Min. Nancy Andrighi. Terceira Turma. Julgado em 12 set. 2023. **Diário da Justiça Eletrônico**: Brasília, DF, 15 set. 2023.

SUPERIOR TRIBUNAL DE JUSTIÇA (Brasil). **Recurso Especial nº 2.124.423/SP**. Relatora: Min. Nancy Andrighi. Terceira Turma. Julgado em 20 ago. 2024. **Diário da Justiça Eletrônico**: Brasília, DF, 27 ago. 2024.

SUPERIOR TRIBUNAL DE JUSTIÇA (Brasil). **Recurso Especial nº 2.222.175/SP**. Relatora: Min. Daniela Teixeira. Terceira Turma. Julgado em 25 ago. 2025. **Diário da Justiça Eletrônico Nacional**: Brasília, DF, 28 ago. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA (Brasil). **Agravo em Recurso Especial nº 3.193.758/SP**. Relator: Min. Raul Araújo. Quarta Turma. Julgado em 15 jun. 2026. **Diário da Justiça Eletrônico Nacional**: Brasília, DF, 19 jun. 2026a.

SUPERIOR TRIBUNAL DE JUSTIÇA (Brasil). **Recurso Especial nº 2.209.868**. Relator: Min. Humberto Martins. Terceira Turma. Acórdão publicado em 24 jun. 2026. Brasília, DF: STJ, 2026b.

ZHANG, Xiaohan; YE, Haoqi; HUANG, Ziqi; YE, Xiao; CAO, Yinzhi; ZHANG, Yuan; YANG, Min. Understanding the (in)security of cross-side face verification systems in mobile apps: a system perspective. In: IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 2023, São Francisco. **Proceedings** [...]. [S. l.]: IEEE, 2023. p. 934-950. DOI: <https://doi.org/10.1109/SP46215.2023.10179474>.