FACULDADE VIASAPIENS – FVS
CURSO DE GRADUAÇÃO EM DIREITO

NATANIEL TOMAZ DA SILVA

CONTRATOS ELETRÔNICOS: SEGURANÇA E VALIDADE JURÍDICA

Orientador: Prof. Me. Francisco Danilo de Souza Gomes

TIANGUÁ – CE
2025.2

NATANIEL TOMAZ DA SILVA

CONTRATOS ELETRÔNICOS: SEGURANÇA E VALIDADE JURÍDICA

Monografia apresentada à Faculdade ViaSapiens – FVS como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientador: Prof. Me. Francisco Danilo de Souza Gomes

Orientador metodológico: Professor Me. Francisco Danilo de Souza Gomes.

TIANGUÁ – CE

2025.2

Dados Internacionais de Catalogação na Publicação
Ficha catalográfica elaborada pela Biblioteca da Faculdade ViaSapiens
com os dados fornecidos pelo(a) autor(a)

S586c

SILVA, NATANIEL TOMAZ DA.
CONTRATOS ELETRÔNICOS: SEGURANÇA E VALIDADE JURÍDICA: / NATANIEL TOMAZ DA SILVA - 2025.
58 f.

Trabalho de Conclusão de Curso (graduação) - Faculdade ViaSapiens, Bacharelado em Direito, Tianguá. 2025
Orientação: Me. FRANCISCO DANILO DE SOUZA GOMES
1. Contratos Eletrônicos. 2. Segurança Jurídica. 3. Assinatura Digital. 4. ICP-Brasil. 5. Fraude.. I. Titulo.

CDD 340

FACULDADE
ViaSapiens
A IDENTIDADE DO CONHECIMENTO

FACULDADE
ViaSapiens
A IDENTIDADE DO CONHECIMENTO

FACULDADE VIASAPIENS – FVS
ATA DE DEFESA DE MONOGRAFIA DO CURSO DE DIREITO

Em 15 de dezembro de 2025, às 17h00min, no Auditório 01 da Faculdade ViaSapiens, de modo presencial, compareceram para a **DEFESA PÚBLICA DE MONOGRAFIA** do curso de graduação Direito, requisito obrigatório para a obtenção da aprovação na disciplina de Trabalho de Conclusão de Curso II, o (a) aluno (a): **NATANIEL TOMAZ DA SILVA,** tendo como título do Trabalho **"CONTRATOS ELETRÔNICOS: SEGURANÇA E VALIDADE JURÍDICA"**, e os professores que constituíram a Banca Examinadora:

a) Professor-orientador: Prof. Me. Francisco Danilo de Souza Gomes;
b) Professora-examinadora: Profa. Esp. Yara Cavalcante da Silva;
c) Professor-examinador: Prof. Esp. Daniel de Vasconcelos Mello.

Após a apresentação da Monografia e as observações dos membros da banca avaliadora, ficou definido que o trabalho foi APROVADO, com média 10, (DEZ), a partir das seguintes notas:

EXAMINADOR(A)	NOTA	VISTO
Prof. Me. Francisco Danilo de Souza Gomes	10,0	
Profa. Esp. Yara Cavalcante da Silva	10,0	
Prof. Esp. Daniel de Vasconcelos Mello	10,0	

Eu, Francisco Danilo de Souza Gomes, professor-orientador, lavrei a presente ata, que segue assinada por mim e pelos demais membros da Banca Examinadora.

Reformulações:
(X) Não.
( ) Sugeridas
( ) Exigidas

Professor Me. Francisco Danilo de Souza Gomes
Orientador

Professora Esp. Yara Cavalcante da Silva
Examinadora

Professor Esp. Daniel de Vasconcelos Mello
Examinador

NATANIEL TOMAZ DA SILVA
Aluno

FACULDADE
ViaSapiens
A IDENTIDADE DO CONHECIMENTO

Dedico este estudo monográfico, em primeiro lugar, a Deus, Senhor da minha vida, que me sustenta e me concede sabedoria. Em segundo lugar, à minha esposa, pelo incentivo e pelos conselhos que me impulsionam a crescer, e aos meus pais, que sempre estiveram ao meu lado e me apoiaram até aqui em vários sentidos.

FACULDADE
ViaSapiens
A IDENTIDADE DO CONHECIMENTO

AGRADECIMENTOS

Agradeço à minha esposa pelo apoio, pelas palavras de incentivo e por acreditar em mim. Aos meus pais, sou muito grato pelo amor e por confiarem no meu potencial.

Ao meu orientador, Prof. Me. Francisco Danilo de Souza Gomes, deixo meu reconhecimento pelas orientações e incentivo. Obrigado também aos colegas de turma pela colaboração ao longo da graduação.

E, por fim, a todos que, de alguma forma, tornaram este trabalho possível, expresso meu agradecimento.

FACULDADE
ViaSapiens
A IDENTIDADE DO CONHECIMENTO

"Abre a tua boca em favor dos que não podem se defender; sê o protetor dos direitos de todos os desamparados!
Ergue a tua voz e julga com justiça, defende o pobre e o indigente."

- Provérbios 31:8 e 9 | KJA

RESUMO

O presente estudo monográfico objetivou analisar os contratos eletrônicos no Brasil, focando nos mecanismos de segurança e na validade jurídica, diante do crescente desafio de garantir a integridade desses acordos em um ambiente digital suscetível a fraudes e manipulações de dados. A pesquisa, de abordagem qualitativa, examinou a legislação, a doutrina e a jurisprudência, percorrendo a evolução do Direito Contratual desde o Código Civil de 2002 até os marcos da ICP-Brasil, do Marco Civil da Internet e da LGPD. Constatou-se que o arcabouço normativo nacional é sólido para a validade formal, mas que a principal vulnerabilidade reside na prova do consentimento e na autenticidade das partes frente às modernas fraudes de engenharia social. Os resultados demonstram que a validade jurídica está cada vez mais atrelada à capacidade das instituições de construir uma forte cadeia de custódia da prova, exigindo a adoção de métodos de autenticação avançada, como a biometria e o uso de certificados digitais qualificados, para mitigar os riscos e fortalecer a confiança nas transações. Conclui-se que o futuro da segurança contratual digital no país reside no investimento em tecnologias de prova irrefutável e no contínuo diálogo das fontes jurídicas.

Palavras-chave: Contratos Eletrônicos. Segurança Jurídica. Assinatura Digital. ICP-Brasil. Fraude.

ABSTRACT

This monographic study aimed to analyze electronic contracts in Brazil, focusing on security mechanisms and legal validity, in light of the growing challenge of ensuring the integrity of these agreements in a digital environment susceptible to fraud and data manipulation. The research, with a qualitative approach, examined legislation, doctrine, and jurisprudence, tracing the evolution of Contract Law from the Civil Code of 2002 to the milestones of ICP-Brasil, the Brazilian Internet Civil Framework, and the LGPD. It was found that the national normative framework is solid with regard to formal validity, but that the main vulnerability lies in the proof of consent and in the authenticity of the parties in the face of modern social engineering frauds. The results demonstrate that legal validity is increasingly tied to the ability of institutions to build a strong chain of custody of evidence, requiring the adoption of advanced authentication methods, such as biometrics and the use of qualified digital certificates, to mitigate risks and strengthen trust in transactions. It is concluded that the future of digital contractual security in the country lies in investment in irrefutable proof technologies and in the continuous dialogue of legal sources.

Keywords: Electronic Contracts. Legal Security. Digital Signature. ICP-Brasil; Fraud.

FACULDADE
ViaSapiens
A IDENTIDADE DO CONHECIMENTO

LISTA DE SIGLAS

CF88 – Constituição Federal de 1988.

CGI.br – Comitê Gestor da Internet no Brasil

EDI – Electronic Data Interchange

ICP-Brasil – Infraestrutura de Chaves Públicas Brasileira

LGPD – Lei Geral de Proteção de Dados

STF – Supremo Tribunal Federal.

STJ – Superior Tribunal de Justiça.

UNCITRAL – United Nations Commission on International Trade Law

FACULDADE
ViaSapiens
A IDENTIDADE DO CONHECIMENTO

SUMÁRIO

INTRODUÇÃO

O ato de contratar, solene e físico, migrou para o ambiente virtual. A complexidade jurídica é inversamente proporcional à facilidade do clique.

O presente trabalho tem como tema os contratos eletrônicos, com uma delimitação específica voltada para os mecanismos de segurança e a validade jurídica desses instrumentos no ordenamento brasileiro. O foco está na gestão da tensão entre a agilidade demandada pelo ambiente digital e a proteção contra fraudes e vícios de consentimento.

Vivemos uma era em que a celeridade dita as normas. A possibilidade de fechar negócios internacionais ou resolver pendências cotidianas sem barreiras geográficas é uma conquista que não pode ser revertida. Essa liberdade, contudo, implica o risco à segurança.

No Brasil, o respaldo legal existe, ancorado no Código Civil e na Medida Provisória nº 2.200-2/2001, que equiparam o documento eletrônico ao físico (Brasil, 2001). Entretanto, como bem elucida Carlos Roberto Gonçalves, em seu Direito Civil Brasileiro (2015), as normas gerais de validade, que incluem acordo de vontades, capacidade das partes e objeto lícito, aplicam-se integralmente ao meio eletrônico. A disputa se situa em como transpor esses requisitos clássicos para um ambiente onde a identidade é momentânea e a materialidade do papel inexiste.

O tempo de incerteza e riscos crescentes impõe a formulação do problema de pesquisa que norteia este estudo: como garantir a segurança e a validade jurídica dos contratos eletrônicos em um ambiente digital suscetível a fraudes e manipulações de dados?

A tese central desta monografia reside na insuficiência da mera formalidade legal (como a MP 2.200-2/2001 já é insuficiente), sendo a cadeia de custódia a espinha dorsal da validade.

A justificativa para esta investigação apoia-se na relevância social e econômica do tema. Os contratos eletrônicos já movimentam cifras bilionárias e são o motor do comércio moderno, porém a fragilidade do sistema atinge sua ponta mais vulnerável: o consumidor. Marcelo Barros Falcão da Paixão (2019) demonstra como a hipossuficiência se agrava no ambiente online, onde usuários aderem a termos sem ler ou caem em golpes sofisticados. O trabalho de Paixão (2019) serve como um alerta crítico de que a funcionalidade não pode custar a proteção do indivíduo. Além disso, a segurança jurídica é primordial para o desenvolvimento econômico; sem confiança nas transações digitais, o mercado interrompe a atividade.

A evolução tecnológica deveria democratizar o acesso. Em 2025, ela se tornou um vetor de vulnerabilidade, especialmente para o idoso.

Para responder ao problema proposto, o objetivo geral deste trabalho é analisar os contratos eletrônicos no Brasil, com foco nos mecanismos de segurança e na validade jurídica,

a fim de identificar os principais contrastes presentes no ambiente digital. Desdobram-se, a partir deste, os objetivos específicos: (i) investigar a evolução da legislação brasileira sobre o tema; (ii) identificar os principais tipos de fraudes e a vulnerabilidade dos consumidores; e (iii) propor soluções e analisar as tendências jurisprudenciais para aprimorar a segurança jurídica.

No que tange aos aspectos metodológicos, a pesquisa adota uma abordagem qualitativa, de natureza exploratória e descritiva. O procedimento técnico utilizado é a revisão bibliográfica e documental, baseada na análise de leis, doutrinas e jurisprudências. O embasamento teórico dialoga com autores clássicos e contemporâneos, os quais destacam a segurança no comércio internacional e sugerem a análise de soluções baseadas em evidências. A pesquisa consultou fontes primárias, como o Código Civil, o Código de Defesa do Consumidor (CDC) e a Lei Geral de Proteção de Dados (LGPD), além de decisões do Superior Tribunal de Justiça (STJ).

O autor organizou a monografia em três capítulos, visando a clareza e a progressão lógica das ideias.

O Capítulo 1 realiza a contextualização histórica e conceitual necessária para entender onde estamos. Ele narra a evolução da internet no Brasil, desde os tempos vagarosos da conexão discada até a explosão do comércio eletrônico, e destaca o surgimento da ICP-Brasil como o primeiro grande marco de segurança. Além disso, demonstra como princípios clássicos do Direito, como a autonomia da vontade e a boa-fé, tiveram que se adaptar às pressas para legitimar transações que dispensam o papel.

Já o Capítulo 2 toca na ferida aberta das fraudes e da responsabilidade civil. Discute-se aqui a vulnerabilidade crítica do consumidor, com um olhar que beira a indignação diante dos idosos, o elo mais fraco da corrente digital, que se tornaram alvos preferenciais da manipulação psicológica e da predação eletrônica. O texto analisa como o Judiciário aplica a responsabilidade objetiva aos bancos e expõe um grave gargalo processual: a dificuldade técnica de produzir provas periciais complexas nos Juizados Especiais. Isso muitas vezes deixa a vítima sem saída.

Por fim, o Capítulo 3 aponta caminhos e soluções. O foco recai sobre a jurisprudência recente do STJ, que validou as assinaturas eletrônicas avançadas, quebrando o antigo monopólio da ICP-Brasil e valorizando a prova técnica, como as trilhas de auditoria. Em julgado recente, o Tribunal Superior reconheceu a validade de contratos celebrados por meio de assinaturas eletrônicas que não pertencem ao sistema ICP-Brasil, desde que haja outros elementos que atestem o consentimento e a identidade das partes, como o histórico de auditoria e biometria (SUPERIOR TRIBUNAL DE JUSTIÇA, 2024).

A conclusão deste estudo aponta para o futuro, investigando tecnologias emergentes, a exemplo do *Blockchain*.

Dessa forma, o presente estudo contribuirá não somente para o debate acadêmico, mas para oferecer uma visão eficaz sobre como equilibrar inovação tecnológica e segurança jurídica em uma sociedade cada vez mais conectada.

1. CONTEXTUALIZAÇÃO HISTÓRICA DOS CONTRATOS DIGITAIS

O crescimento dos contratos eletrônicos não foi apenas uma mudança de pequena monta; representou uma revolução histórica na forma como negociamos e interagimos socialmente.

Para compreender esse fenômeno no Brasil, é preciso antes olhar para o processo de democratização da internet, cujos primeiros passos, bem discretos, se deram na década de 1990. Naquele período, a rede mundial de computadores ainda era um território em estágio inicial, restrito aos corredores de universidades e instituições governamentais, alcançando somente 0,5% da população (CGI.br, 1995). Naturalmente, a esfera jurídica reconhecia essa realidade analógica, e os contratos, por sua vez, obedeciam a rituais solenes, dependendo da presença das partes, do papel e do selo dos cartórios, sob a vigência do Código Civil de 1916 (Venosa, 2003).

A virada de chave, contudo, aconteceu em 1995, quando a Embratel começou a comercializar conexões dial-up, inaugurando oficialmente a era da internet comercial no país (Pedrosa; Ferreira, 2021). No entanto, o exato impulso para o comércio eletrônico só veio nos momentos finais daquela década. O surgimento de plataformas pioneiras como Submarino e Mercado Livre, ambas em 1999, transações instantâneas, baseadas em cliques e na aceitação imediata de termos de uso, introduziram uma nova dinâmica (Diniz, 2010).

Apesar de seu caráter inovador, tais iniciativas se desenvolveram em um ambiente de ausência ou deficiência regulatória. O ordenamento jurídico brasileiro meramente não previa as especificidades do digital, evidenciando a urgência de o Direito evoluir para amparar essas novas transações (Coelho, 2016).

A resposta legislativa mais consistente veio em 2001, um marco divisor para a segurança jurídica no ambiente virtual, pois a Medida Provisória nº 2.200-2 instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Essa medida foi indispensável, por estabelecer a equiparação da validade dos contratos realizados online com a dos contratos tradicionais. A lógica baseia-se na confiança técnica: a ICP-Brasil criou um sistema que garante a autenticidade (quem assinou) e a integridade (o que foi assinado) dos documentos. Funciona como um selo de fé pública virtual (Brasil, 2001).

Essa inovação alterou a própria mecânica da manifestação de vontade. Se antes a assinatura em papel era a única prova válida de consentimento, a assinatura digital assumiu esse papel no ambiente imaterial. Agora, um clique, quando suportado pela cadeia de confiança da ICP-Brasil, possui força vinculante. Para entender isso, Guelfi (2007, p. 103) oferece uma explicação precisa:

> As garantias oferecidas pela ICP-Brasil às assinaturas digitais produzidas com certificados emitidos sob a sua égide, dependem da observância desses requisitos técnicos, como a utilização do SHA-1 para a geração do resumo hash.

A crítica que Guelfi teceu em 2007, que parecia uma preocupação acadêmica, hoje se manifesta como um risco de segurança estrutural. O autor defende que a segurança das

assinaturas digitais nessa infraestrutura só se mantém se a Autoridade Certificadora seguir rigorosamente os requisitos técnicos, como o uso do *SHA-1* para a geração do resumo *hash*. Nesse sentido, o autor ressalta que a definição inflexível de algoritmos de função *hash* pelo Comitê Gestor representa um risco estrutural de insegurança, embora assegure teoricamente a responsabilidade da Autoridade Certificadora Raiz (AC-Raiz). No entanto, torna-se problemática quando confrontada a evolução tecnológica, uma vez que a lei não acompanha a velocidade da obsolescência técnica.

É importante notar que nem toda assinatura digital é igual. Dentro dessa estrutura, o sistema se divide em três modalidades, os quais são: simples, avançada e qualificada, assim permitindo que o nível de segurança seja proporcional ao risco do negócio. Uma assinatura simples pode bastar para um formulário de cadastro, mas contratos de alto valor ou risco exigem a assinatura qualificada, que carrega a certeza jurídica da ICP-Brasil (BRASIL, 2020).

Por trás dessa aparente facilidade para o usuário final, existe uma arquitetura criptográfica densa. Algoritmos complexos, autoridades certificadoras e protocolos de segurança atuam discretamente para conferir inquestionabilidade à transação.

O ordenamento jurídico ganhou novo fôlego com o Código Civil de 2002. O novo texto reforçou que princípios clássicos, como a autonomia da vontade e a boa-fé objetiva, não são restritos ao papel; eles permeiam qualquer acordo. Artigos como o 104 (requisitos de validade), que preceituam:

> Art. 104. A validade do negócio jurídico requer:
> I - agente capaz;
> II - objeto lícito, possível, determinado ou determinável;
> III - forma prescrita ou não defesa em lei.

E o Art. 421 (função social do contrato), que preceitua: “A liberdade contratual será exercida nos limites da função social do contrato.” O Judiciário ainda observa as disputas digitais através das lentes opacas do Código Civil de 2002. Em 2023, o Superior Tribunal de Justiça validou a citação realizada por meio de aplicativo de mensagem (SUPERIOR TRIBUNAL DE JUSTIÇA, 2023), sinalizando que a eficácia do ato é superior à sua forma, desde que comprovada a identidade do receptor.

Fábio Ulhoa Coelho (2016) acerta ao observar que os contratos eletrônicos não são coisas estranhas, mas sim uma adaptação dos contratos tradicionais ao meio online, submetendo-se às mesmas diretrizes básicas.

Segundo Rebouças (2018), o avanço tecnológico inédito no fim do século XX criou novas formas de relações jurídicas, permitindo a contratação de produtos e serviços pela

internet. O autor destaca que, desde então, esses contratos eletrônicos se tornaram uma ferramenta principal para a economia moderna e para as empresas, transformando diretamente o mundo jurídico.

Foi nessa ocasião de expansão e risco que depois surgiram novas legislações para conter abusos, notadamente o Marco Civil da Internet, Lei nº 12.965/2014 e a Lei Geral de Proteção de Dados - LGPD, Lei nº 13.709/2018 (Brasil, 2014; Brasil, 2018). O Marco Civil, frequentemente chamado de Constituição da Internet, estabeleceu pilares como a neutralidade da rede e a privacidade, além de validar legalmente documentos com assinatura digital. A lei estabeleceu previsibilidade ao definir a responsabilidade civil dos provedores, que só respondem por danos se descumprirem ordens judiciais de remoção de conteúdo (BRASIL, 2014).

Apesar desses avanços, a tecnologia costuma ser mais rápida que a tinta do legislador. Como bem observa Marcelo Paixão (2019), essa velocidade pode gerar lacunas perigosas, permitindo cláusulas abusivas ou falhas de segurança enquanto a lei tenta se ajustar. Ainda assim, o Marco Civil foi central para criar um ambiente onde direitos e deveres são conhecidos.

Hoje, estamos falando de um mercado que movimenta bilhões. Normas como a Resolução nº 4.283/2013 do Banco Central (Brasil, 2013) regulam contratos bancários digitais para tentar blindar transferências e empréstimos. Contudo, a tecnologia não é infalível e o fator humano continua sendo um ponto crítico.

Os golpes crescem na mesma proporção da digitalização. Uma reportagem citada por Vera Batista (2020) no Correio Braziliense revelou um dado alarmante, que durante a quarentena, as tentativas de fraude contra idosos saltaram 60%, segundo a Febraban. E o perigo não vem apenas de hackers anônimos; muitas vezes envolve táticas de sedução enganosa. O famigerado golpe do motoboy ilustra isso bem, por exemplo, quando criminosos convencem a vítima a entregar seu cartão físico sob o pretexto de uma falsa fraude bancária.

No entanto, o maior risco reside na maneira como o Judiciário tem tratado a questão. Ao aplicar a Súmula 479 do STJ (responsabilidade objetiva dos bancos) sem olhar para a engenharia social subjacente à fraude, o Judiciário corre o risco de fechar os olhos para a causa, tratando apenas o sintoma (o prejuízo). A jurisprudência necessita de maior solidez, exigindo das instituições bancárias uma vigilância redobrada sobre operações atípicas de clientes vulneráveis (Brasil, 2012). Nesse sentido, o Superior Tribunal de Justiça já se manifestou no sentido de que é da instituição financeira o ônus de comprovar a autenticidade da assinatura ou da manifestação de vontade que gerou a contratação, especialmente em casos de empréstimos consignados digitais (SUPERIOR TRIBUNAL DE JUSTIÇA, 2022).

Esse quadro comprova que, embora tenhamos evoluído com a ICP-Brasil e leis de proteção de dados, a competição persiste. Para que o contrato digital inspire confiança equivalente ou superior à do papel, é urgente que o futuro promova a harmonização entre a tecnologia e a legislação.

Em suma, os contratos eletrônicos no Brasil são a consequência natural dessa revolução digital. Para fechar esta contextualização com precisão técnica, recorremos à definição de Andrade (2004, p. 31), que sintetiza a natureza desses instrumentos.

> Negócio jurídico concretizado através da transmissão de mensagens eletrônicas pela internet, entre duas ou mais pessoas a fim de adquirir modificar ou extinguir relações jurídicas de natureza patrimonial.

Ao inserir o contrato eletrônico na Teoria Geral dos Contratos, a doutrina esclarece que não estamos diante de uma nova modalidade jurídica. Trata-se de uma nova técnica de formação de vínculo, ou seja, apenas uma nova forma de contratar que utiliza a tecnologia como meio. Mudou o meio (e-mail, apps, plataformas), mas a forma de criar obrigações patrimoniais permanece. Isso exige do Direito um estado de vigilância constante.

Ao olharmos pelo retrovisor do final do século XX, percebemos que a ideia de contratar sem estar presente fisicamente não é uma invenção da era digital. O mundo jurídico já convivia com contratos por fax, telex, telefone e até por carta. O que mudou, com a expansão da infraestrutura de rede no Brasil, foi a escala e a segurança. Hoje, a tecnologia de chaves criptográficas e certificados digitais transformou aquela antiga validação precária em um sistema ágil e blindado (Silva Júnior et al., 2025).

É indispensável entender, no entanto, que não estamos diante de uma nova espécie jurídica. Trata-se de uma evolução tecnológica do rito, não do direito em si. Em linhas gerais, substituímos a caneta-tinteiro e o carimbo por um *login* e uma senha; a substância, contudo, que engloba a oferta, a aceitação e a manifestação de vontade, mantém-se inalterada.

Para compreendermos como essa mecânica funciona na prática, Tonoli (2013, p. 45 e 46) propõe uma classificação elucidativa sobre as formas de contrato eletrônico. O autor explica que:

> a primeira ocorre inteiramente automatizada, ou ainda, aquela que a relação negocial é ficada entre um indivíduo e um sistema previamente programado. Já segunda é aquela estabelecida diretamente entre duas pessoas via Internet, enquanto a terceira, que seria a mais largamente utilizada, corre entre a pessoa e o site do proponente.

Para compreender as nuances da contratação eletrônica, a doutrina classifica essas interações em três modalidades distintas. A primeira, denominada intersistêmica ou automática, ocorre de forma inteiramente automatizada entre sistemas ou aplicativos, dispensando a

intervenção humana no momento exato da formação do vínculo. A segunda é a modalidade interpessoal, que se estabelece diretamente entre duas pessoas utilizando a internet como meio de comunicação, seja através de e-mail, videoconferência ou aplicativos de mensagens instantâneas. Por fim, a terceira modalidade é a interativa, que acontece entre uma pessoa e o site ou sistema previamente configurado pelo proponente, sendo esta a forma mais largamente utilizada no comércio eletrônico atual (Tonoli, 2013).

Essa distinção nos mostra a amplitude do mercado atual. Temos desde sistemas invisíveis que vendem créditos automaticamente, passando por negociações acordadas diretamente, por videoconferência, até a massiva compra em marketplaces resolvida com um único clique em concordo. O resultado é um mercado dinâmico, mas que exigiu normas coerentes, como a ICP-Brasil, para não operar na base da sorte.

O alicerce teórico internacional que permitiu essa evolução no Brasil foi plantado em 1996, quando a Assembleia Geral da ONU aprovou a Lei Modelo da UNCITRAL sobre Comércio Eletrônico (UNCITRAL, 1996). Pinheiro (2021) destaca o caráter inovador dessa norma, em que o artigo 5º decretou que o formato eletrônico não retira a solidez do vínculo contratual; e no artigo 11, consagrou que contratos formados por mensagens de dados são tão legítimos quanto os de papel.

Aqui consiste o conceito genial da equivalência funcional. A UNCITRAL propôs essa lógica, pois em vez de criarmos um universo paralelo de leis para a internet, basta verificar se o documento digital cumpre a função do impresso. Se ele autentica quem assina, demonstra a oferta e permite consulta futura, não há razão para tratá-lo como inferior. Foi esse princípio que permitiu ao Brasil aceitar toda a infraestrutura de certificação digital sem precisar reinventar a teoria dos contratos (Pinheiro, 2021).

Na realidade, isso evitou um atraso legislativo de décadas. O Brasil pôde adaptar leis existentes ao contexto digital enquanto construía a segurança técnica da ICP-Brasil. Sem esse empurrão internacional, a caminhada rumo aos negócios eletrônicos seria muito mais lenta e permeada por insegurança jurídica.

Curiosamente, o próprio Código Civil de 2002 já deixava uma porta aberta para essa modernização. O artigo 107 estabelece a liberdade de forma, ou seja, a declaração de vontade não precisa seguir um ritual específico, salvo quando a lei exige expressamente. Em outras palavras, a manifestação do consentimento pelo indivíduo pode ocorrer livremente, seja por escrito, verbalmente ou através de qualquer ação que não deixe dúvidas quanto à sua vontade (BRASIL, 2002).

Em conformidade com Silva Júnior et al. (2025), entende-se que esse princípio da

liberdade de forma foi o catalisador que permitiu aos contratos eletrônicos respirarem no Brasil antes mesmo de haver leis específicas. A lógica é cristalina: se a vontade não depende da tinta no papel, por que invalidar um clique, um e-mail ou uma interação em plataforma? O legislador, assim, pôde inserir normas digitais específicas sem demolir a base do Código Civil.

Mais recentemente, a Lei da Liberdade Econômica (Lei 13.874/2019) funcionou como um catalisador, transformando a assinatura eletrônica de uma possibilidade em uma prática corriqueira de mercado. O dispositivo consigna que, desde que resguardada a inviolabilidade do instrumento e a certeza da autoria, a legitimação do negócio digital é inquestionável. (Brasil, 2019).

Embora a Lei da Liberdade Econômica tenha sido um catalisador burocrático, ela delegou ao mercado a definição do que é suficiente em segurança. Essa abertura, sem a devida fiscalização regulatória, pode ser uma porta aberta para o uso de assinaturas simples em negócios de alto risco, enfraquecendo a proteção do consumidor em nome da agilidade.

Para quem vive o dia a dia de startups ou departamentos jurídicos, isso foi uma libertação burocrática. O reconhecimento legal estimulou o uso de autenticações ágeis, como biometria e tokens, provando que um contrato seguro depende mais de tecnologia de ponta do que de pilhas de papel.

Complementando esse panorama, a Lei 14.063 de 2020 (Brasil, 2020) veio para colocar ordem na casa, estabelecendo diretrizes inequívocas para o uso de assinaturas eletrônicas em interações com entes públicos e privados. Ao estabelecer requisitos de segurança e proteção de dados, a lei garantiu que a eficiência não passe por cima da privacidade.

A doutrina jurídica brasileira, atenta a essas mudanças, rapidamente conceituou o fenômeno. Boiago Júnior (2005) oferece uma definição precisa do contrato eletrônico como:

> o negócio jurídico concluído com base na transferência de informações entre computadores e cujo instrumento pode ser plagiado em mídia eletrônica, compreendendo nessa categoria os contratos celebrados via correio eletrônico, Internet, Intranet, EDI (Electronic Data Interchange) ou qualquer outro meio eletrônico.

Essa definição reforça que, apesar da roupagem tecnológica, o Direito mantém o foco no acordo de vontades.

Para organizar esse meio, Pinheiro (2010) estruturou a contratação virtual em três modalidades que nos ajudam a visualizar os enfrentamentos jurídicos. A primeira é a intersistêmica (automática), onde máquinas negociam com máquinas sem intervenção humana direta no momento do fechamento. A segunda é a interpessoal, o clássico acordo entre duas pessoas usando a internet como meio de comunicação. E a terceira, talvez a mais onipresente

hoje, é a interativa, é aquela em que o usuário dialoga com um site, clicando em concordo nos termos de uso. Compreender essas categorias é vital, pois cada uma exige provas e verificações de segurança distintas.

O Poder Judiciário não assistiu passivamente a essa evolução; ele foi protagonista na legitimação dessas tecnologias. O Superior Tribunal de Justiça (STJ, 2018), por exemplo, consolidou o entendimento vital de que a validade dos contratos eletrônicos vai além da mera existência, logo a assinatura digital pode conferir a esses documentos a força de um título executivo extrajudicial. Essa posição foi firmada de maneira contundente no julgamento do Recurso Especial 1.495.920/DF, sob a relatoria do ministro Paulo de Tarso Sanseverino. Em 15 de maio de 2018 (publicado em 07/06/2018), a 3ª Turma estabeleceu uma premissa que hoje sustenta o mercado de crédito digital:

> A assinatura digital de contrato eletrônico tem a vocação de certificar, através de terceiro desinteressado (autoridade certificadora), que determinado usuário de certa assinatura a utilizara e, assim, está efetivamente a firmar o documento eletrônico e a garantir serem os mesmos os dados do documento assinado que estão a ser sigilosamente enviados.

Contudo, se por um lado a tecnologia resolveu o problema da execução da dívida, por outro ela inaugurou uma nova era de preocupações com a privacidade. A entrada em vigor da Lei Geral de Proteção de Dados (LGPD, 2018) adicionou uma camada densa de complexidade a essas relações.

O problema consiste na facilidade perigosa do clique. Basan, Oliveira e Couto (2021, p. 1) alertam que, "em decorrência da *clickwrap*, uma característica própria dos contratos eletrônicos, os dados pessoais dos consumidores se tornaram alvos da coleta, armazenamento e compartilhamento pelos empresários digitais". Ou seja, a mesma ferramenta que agiliza a contratação abre as comportas para a exploração de dados, exigindo que as empresas caminhem na linha entre a usabilidade (UX) e o respeito rigoroso à privacidade.

A situação se agrava, tornando-se crítica, quando consideramos a perspectiva de quem interage com o conteúdo digital. A tecnologia não afeta a todos da mesma forma; existem grupos cuja vulnerabilidade é amplificada pelo digital. Figueira e Couto (2024, p. 1108) concentraram-se na realidade da (hiper)vulnerabilidade do consumidor idoso e proporcionaram uma reflexão necessária sobre cidadania:

> é possível concluir que a pessoa idosa no Brasil se encontra em uma situação de hiper vulnerabilidade diante dos contratos eletrônicos e a forma de minimizar os danos e reconstruir a confiança dos consumidores idosos é a compreensão de todos que a proteção jurídica do consumidor idoso é uma questão de cidadania. Tal visão requer o diálogo das fontes jurídicas na defesa dos direitos dos idosos usando não apenas o Código de Defesa do Consumidor, mas de forma precípua a Constituição Federal e

também o Estatuto da Pessoa Idosa, bem como o Código Civil e jurisprudências.

Essa realidade galhardeia que o sistema jurídico precisa estar em permanente estado de adaptação. As transformações sociais não param. Além dos desafios internos com a população idosa, o Brasil enfrenta a pressão da globalização. O desenvolvimento dos contratos eletrônicos internacionais impõe dilemas de soberania e jurisdição

Como bem observam Pasquot Polido e Silva (2017), quando um contrato possui elementos de conexão com vários países (ex.: servidor nos EUA, comprador no Brasil, pagamento na Europa), gera-se uma incerteza jurídica sobre qual lei aplicar e até sobre a validade da formação do vínculo. É um debate que ganha urgência à medida que o comércio eletrônico ignora fronteiras geográficas.

Olhando para o contexto nacional em retrospectiva, a evolução histórica dos contratos eletrônicos transparece um processo perceptível de amadurecimento. Saímos de uma lacuna legislativa e chegamos a uma regulamentação consideravelmente sólida. O Brasil soube estruturar um sistema jurídico poderoso para disciplinar as transações digitais, equilibrando a doutrina clássica com as novas necessidades.

Corroborando essa visão otimista, a pesquisa de Meira et al. (2024, p. 26) destaca que "a assinatura digital representa um avanço importante na formalização de contratos, proporcionando maior segurança, agilidade e eficiência nas relações jurídicas". Essa afirmação sintetiza o êxito brasileiro, haja vista conseguimos incorporar a inovação tecnológica sem rasgar os princípios fundamentais da segurança jurídica.

O futuro dos contratos eletrônicos no país, portanto, dependerá da nossa capacidade de manter esse equilíbrio delicado. A questão agora não é mais provar que o digital é válido, mas garantir que a inovação tecnológica não empurre a proteção de dados ou a dignidade dos consumidores vulneráveis. Felizmente, a experiência normativa acumulada nas últimas décadas oferece uma base sólida para enfrentarmos o que vem por aí.

1.1. O diálogo das fontes: fundamentos jurídicos e a adaptação do direito contratual

Para compreender a validade dos contratos eletrônicos, não basta analisar a tecnologia; é preciso revisitar os alicerces do Direito Contratual. O primeiro e mais clássico deles, a autonomia da vontade, continua sendo a força motriz que legitima qualquer pacto. No entanto, ao migrarmos para o ambiente digital, esse princípio enfrenta uma crise de identidade. Num contexto onde a concessão de consentimento se tornou, muitas vezes, automática e imediata, a doutrina identifica um fenômeno preocupante, no qual se refere a situação descrita como o

acordo de vontades deixou de ser real para ser aparente (Figueira; Couto, 2024).

O usuário médio aceita termos quilométricos sem qualquer leitura efetiva. Essa assimetria de informação se agrava drasticamente quando olhamos para consumidores idosos, que muitas vezes carecem das ferramentas técnicas para manifestar uma vontade realmente livre. Por isso, a validade do contrato digital não pode se restringir ou depender exclusivamente do simples clique., mas da adoção de interfaces transparentes e mecanismos que garantam a compreensão do que está sendo acordado (Figueira; Couto, 2024).

Historicamente, o Direito Contratual vem evoluindo de uma rigidez formalista para uma valorização da vontade real das partes. Essa transição explica a busca atual pelo equilíbrio. É necessário respeitar a liberdade de contratar, mas estabelecendo proteções contra abusos em contratos de adesão e tecnologias que forçam padrões preestabelecidos. Como apontam Meira et al. (2024), isso requer o desenvolvimento de instrumentos, como cláusulas bem definidas e mecanismos de auditoria da transparência, para as partes envolvidas terem pleno conhecimento dos riscos e compromissos assumidos.

No plano técnico, os elementos estruturais do contrato (manifestação de vontade e capacidade) permanecem intactos, mas ganham uma nova roupagem probatória. A liberdade de forma permite que o negócio seja digital, mas a segurança jurídica exige que a autoria e a integridade sejam auditáveis através de *logs, hashes* e cadeias de certificação. Assim, a autonomia da vontade precisa ser blindada por meios que permitam sua verificação posterior, evitando que a impermanência eletrônica fragilize o consentimento (Silva Júnior et al., 2025).

A complexidade aumenta quando as fronteiras desaparecem. Nos contratos internacionais eletrônicos, a autonomia das partes esbarra na conexão entre ordenamentos jurídicos distintos. Regras antigas, como as da LINDB, muitas vezes se mostram obsoletas diante da fluidez da internet, gerando dúvidas sobre qual lei aplicar. Para mitigar o risco de forum shopping e litígios intermináveis, Pasquot Polido e Silva (2017) propõem soluções, que consistem na previsão contratual expressa da lei aplicável e no uso de arbitragem, além de esforços para uma harmonização normativa internacional.

Por fim, não podemos ignorar a tensão entre a vontade interna (subjetiva) e a declarada. No ambiente digital, a coleta massiva de dados e técnicas de nudging (empurrãozinho comportamental) podem manipular a intenção do usuário. Por isso, a proteção do consumidor exige tanto instrumentos jurídicos quanto barreiras técnicas contra medidas predatórias de dados. A literatura de Basan, Oliveira e Couto (2021) aprofunda essa questão, indicando que, para o consentimento ser livre, é preciso impedir que a tecnologia distorça a vontade real do contratante.

Se a autonomia é o impulso, a boa-fé objetiva é o norte. Ela impõe deveres de lealdade e cooperação que excedem a mera intenção. No mundo online, a boa-fé ganha contornos de experiência geral, assim exige-se transparência nas interfaces e a proibição absoluta de dark patterns que induzam o usuário ao erro ou ao aceite por impulso (Figueira; Couto, 2024).

A transparência torna-se, assim, o escudo do consumidor contra a assimetria informativa. Para que a autonomia não seja uma ficção, Rocha (2024) argumenta que plataformas devem adotar formas de informação acessível, reduzindo o risco de pegadinhas contratuais.

A positivação da boa-fé no Código Civil reforça que a integridade deve estar presente desde a fase pré-contratual. Na quietude do espaço virtual, onde não há o contato pessoal, isso se traduz em avisos prévios e na comunicação honesta sobre as funcionalidades do serviço (Meira et al., 2024). E, para provar que houve lealdade, a tecnologia novamente serve ao Direito, dessa forma, registros de logs e históricos de alterações funcionam como a materialização da boa-fé, permitindo auditorias que garantem a integridade do que foi pactuado (Silva Júnior et al., 2025).

Em escala mundial, a boa-fé é um dos pilares da Convenção das Nações Unidas sobre o Uso de Comunicações Eletrônicas (UNECIC). Em contratos que atravessam fronteiras, cláusulas de governança de dados e resolução de conflitos são centrais para preservar a confiança entre partes sujeitas a leis diferentes (Pasquot Polido; Silva, 2017).

Finalmente, a função social do contrato serve como um limite ético, enfatizando que o acordo privado ultrapassa a esfera individual. Ele deve atender a expectativas de justiça e equilíbrio. No ambiente digital, isso significa que o contrato não pode ser um instrumento de opressão ou de transferência desproporcional de riscos para a parte vulnerável. A dignidade do consumidor e os valores coletivos devem prevalecer sobre a lógica puramente algorítmica (Figueira; Couto, 2024).

Essa exigência é vital nas relações de consumo online. A função social limita a liberdade contratual sempre que cláusulas padronizadas degradam a proteção mínima legal. Em termos operacionais, na perspectiva dos autores Silva Júnior et al. (2025), isso implica criar mecanismos que corrijam desigualdades, evitando que a tecnologia sirva apenas para acelerar a injustiça.

Teoricamente, a discussão conecta a causa do contrato à sua função social. O vínculo jurídico só é legítimo se produzir efeitos econômicos e sociais positivos, respeitando a convivência justa no mercado digital. Essa ênfase amplia o escopo da revisão contratual, visto que o intérprete não deve olhar apenas se a assinatura é válida, mas se o contrato atende ao

interesse público e protege os vulneráveis (Basan et al., 2021).

2. AS FRAUDES ELETRÔNICAS NO CONTEXTO JURÍDICO BRASILEIRO

Para adentrarmos no problema das fraudes eletrônicas, é preciso primeiro despir o conceito de sua roupagem tecnológica e entender sua natureza jurídica. A fraude, infelizmente, tornou-se uma companheira indesejada do cotidiano moderno, mas ela não é um fenômeno novo. Em outras palavras, representa a materialização da má-fé, uma manobra deliberada para enganar a outra parte e obter vantagem indevida, burlando a lei ou o contrato.

O jurista Carlos Gonçalves (2019) nos oferece uma dissecação precisa desse instituto. Ele explica que a fraude ocorre quando alguém, sob a aparência de normalidade contratual, esconde a intenção de prejudicar terceiros, como credores. A doutrina estabelece que essa conduta se sustenta em dois elementos obrigatórios: o elemento objetivo (*eventus damni*), que consiste no ato lesivo concreto, como a alienação de um ativo para forjar a insolvência; e o elemento subjetivo (*consilium fraudis*), o qual é a intenção maliciosa, o acordo ou conluio visando a produção do dano. Sem a união desses fatores, não há fraude; com eles, o negócio jurídico nasce viciado.

No ambiente digital, essa má-fé ganha escala e sofisticação. As fraudes eletrônicas são multiformes. Não estamos falando apenas de falhas de sistema, mas de armadilhas semânticas e visuais. Um exemplo clássico é o *phishing*, o usuário acessa um site que é um exemplo perfeito do seu banco, mas que serve somente para capturar credenciais. Ou então, a falsificação ideológica, onde criminosos utilizam dados vazados para constituir empresas fantasmas ou contrair empréstimos em nome de terceiros, deixando para a vítima o rastro de dívidas e a negativação do nome.

Além dos ataques externos, existe a fraude institucionalizada nas entrelinhas, materializada nas cláusulas abusivas. Especialmente em contratos de empréstimo, é comum encontrar disposições disfarçadas, por exemplo, juros estratosféricos, desrespeito às margens consignáveis (comprometendo a subsistência do devedor) e a cumulação de taxas que transformam a dívida original em uma impagável, na perspectiva dos autores Soares e Carvalho (2023).

O impacto dessas atitudes não é uniforme; ele atinge com crueldade cirúrgica os grupos mais vulneráveis. Nesse contexto, os idosos aparecem como o alvo preferencial. Paixão (2019) argumenta que a vulnerabilidade digital dessa demografia é um convite aos golpistas. Muitos idosos, por não terem nascido na era digital, possuem uma relação de confiança ingênua com a

tecnologia ou dependem de terceiros para operar seus dispositivos. O criminoso, percebendo essa brecha, oferece empréstimos ou serviços facilitados por telefone ou internet. O resultado é a adesão a contratos não compreendidos, gerando prejuízos financeiros devastadores (Paixão, 2019).

A proteção a esse grupo não é apenas uma questão de empatia, mas um mandamento constitucional. O artigo 230 da Constituição Federal (Brasil, 1988) é taxativo ao impor à família, à sociedade e ao Estado o dever de amparar as pessoas idosas, garantindo sua dignidade. Portanto, a segurança digital do idoso sobressai à esfera privada; é uma responsabilidade compartilhada.

Para mitigar esses riscos, a prevenção passa pela educação e pela cautela. Doneda (2021) sugere uma postura de desconfiança ativa. A supervisão de finanças por pessoas de confiança, o ceticismo diante de ofertas urgentes ou vantajosas demais e, precisamente, nunca forneça senhas ou informações sigilosas a indivíduos que se apresentem como funcionários do banco sem antes confirmar a identidade e a solicitação através dos canais de comunicação oficiais da instituição financeira.

Quando a prevenção falha, entramos no território da fraude bancária propriamente dita. Segundo o dicionário Michaelis (2020), trata-se do ato de ludibriar para obter vantagem ilícita. No entanto, as consequências jurídicas desse ato se ramificam.

No campo do Direito Penal, tal conduta está prevista como o crime de estelionato, conforme o artigo 171 do Código Penal. A lei define o crime como a obtenção de vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro mediante artifício ou ardil (Brasil, 2012). É a punição do Estado contra a quebra da ordem social.

Já na esfera cível, o foco muda da punição para a reparação. A vítima tem o direito de buscar o restabelecimento do status quo ante. Isso implica não apenas a devolução dos valores subtraídos (dano patrimonial), mas também a compensação pelo abalo psíquico e o transtorno causado (dano extrapatrimonial). Como bem pontua Paes (2019), o fraudador responde com seu próprio patrimônio para cobrir o prejuízo deixado na vida da vítima.

Para que o golpe se concretize, é necessário um alinhamento de fatores. O fraudador precisa de um ponto de entrada, que geralmente é o vínculo da vítima com uma instituição financeira. Consequentemente, a segurança é comprometida em seu ponto mais vulnerável: as informações pessoais. O comprometimento de senhas e tokens é a principal via para a realização de crimes cibernéticos, seja por meio da entrega voluntária das credenciais pela própria vítima (em casos de engano), ou pela extração técnica, como a utilização de *malware* para infectar dispositivos e furtar informações (Silva, 2020).

Podemos fazer uma analogia com a segurança residencial, a título de exemplo, se deixamos a porta destrancada, facilitamos a invasão. No mundo digital, a porta são os nossos dados. Contudo, diferentemente de um arrombamento físico, a fraude eletrônica muitas vezes conta com a colaboração involuntária da vítima. Os golpistas exploram para manipular emoções, tais como: medo, ganância ou urgência e, assim, perverter a lógica da proteção tecnológica, levando a própria vítima a entregar o que eles buscam.

A resposta do Estado brasileiro a esse panorama busca um ponto de equilíbrio entre o tradicional e o inovador. O sistema jurídico opera como uma colcha de retalhos, unindo leis seculares a normas criadas especificamente para o ecossistema digital. O Código Penal Brasileiro ainda é a primeira linha de defesa, utilizando tipos clássicos como o artigo 171 (estelionato) e o 155 (furto) para punir fraudes eletrônicas, dependendo da moldura do caso (Brasil, 2012). No entanto, a sofisticação do cibercrime logo tornou evidente que as ferramentas analógicas eram insuficientes.

Foi dessa necessidade de tipificação específica que nasceu a Lei de Crimes Cibernéticos (Lei 12.737/2012), popularmente batizada de Lei Carolina Dieckmann. Essa norma foi um marco ao criminalizar a invasão de dispositivo informático, seja ele um celular ou um servidor corporativo (Brasil, 2012). No entanto, a mera literalidade da lei carece de vigor, sendo preenchida pelo papel hermenêutico desempenhado pelos tribunais. O Superior Tribunal de Justiça (STJ) e o Supremo Tribunal Federal (STF) atuam como orientação da aplicação dessas normas aos casos concretos, tentando fechar as brechas que a legislação não previu.

Nessa esfera, a tecnologia funciona como um fiel da balança, muitas vezes inclinando-se para lados opostos. Há décadas, o Judiciário já alertava que a segurança jurídica no ambiente virtual dependeria mais de soluções técnicas do que apenas de leis. Nas palavras visionárias do Ministro do STJ Ruy Rosado de Aguiar (citado na Agência Estado de Notícias, apud Eduardo de Lascio, Módulo e-security, seminário Assinatura e Certificação Digital no Brasil, São Paulo em 19/10/2000):

> O consumidor precisa saber que existe um sistema moderno, já usado em outros países, chamado criptografia. Só com ele é possível controlar a autenticidade e a veracidade das informações em um documento eletrônico. Sem assinatura criptográfica, um documento eletrônico não tem força de prova na justiça (Brasil, 2000).

Foi a tecnologia de criptografia assimétrica (ou de chave pública) que forneceu o lastro técnico necessário para que o documento eletrônico alcançasse a mesma estatura jurídica do documento tradicional. O diferencial dessa técnica existe na capacidade de gerar assinaturas pessoais exclusivas ao cifrar a mensagem com uma chave privada, convertendo um arquivo

comum em evidência legal. Para que esses documentos tenham força probante em juízo, eles precisam superar dois desafios importantes inerentes à sua essência digital, assim precisam garantir a autenticidade e preservar a integridade.

A assinatura digital baseada em criptografia resolve esses problemas de forma simultânea. No que tange à integridade, a tecnologia institui uma forma de imutabilidade lógica. A assinatura está ligada de tal forma à estrutura do arquivo que qualquer mínima modificação posterior no seu conteúdo resulta na quebra imediata do vínculo criptográfico, invalidando automaticamente a assinatura. Já no campo da autenticidade, o sistema permite comprovar a autoria sem margem para dúvidas. Isso ocorre porque o certificado digital, emitido por uma autoridade de confiança, atua como o elo irrefutável que conecta a chave pública ao signatário real, garantindo a individualização segura. Sem essa arquitetura de assinatura criptográfica, o documento eletrônico seria apenas um arquivo volátil, facilmente modificável sem deixar vestígios, o que tornaria inviável provar juridicamente a concordância do remetente.

Essa observação permanece assustadoramente atual, pois a tecnologia apresenta consequências tanto positivas quanto negativas. De um lado, ela potencializa o crime. Atualmente, ferramentas de Inteligência Artificial (IA) são empregadas na criação de *deepfakes*, que são vídeos e áudios sintéticos com um nível de realismo capaz de enganar tanto sistemas biométricos quanto familiares mais atentos. Além disso, a IA é usada para automatizar ataques de *phishing* em escala industrial, permitindo a personalização de mensagens para atingir milhares de vítimas simultaneamente (Rocha, 2024).

Por outro lado, essa mesma tecnologia oferece o antídoto. O *blockchain*, por exemplo, surge como uma arquitetura de confiança, criando registros imutáveis que tornam a fraude financeira muito mais difícil de ser ocultada. Da mesma forma, algoritmos de IA são utilizados para a vigilância e proteção dos bancos modernos, detectando padrões de transações suspeitas em milissegundos, antes que o prejuízo se concretize. O grande dilema, porém, é o compasso descompassado, exemplificando, a legislação é lenta e reflexiva, enquanto a inovação criminosa é ágil. Quase sempre, quando uma lei é aprovada, o modus operandi do crime já evoluiu para explorar uma nova vulnerabilidade (Ferraz, 2019).

Essa dinâmica de perseguição e fuga provoca consequências sociais e econômicas que são quantificáveis. Os relatórios do CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) desenham uma curva ascendente preocupante nos crimes digitais, atingindo indiscriminadamente do cidadão comum às grandes corporações. Essa pressão estatística força o sistema jurídico a agir, mas levanta um debate profundo na academia

e nos tribunais o punitivismo penal é a solução? Ou deveríamos focar recursos na prevenção e na educação digital da população? (Silva, 2020).

A doutrina jurídica tenta iluminar esse caminho. Autores como Danilo Doneda (2021), referência em direito e tecnologia, provocam reflexões sobre como o Brasil pode equilibrar o incentivo à inovação com a necessária segurança. A literatura especializada, tanto nacional quanto estrangeira adaptada à nossa realidade, aponta que as lacunas legislativas não serão resolvidas apenas criando novos crimes, mas entendendo a arquitetura da rede. Além disso, os dados técnicos do CERT.br são vitais para tirar a discussão do campo teórico e focar nas tendências reais das fraudes.

Por fim, é primordial lembrar que o Brasil não é uma ilha digital. Nosso ordenamento jurídico bebeu de fontes internacionais, inspirando-se fortemente em modelos como o da União Europeia, que enfrenta situações idênticas. A análise comparada é útil para refinarmos nossas estratégias. O Brasil historicamente focou muito na tipificação da invasão (o ato do hacker). Jurisdições internacionais têm progredido mais rapidamente na aplicação da responsabilização objetiva de empresas que negligenciam a guarda de dados. Embora o Marco Civil brasileiro trate dessa questão, ainda se observa uma lacuna na sua aplicação com o devido rigor (Pasquot Polido; Silva, 2017).

2.1. Vulnerabilidade e risco: responsabilidade civil e o desafio probatório do consumidor

Não é exagero afirmar que a sociedade moderna atravessa uma revolução comportamental sem precedentes, motorizada pelos avanços tecnológicos das últimas décadas (Rebouças, 2018). Essa virada digital não apenas redefiniu hábitos triviais, mas integrou a tecnologia à própria ossatura do cotidiano, alterando radicalmente como vivemos, nos comunicamos e, sobretudo, como fazemos negócios. Nesse novo ecossistema, a internet deixou de ser acessória para assumir um papel central, impulsionando o comércio eletrônico e gerando um volume massivo de contratos virtuais (Pinheiro, 2016). Contudo, essa moeda tem duas faces se por um lado ganhamos em agilidade e redução de custos, por outro, expusemos consumidores e empresas a uma nova tipologia de delitos e a uma onda crescente de fraudes eletrônicas (Gagliano; Pamplona Filho, 2019).

É necessário desmistificar a natureza jurídica desse fenômeno. Longe de ser uma criação jurídica inédita, o contrato eletrônico é, precisamente, uma nova forma de contratar. Trata-se de um negócio jurídico bilateral, mas agora formalizado através de dispositivos tecnológicos (Rebouças, 2018), onde a manifestação de vontade viaja por dados transmitidos

eletronicamente (Coelho, 2016). Ou seja, mudou-se o meio, mas a estrutura do vínculo obrigacional se mantém (Aquino, 2025).

Portanto, essa modalidade não está isenta de regulamentação legal. Mesmo na ausência de um código exclusivo para a internet, o ordenamento jurídico brasileiro estende seu manto protetor sobre essas relações, aplicando as disposições do Código Civil e, fundamentalmente, do Código de Defesa do Consumidor (Aquino, 2025). O próprio Código Civil já trazia em seu início essa adaptação, ao considerar presente o contratante que negocia por meio de comunicação similar ao telefone (Brasil, 2002); é uma analogia que hoje abraça as interações online instantâneas (Rebouças, 2018). O Superior Tribunal de Justiça (STJ), atento a essa realidade, já reconheceu a executividade desses contratos, desde que blindados por garantias mínimas de autenticidade, como a assinatura digital (Brasil, 2018).

A vulnerabilidade constitui o cerne dessa discussão. O Código de Defesa do Consumidor (CDC) parte da premissa de que o consumidor é a parte frágil da relação (artigo 4º, I), uma realidade que se torna ainda mais aguda no ambiente digital (Brasil, 1990).

A contratação eletrônica traz implicações que o cidadão comum muitas vezes não está aparelhado para enfrentar. A falta de contato físico, a velocidade vertiginosa das transações e a opacidade técnica dos sistemas geram uma assimetria informacional severa (Souza, 2013). O consumidor, seduzido pela conveniência, adere a contratos sem leitura prévia, depositando sua confiança na aparência de segurança da plataforma. É justamente essa confiança que os fraudadores exploram, mimetizando a legitimidade dos canais oficiais para aplicar golpes.

Para agravar a situação, a doutrina aponta para o surgimento de uma vulnerabilidade algorítmica. Empresas utilizam Inteligência Artificial para coletar e tratar dados de forma pouco transparente, moldando a experiência do usuário (Soares; Carvalho, 2023). O vazamento desses dados, seja por negligência ou ataque hacker, transforma-os rapidamente em matéria-prima para a execução de golpes sofisticados. O criminoso aborda a vítima já sabendo seus dados pessoais, conferindo à fraude uma aparência de autenticidade (Pinheiro, 2020).

A situação atinge contornos dramáticos quando falamos dos hipervulneráveis, que são idosos, analfabetos digitais ou pessoas pouco familiarizadas com a tecnologia (Soares; Carvalho, 2023). Paradoxalmente, ferramentas criadas para aumentar a segurança, como a biometria facial ou o QR code, podem se tornar armadilhas. Não são raros os casos no qual se induz a vítima a validar uma operação fraudulenta, acreditando estar cumprindo um procedimento de segurança do banco (Tavares, 2022).

Diante do prejuízo, a questão que deságua no Judiciário é sempre a mesma. Quem paga a conta? A instituição financeira, que aufere lucros com a digitalização, ou o consumidor, que cedeu seus dados?

O norte para essa resposta é a Súmula 479 do STJ: “As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos realizados por terceiros no âmbito de operações bancárias.” (Brasil, 2012). A jurisprudência majoritária entende que as instituições financeiras respondem objetivamente pelos danos gerados por fraudes desempenhadas por terceiros. A lógica é a do fortuito interno, a fraude não é um evento externo imprevisível, mas um risco inerente à atividade bancária digital (Cavalieri Filho, 2012). Se o banco escolhe operar no meio virtual para reduzir custos e aumentar lucros, ele atrai para si a responsabilidade pelos riscos desse empreendimento (Nunes, 2012).

Essa Súmula, ao proteger o consumidor, falha ao incentivar os bancos a aprimorarem a segurança na autenticação. A responsabilidade objetiva deve ser acompanhada por um dever de vigilância reforçada (com base em IA/comportamento atípico do cliente) contra a manipulação psicológica, especialmente com idosos.

No entanto, essa responsabilidade não é absoluta. A soberania constitui-se na análise do caso concreto. Quando a negligência ou o descuido do consumidor é manifesta, manifestada ao ignorar alertas claros ou fornecer senhas voluntariamente, os tribunais podem, assim, reconhecer a culpa exclusiva da vítima, isentando o banco com base no art. 14, § 3º, II, do CDC (Brasil, 1990).

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
> § 3° O fornecedor de serviços só não será responsabilizado quando provar:
> II - a culpa exclusiva do consumidor ou de terceiro.

Existe ainda o caminho do meio, assim a culpa concorrente, onde o prejuízo é rateado porque ambos, banco (por falha de segurança) e consumidor (por negligência), contribuíram para o evento (Gagliano; Pamplona Filho, 2017).

Essa zona cinzenta gera insegurança jurídica. Uma análise dos julgados do Tribunal de Justiça de São Paulo, por exemplo, demonstra disparidade de julgamentos em situações análogas, como o golpe do motoboy, ora condenando o banco, ora absolvendo-o. Isso demonstra a dificuldade real de equilibrar o dever de proteção com o dever de cautela que também cabe ao correntista.

Por fim, a batalha judicial quase sempre se decide no campo probatório. Quando o banco nega a falha e o consumidor alega inocência, a palavra final costuma vir da perícia técnica (Soares; Carvalho, 2023).

A perícia que irá se aprofundar nos registros *(logs)* do sistema para rastrear o *IP*, a geolocalização e o dispositivo usado na fraude, verificando se houve falha na autenticação biométrica (Tavares, 2022). O grande obstáculo, porém, é que essa prova é complexa e cara, o que muitas vezes inviabiliza sua produção nos Juizados Especiais Cíveis (JECs), deixando o consumidor, mais uma vez, em uma encruzilhada jurídica (Soares; Carvalho, 2023).

Paradoxalmente, a estrutura judiciária criada para facilitar a vida do cidadão tornou-se um gargalo para as vítimas de fraudes digitais complexas. Os Juizados Especiais Cíveis (JECs) nasceram sob a égide da celeridade e da simplicidade (Lei nº 9.099/1995), desenhados para causas de menor complexidade (Brasil, 1995). O problema é que auditar uma fraude bancária digital exige uma pericia técnica bem vigorosa, algo que a estrutura sumaríssima dos JECs não comporta (Soares; Carvalho, 2023). O artigo 35 estabelece: “Quando a prova do fato exigir, o Juiz poderá inquirir técnicos de sua confiança, permitida às partes a apresentação de parecer técnico.” A lei permite somente pareceres técnicos ou inquirições simples, ferramentas insuficientes para desvendar os rastros digitais de um crime cibernético.

A proibição de prova pericial complexa nesses tribunais inviabiliza a defesa do consumidor. Sem a análise de logs, time-stamps ou trilhas de auditoria, a vítima é obrigada a provar um fato negativo (não ter autorizado a transação), o que é juridicamente inviável.

A recusa ou incapacidade do Juizado Especial Cível em lidar com a complexidade da prova técnica digital (como a análise de trilhas de auditoria, *IPs* e logs) cria uma barreira de acesso à justiça. O baixo custo da Justiça é pago com a perda da qualidade da prova, deixando o consumidor lesado sem um mecanismo efetivo de defesa pericial.

O resultado é frustrante, pois diante da necessidade de uma perícia complexa, nessa perspectiva, o juiz declara a incompetência do Juizado Especial Cível (JEC) e, com base no artigo 51, inciso II, da Lei nº 9.099/1995, extingue o processo sem resolução de mérito. O dispositivo legal em questão estabelece que o processo será extinto "quando inadmissível o procedimento instituído por esta Lei ou seu prosseguimento, após a conciliação" (Brasil, 1995). O consumidor, que buscou o Juizado justamente pela promessa de rapidez e gratuidade, vê-se obrigado a reiniciar a batalha na Justiça Comum, onde o rito é mais lento e oneroso. Isso cria, na realidade, uma barreira de acesso à justiça (Soares; Carvalho, 2023).

Diante desse impasse processual, a inversão do ônus da prova (artigo 6º, VIII, do CDC) surge como um escudo vital. A lei permite que o juiz inverta o ônus da prova, reconhecendo a

hipossuficiência técnica do consumidor, que não possui meios de auditar os servidores da instituição bancária. Cabe à instituição financeira provar que seu sistema é infalível e que a transação foi legítima (Brasil, 1990). Essa ferramenta é central para tentar reequilibrar uma luta que, tecnicamente, é desigual.

Mas a corrida tecnológica não é unilateral. Enquanto o crime evolui, a arquitetura de segurança também avança. Duas tecnologias despontam como promessas para blindar o futuro dos contratos: o *blockchain* e os contratos inteligentes (*smart contracts*) (Ferraz, 2019).

O *blockchain* funciona como um livro-razão digital com estrutura fundamentada. Ele registra transações de forma descentralizada e permanente. A lógica é de encadeamento, logo cada novo bloco de informação contém uma impressão digital criptográfica do anterior, criando uma corrente (*chain*) inquebrável (Braga, 2019). Como esses registros estão espalhados por milhares de máquinas e não em um servidor central, rastrear o histórico é uma tarefa muito difícil. Por isso, governos e empresas já vislumbram nessa tecnologia a base para uma nova identidade digital (Ferraz, 2019).

Dessa inovação nascem os *smart contracts*. Imagine um contrato que não precisa de um juiz ou de um banco para ser cumprido, pois ele se autoexecuta. Segundo Bashir (2017), são códigos de computador que traduzem cláusulas contratuais para a linguagem de programação. Uma vez inserido no *blockchain*, o contrato aguarda o gatilho (uma condição pactuada, como a confirmação de uma entrega). Aconteceu o gatilho? O contrato executa a consequência (libera o pagamento) instantaneamente, sem intermediários e de forma irreversível (Ferraz, 2019).

Um empréstimo regido por *smart contract* teria cada centavo rastreado e cada cláusula executada automaticamente, reduzindo drasticamente o espaço para fraudes ou inadimplência (Ferraz, 2019).

No entanto, não podemos ser ingênuos. A implementação massiva esbarra em afrontas humanas e técnicas. Falta mão de obra híbrida (profissionais que conheçam de Direito e Computação), falta regulamentação e, o mais difícil, se diz respeito, como traduzir conceitos subjetivos como boa-fé ou caso fortuito para um código binário e frio? (Ferraz, 2019). Apesar disso, a bússola aponta para essa direção, exigindo que o Direito se prepare para uma nova era contratual.

Em suma, as fraudes eletrônicas representam um dos testes de estresse mais severos para o Direito contemporâneo. Temos um arcabouço jurídico sólido no Brasil, alicerçado no Código Civil e no CDC, mas a aplicação formal ainda patina em incertezas.

A responsabilidade objetiva dos bancos (Súmula 479 do STJ) é o grande pilar de defesa do consumidor (Brasil, 2012), baseada na lógica de que quem lucra com o digital deve assumir

seus riscos. No entanto, a crescente sofisticação da subversão do consentimento, ao manipular a vítima para que esta forneça seus próprios dados, torna o nexo causal mais indefinido, gerando debates intermináveis sobre culpa exclusiva ou concorrente. A ausência de uniformidade nas decisões judiciais apenas intensifica a insegurança jurídica.

Nessa situação de desigualdade, a figura do consumidor, sobretudo a do hipervulnerável, exige uma atuação do Poder Judiciário que não seja apenas de resposta, mas que se antecipe aos problemas (Soares, 2022). Embora a inversão do ônus da prova atue como um contrapeso para equilibrar a relação, ela encontra um obstáculo severo, no qual é a barreira da perícia técnica complexa nos Juizados Especiais Cíveis (JECs). Essa limitação estrutural acaba, paradoxalmente, desamparando justamente quem mais precisa da tutela jurisdicional célere, criando uma zona de exclusão onde a fraude complexa muitas vezes prevalece pela dificuldade de auditagem (Soares; Carvalho, 2023).

A concepção de um ecossistema mais íntegro se fundamenta em dois pilares, projetando a esperança no futuro, como a massificação da educação digital e a maturação de tecnologias de registro imutável, o que é o blockchain. Entretanto, enquanto esse futuro automatizado e blindado não se concretiza, recai sobre os operadores do Direito uma missão quase artesanal, a de calibrar, caso a caso, a responsabilidade objetiva das empresas frente ao dever de vigilância dos usuários. O objetivo final é assegurar que a inovação tecnológica não degenere em um campo propício para a injustiça, mas permaneça sendo a alavanca propulsora do desenvolvimento social e econômico.

3. PROPOSTAS E DESAFIOS NA EFETIVAÇÃO DA SEGURANÇA E VALIDADE JURÍDICA DOS CONTRATOS ELETRÔNICOS NO BRASIL

A dinâmica contratual contemporânea atravessou uma compressão física e temporal severa. O ato de contratar tornou-se, literalmente, algo portátil e instantâneo, basta apenas tirar o celular do bolso. Impulsionado pela onipresença dos smartphones, o ambiente de negociação abandonou a solenidade das salas de reunião tradicionais para ocupar a volatilidade dos aplicativos de mensagem instantânea, como o WhatsApp. É nesse ecossistema fluido que propostas são lançadas, as cláusulas são debatidas e a concordância é formalizada, muitas vezes intercalado entre um emoji e outro (Ramos, 2023).

O Judiciário, por sua vez, não poderia fechar os olhos para essa realidade fática. Alicerçados no princípio da liberdade das formas, os tribunais vêm validando essas interações, desde que a substância do acordo seja inequívoca. O Superior Tribunal de Justiça (STJ), ao analisar a validade de atos solenes como a citação processual, estabeleceu um norte interpretativo que deve guiar o Direito Privado. O que prevalece é a ciência inequívoca da parte (Brasil, 2023). Ao aplicar essa inteligência ao contexto contratual, a validade de um negócio realizado por meio de aplicativo transcende a mera formalidade. O cerne da questão passa a ser a capacidade probatória, ou seja, o estímulo de estabelecer, de forma inequívoca, a autoria da mensagem e o conteúdo exato do acordo estabelecido.

Contudo, é preciso cautela, visto que nem todo "clique" possui o mesmo valor jurídico, no vasto universo do comércio eletrônico. Tanto a doutrina quanto o empreendimento de mercado consolidaram a distinção entre duas modalidades de aceite, cujas forças probantes são drasticamente diferentes.

A primeira, considerada bem sólida, é o *Click-wrap*, nela, o usuário precisa realizar um movimento ativo e inequívoco, marcar uma caixa de seleção (*checkbox*) e clicar em um botão com texto explícito, como "Eu Aceito". Há aqui uma manifestação de vontade expressa, da mesma forma que um contrato de adesão (Docusign, 2022). O consenso jurisprudencial é de que esses pactos são válidos, pressupondo que os termos estavam visíveis e legíveis (Brasil, 2023).

O problema real habita no *Browse-wrap*. Imagine aqueles termos de uso escondidos em um *hyperlink* discreto no rodapé da página. O usuário navega pelo serviço sem jamais declarar ativamente seu aceite. A doutrina olha para essa modalidade com extrema reserva, pois o consentimento é, na melhor das hipóteses, tácito. Provar que o consumidor sequer teve ciência das cláusulas torna-se uma tarefa extremamente penosa, fragilizando a segurança jurídica do

negócio.

A facilidade de contratação, especialmente por meio de métodos vulneráveis como o *browse-wrap* ou assinaturas simples, tem sido um fator que abriu caminho para uma crescente onda de fraudes, notadamente em relações de consumo, como os famigerados empréstimos consignados não solicitados.

A consequência foi a inundação do Judiciário com ações declaratórias de inexistência de débito. Isso forçou o STJ a se posicionar de forma contundente no Tema Repetitivo 1061 (análise do REsp 1.846.649) (Superior Tribunal de Justiça, 2022). Embora a origem da discussão fosse a assinatura física de analfabetos, a ratio decidendi é perfeitamente transponível para o digital.

A decisão firmou-se como um divisor de águas ao realocar o risco do negócio. O STJ (Superior Tribunal de Justiça, 2022) foi taxativo em afirmar que o ônus da prova acerca da autenticidade da assinatura recai sobre a instituição financeira. A lógica é econômica e processual. Caso o banco opte por um método de contratação de baixa segurança para ganhar agilidade, ele assume integralmente o risco de não conseguir provar a validade desse ato em juízo.

A atual inundação do Judiciário com ações declaratórias de inexistência de débito é o sintoma direto de um mercado infestado por contratações eletrônicas fraudulentas, especialmente em empréstimos bancários. A massificação dessas fraudes, que gera uma pulverização de demandas individuais, contribui decisivamente para o engessamento da máquina judiciária. Nessa circunstância caótica, o posicionamento contundente do STJ no julgamento do Tema Repetitivo 1.061 (REsp 1.846.649), ocorrido em novembro de 2021, foi para estabelecer uma baliza processual segura.

Ao fixar a tese, a Corte estabeleceu uma norma sobre a dinâmica da prova em disputas bancárias. Sempre que o consumidor impugnar a autenticidade da assinatura em um contrato apresentado pela instituição financeira, recai sobre o banco o ônus de provar que aquela firma é legítima, por analogia, esse entendimento confirma que também cabe ao banco provar a inviolabilidade de seus sistemas de biometria digital. Essa lógica somente reforça o princípio da responsabilidade objetiva consolidado na Súmula nº 479 do STJ, com base na noção de fortuito interno. Ou seja, como as instituições financeiras lucram com o risco da atividade, elas respondem objetivamente por fraudes cometidas por terceiros (Brasil, 2012).

Para o consumidor, basta demonstrar a fraude na contratação e o prejuízo financeiro. Em contrapartida, para se desincumbir desse pesado ônus probatório, a instituição financeira é frequentemente compelida a demonstrar tecnicamente que suas barreiras de segurança não

foram violadas. É nesse ponto que a prova pericial digital, realizada diretamente sobre o sistema biométrico ou os logs do banco, se impõe como a modalidade mais adequada e eficiente para resolver a controvérsia.

O impacto no mercado foi imediato. Para grandes players (bancos, *fintechs*, varejistas), tornou-se inviável depender de métodos de assinatura meramente "simples" (como um login básico). Para ter segurança nos tribunais, foi necessário adotar mecanismos de prova reforçados.

Aqui entra a distinção central, haja vista a assinatura ICP-Brasil (qualificada) goza de presunção legal de veracidade, já as assinaturas não-ICP-Brasil (avançadas) dependem de uma trilha de auditoria, que é uma construção probatória. (*audit trail*) (Alohi, 2024). Plataformas de assinatura eletrônica de renome (como *Docusign* e *Clicksign*) (Clicksign, 2024) sustentam sua validade jurídica não em um certificado público, mas na firmeza dessa trilha. Ela atua como o equivalente digital das testemunhas e do reconhecimento de firma.

Para que uma trilha de auditoria seja considerada eficaz e robusta o suficiente para prevalecer em uma disputa judicial (Supersign, 2025; Certisign, 2024), ela deve constituir um efetivo dossiê rico em dados, superando a fragilidade de registros habituais. A construção dessa prova inicia-se pela identificação inequívoca do signatário, validada por múltiplos fatores como e-mail, tokens via SMS ou cruzamento de CPF, e aprofunda-se com a captura dos metadados da transação, registrando o endereço de IP, o dispositivo utilizado e, mediante consentimento, a geolocalização.

O pilar técnico dessa segurança é a garantia de integridade fornecida pelo *Hash*, um código criptográfico (geralmente SHA-256) gerado matematicamente a partir do documento original. Sua função é assegurar a imutabilidade, assim qualquer alteração mínima no arquivo, por menor que seja, modifica o *hash* final, denunciando instantaneamente a adulteração. A essa estrutura soma-se a garantia temporal (*Timestamp*), que atesta o momento exato da assinatura, e, para contratos de alto risco, a autenticação reforçada, que insere camadas como a biometria facial com liveness check para validar a identidade em tempo real. A conclusão lógica é direta, visto que a força probante de um contrato firmado fora da ICP-Brasil é diretamente proporcional à riqueza e à solidez técnica de sua trilha de auditoria.

Com o mercado massificando o uso dessas assinaturas avançadas e a antiga Medida Provisória 2.200-2 (Brasil, 2001) gerando dúvidas interpretativas, cabia ao STJ harmonizar o olhar. E a Corte o fez de maneira decisiva.

Em julgados recentes e de grande repercussão, como o REsp 2.159.442/PR, o Tribunal pacificou o entendimento de que a ICP-Brasil não detém o monopólio da validade. A ausência do certificado público, por si só, não anula o contrato eletrônico (Brasil, 2001; Brasil, 2024).

O argumento central do STJ (Superior Tribunal de Justiça, 2024) baseou-se em uma interpretação finalística do artigo 10º, § 2º, da MP 2.200-2 (Brasil, 2001).

> Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.
> § 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

A Corte entendeu que, ao empregarem uma plataforma privada específica, como a Clicksign, mencionada explicitamente no julgado (Superior Tribunal de Justiça, 2024) e cumprirem seus ritos de verificação (como a inserção de tokens), as partes admitiram aquele meio como válido.

Essa jurisprudência recente não surgiu do nada; ela veio ao encontro do que a doutrina já preconizava, encontrando respaldo no Enunciado 297 da IV Jornada de Direito Civil (CJF, 2008). Estamos, de fato, diante de uma mudança radical de paradigma na teoria da prova digital, onde o STJ (Superior Tribunal de Justiça, 2024) e a doutrina (CJF, 2008) alteraram o eixo de rotação do sistema.

A Trilha de Auditoria (Audit Trail) representa a segura cadeia de custódia da prova digital (que inclui IP, geolocalização, ID do dispositivo, hash do documento e timestamp). Ela se estabelece como um novo e primordial requisito para a validade jurídica, indo além da comum certificação.

O movimento marca a transição de um paradigma antigo, onde a confiança era um atributo derivado exclusivamente da tecnologia oficial (ICP-Brasil) e a prova era presumida, para um novo paradigma, no qual a confiança deriva da robustez da prova técnica de autoria e integridade. Nesse novo enquadramento, a tecnologia deixa de ser o fim para se tornar apenas o meio capaz de gerar essa distinção (Brasil, 2024). O recado do Judiciário ao mercado foi cristalino. O uso do selo ICP-Brasil tornou-se facultativo, mas impôs uma condição severa, assim quem optar por não utilizá-lo deve apresentar uma trilha de auditoria tão sólida que não deixe margem para dúvidas razoáveis sobre a autoria e a integridade do documento.

A decisão do STJ não se limitou a resolver casos isolados; na realidade, ela pavimentou a estrada para a edição da Lei nº 14.063/2020 (Brasil, 2020). Embora essa legislação tenha nascido com o foco primário na desburocratização do setor público, seu impacto no mercado privado foi monumental, pois finalmente conferiu nomenclatura legal e definiu a segurança semântica dos três níveis de assinatura que o mercado já consumava empiricamente.

Na base dessa pirâmide normativa encontra-se a “Assinatura Eletrônica Simples”,

caracterizada pela identificação via dados rudimentares, como conferência de login, e-mail ou mero aceite em formulário web; uma modalidade funcional, porém de baixa resistência probatória (Brasil, 2020; Certisign, 2024). Ascendendo na escala de segurança, surge a "Assinatura Eletrônica Avançada", a exata protagonista do mercado atual. Ela assegura a autenticidade através de mecanismos de vinculação inequívoca, como biometria, *tokens* via SMS ou autenticação em dois fatores, eliminando assim a necessidade da estrutura burocrática da ICP-Brasil. Neste contexto, a trilha de auditoria desempenha um papel crítico, funcionando como o fiel da balança (Brasil, 2020; Brasil, 2024). Por fim, no topo da hierarquia, permanece a "Assinatura Eletrônica Qualificada", aquela que utiliza o certificado digital ICP-Brasil e mantém a presunção legal de veracidade, reservada para atos de altíssima criticidade (Brasil, 2001; Brasil, 2020).

Ao legitimar a assinatura avançada, a Lei 14.063 (Brasil, 2020) ratificou o entendimento do STJ (Brasil, 2024) e o Enunciado 297 (CJF, 2008). Por via legislativa, confirmou-se que existe muita validade jurídica fora dos muros da ICP-Brasil.

Nesse ecossistema, a Lei Geral de Proteção de Dados (LGPD, Lei 13.709/2018) entra em cena não para discutir a validade do contrato, mas para balizar a produção da sua prova (Brasil, 2018). Surge aqui uma tensão aparente, assim, para construir uma trilha de auditoria (assinatura avançada), as plataformas precisam coletar um arsenal de dados, muitas vezes sensíveis, como IP, geolocalização e biometria facial (Certisign, 2024; Supersign, 2025). Por outro lado, a LGPD impõe o princípio da minimização.

Como harmonizar segurança máxima com coleta mínima? A resposta encontra-se na escolha correta da base legal (Brasil, 2018). Fundamentar essa coleta no consentimento é um erro estratégico, pois o consentimento é revogável e instável. A base sólida para a trilha de auditoria é, primariamente, a execução do contrato (Art. 7º, V), visto que a prova é condição de existência segura do pacto. Para dados sensíveis como a biometria, a base é a garantia da prevenção à fraude e à segurança do titular (Art. 11, II, 'g').

Em última análise, a LGPD (Brasil, 2018) não é um obstáculo, mas um filtro de compliance. O usuário deve ser informado de que sua biometria está sendo capturada não para marketing, mas como um seguro da sua própria vontade, blindando-o contra fraudes.

A *blockchain* e os *smart contracts* representam a próxima fronteira para a efetividade contratual (Dykstra; Moraes; Moraes, 2023). Em sua composição técnica, um contrato inteligente nada mais é do que um código de software autoexecutável rodando sobre uma rede descentralizada (Dykstra; Moraes; Moraes, 2023).

O *Blockchain* não deve ser visto como uma substituição à ICP-Brasil, mas como um

complemento de prova irrefutável. Ele resolve o problema da prova do consentimento ao criar um registro distribuído e imutável que, diferentemente do certificado digital centralizado, não depende de uma única Autoridade Certificadora para sua fé pública.

O *Blockchain* não é meramente uma tecnologia isolada, mas é uma solução definitiva para garantir a imutabilidade central. Em contraste com a ICP-Brasil, que opera como um sistema de confiança centralizado, o *Blockchain* oferece um paradigma distribuído. Essa distinção é fundamental, pois a segurança futura exige a adoção de tecnologias de prova irrefutável.

Sob a ótica da validade, eles encontram amparo perfeito no Artigo 107 do Código Civil (Brasil, 2002; Dykstra; Moraes; Moraes, 2023). A tecnologia entrega garantias de imutabilidade e carimbo de tempo que superam a maioria dos sistemas cartorários do mundo.

A automação, contudo, gera instigações jurídicas sem precedentes. A lógica do *code is law* (o código é a lei) colide frontalmente com a flexibilidade humanista do Direito brasileiro. Como aplicar a Teoria da Imprevisão ou revisar um contrato por onerosidade excessiva se o código foi programado para ser imparável? E se o vício de consentimento (erro ou dolo) estiver escondido na sintaxe da programação, invisível ao leigo?

Essa ocasião ainda é uma zona cinzenta. Iniciativas como o DREX (o Real Digital) do Banco Central surgem justamente para tentar domar essa tecnologia, trazendo os *smart contracts* para dentro de um ambiente regulado e supervisionado.

A caminhada rumo à concretização da segurança jurídica nos contratos eletrônicos no Brasil é uma narrativa envolvente com uma perspectiva concreta. O mercado e o Judiciário precisaram contornar uma legislação inicial (MP 2.200-2/2001) que, embora bem-intencionada, criou um padrão-ouro (ICP-Brasil) caro e pouco usável, deixando a massa das transações em um limbo jurídico.

O desfecho para a questão da força vinculante não se deu de maneira pontual, mas o resultado de uma convergência estrutural entre três frentes que operaram em sintonia.

No campo da Tecnologia, a mudança foi de paradigma probatório. A criação da trilha de auditoria (audit trail) (Alohi, 2024; Supersign, 2025) possibilitou a captura e fixação em um dossiê forense de elementos anteriormente dispersos e efêmeros, tais como o endereço de IP, a geolocalização, o hash criptográfico e a biometria. A tecnologia transformou metadados em uma prova técnica irrefutável (Certisign, 2024), conferindo ao contrato digital uma firmeza que muitas vezes supera a do próprio papel, sujeito a rasuras e extravios.

Essa evolução técnica forneceu o substrato necessário para a Jurisprudência agir. O Superior Tribunal de Justiça (Brasil, 2024), respaldado pela visão inovadora da doutrina (CJF,

2008), teve a coragem institucional de quebrar o monopólio da ICP-Brasil. Ao reconhecer a validade das assinaturas fora do padrão oficial, a Corte desvencilhou o mercado de uma rigidez burocrática, validando a substância da prova técnica em detrimento da forma solene. Foi o reconhecimento judicial de que a segurança não nasce de um carimbo estatal, mas da inalterabilidade dos dados.

Por fim, esse novo ecossistema foi estabilizado pela Legislação. A Lei 14.063/2020 (Brasil, 2020) não apenas organizou as categorias de assinatura, a aplicação do princípio da proporcionalidade foi fundamental, pois se baseou no entendimento de que riscos distintos demandam níveis de segurança adequados e diferenciados. Paralelamente, a LGPD (Brasil, 2018) assumiu um papel ético fundamental. Ao estabelecer normas bem definidas para o tratamento de dados, a lei garantiu que a coleta de provas (como a biometria facial) não se tornasse uma invasão de privacidade, mas sim um procedimento de segurança legítimo e transparente.

Hoje, é possível afirmar com segurança que o sistema jurídico brasileiro realizou uma transição discreta, mas profunda, por isso a certificação está mudando de um modelo focado na burocracia de quem emitiu para um modelo baseado em validação, que se concentra na solidez técnica do que foi realizado. O contexto contemporâneo, portanto, deixou de ser uma barreira tecnológica. Já dispomos de um arsenal probatório sofisticado e eficaz, capaz de rastrear a vontade humana no ambiente digital com precisão cirúrgica.

A fronteira do problema deslocou-se agora para o campo ético e social. O real teste de estresse do sistema não é mais provar que o contrato existe, mas garantir que essa tecnologia de prova respeite a privacidade do cidadão, operando em sintonia fina com a LGPD (Brasil, 2018) para não transformar vigilância em validação. É urgente evitar que a eficiência digital erga um novo muro de exclusão, onde a legitimidade plena se torne um privilégio de quem domina as ferramentas, deixando à margem os analfabetos digitais.

CONSIDERAÇÕES FINAIS

A missão central deste trabalho foi enfrentar o dilema da confiança digital, dessa forma, analisar como o ordenamento jurídico brasileiro garante a segurança e a validade dos contratos eletrônicos em um ambiente notoriamente hostil, marcado por fraudes e manipulações.

Ao longo deste percurso, conhecemos a evolução do Direito Contratual, partindo das bases clássicas do Código Civil até a moderna arquitetura da ICP-Brasil e as recentes decisões do STJ. O objetivo geral de analisar os mecanismos de segurança e validade no contexto digital foi completamente atingido, permitindo-nos concluir que o Direito brasileiro demonstrou uma notável capacidade de adaptação frente à velocidade vertiginosa da tecnologia.

Conduzida pelo fio condutor dos objetivos específicos traçados inicialmente, esta investigação permitiu desenhar um panorama lúcido e detalhado da realidade nacional. O estudo não apenas mapeou o terreno, mas dissecou as estruturas do nosso sistema, evidenciando com nitidez a coexistência de suas robustas fortalezas legislativas e suas persistentes fragilidades.

No tocante à legislação, confirmou-se que o Brasil possui um arcabouço normativo consistente. A Medida Provisória nº 2.200-2/2001 foi, sem dúvida, o divisor de águas, ao equiparar a assinatura digital à física. Contudo, a pesquisa demonstrou que a validade jurídica não depende de uma tecnologia exclusiva. O Código Civil, com seus princípios de liberdade das formas e boa-fé, provou-se perfeitamente aplicável ao digital. Somado ao Marco Civil da Internet e à LGPD, formou-se um ecossistema onde a validade do contrato não está mais no papel ou apenas no certificado ICP-Brasil, mas na capacidade técnica de se provar a autoria e a integridade do documento por qualquer meio idôneo.

Quanto às ameaças, o estudo revelou uma mudança de paradigma nas fraudes. O risco deixou de ser apenas a quebra da criptografia para se tornar a quebra da confiança humana. A exploração da vulnerabilidade, particularmente de grupos hipervulneráveis como os idosos, estabeleceu-se como o principal meio de ataques, exemplificado por fraudes como o golpe do falso motoboy. É alarmante saber que a sofisticação do cibercrime supera a capacidade de reação do consumidor médio. O perigo, portanto, não é o contrato ser nulo a priori, mas nascer viciado por um consentimento manipulado, gerando batalhas judiciais complexas.

Na busca por soluções, a investigação apontou que o caminho para a segurança não é legislativo, mas técnico e cultural. Ficou evidente que métodos de autenticação simplórios (apenas login e senha) são obsoletos para transações de valor. A resposta do mercado e do Judiciário converge para a trilha de auditoria, o uso de biometria, geolocalização, *timestamp* e

blockchain para criar um dossiê probatório irrefutável. A jurisprudência do STJ foi decisiva ao transferir o ônus da prova para as instituições financeiras, forçando o mercado a investir em segurança não por altruísmo, mas para evitar prejuízos judiciais.

A relevância deste estudo consiste, portanto, em proporcionar um referencial para a compreensão desse contexto. Ao costurar a evolução legislativa com a prática dos tribunais, o estudo indica que a validade jurídica dos contratos eletrônicos deixou de se basear em um modelo de forma legalmente prescrita, passando a adotar um modelo focado na cadeia de custódia da prova. Para o mercado, fica o aviso de que a segurança jurídica está na capacidade de construir um acervo técnico indestrutível sobre a manifestação de vontade do cliente.

Reconhecem-se, contudo, as limitações desta pesquisa. A análise concentrou-se na macrovisão dos Tribunais Superiores, deixando de lado dados quantitativos sobre a realidade dos Juizados Especiais de primeira instância, onde a batalha cotidiana contra as fraudes acontece e onde a perícia técnica muitas vezes é inviável. Da mesma forma, temas de fronteira como os *Smart Contracts* foram abordados como tendência, sem aprofundar o choque teórico que o código autoexecutável provoca na dogmática contratual tradicional.

Essas limitações oferecem oportunidades promissoras para investigações futuras. Sugere-se aos próximos pesquisadores uma investigação dedicada à regulamentação dos *Smart Contracts* no Brasil, testando se princípios como a função social sobrevivem à rigidez do *blockchain*. Outra linha necessária é a análise da eficácia (ou ineficácia) dos Juizados Especiais Cíveis frente às fraudes bancárias complexas, verificando se a simplicidade processual não está, por hábito, cerceando a defesa do consumidor.

A evolução do Direito Contratual exige a migração de um modelo baseado em quem assina (ICP-Brasil) para um modelo baseado em como a transação foi registrada (cadeia de custódia e Blockchain).

Em última análise, o contrato eletrônico consolida-se como o fiel reflexo da sociedade conectada, em virtude de ser uma estrutura veloz, globalizada e de complexidade crescente. A lição primordial extraída deste estudo está na compreensão de que a segurança jurídica superou a antiga dicotomia binária de válido ou inválido; hoje, ela opera em uma escala de gradação probatória, a força do vínculo é determinada pela solidez da garantia técnica. O ordenamento brasileiro teve o mérito de estabelecer as diretrizes dessa competição a tempo, ancorando a confiança no sistema.

Entretanto, o desafio que persiste e se projeta para o futuro é, justamente, garantir que a forma digital não seja apenas uma capa moderna e ágil, mas funcione como um instrumento apto a proteger a natureza do ato jurídico, que é a livre manifestação de vontade. Por trás da

fria automatização de cada clique de aceite, deve subsistir um consentimento informado, consciente e incontestável. Nessa fronteira sutil, no ponto de tensão entre a aceleração da inovação tecnológica e a necessária proteção humana, que o Direito precisa manter sua vigilância permanente.

O futuro da validade jurídica dos contratos eletrônicos no Brasil habita menos na criação de novas leis e mais na harmonização das fontes jurídicas (a técnica da Lei 14.063/2020 e o Código Civil) e na capacitação técnica do Judiciário. É imperativo que os tribunais saiam da lógica do papel e do carimbo, e adotem um olhar pericial sobre as trilhas digitais de auditoria, reconhecendo-as como a nova forma solene da manifestação de vontade.

REFERÊNCIAS

ALOHI. **O que é uma trilha de auditoria?** [S.l.]: Alohi, 2024. Disponível em: https://help.alohi.com/hc/pt/articles/9995551196444-O-que-%C3%A9-uma-trilha-de-auditoria. Acesso em: 13 nov. 2025.

ANDRADE, Ronaldo Alves de. **Contrato Eletrônico**. São Paulo: Manole, 2004.

AQUINO, Emílio Moreira. Contrato eletrônico: análise de sua validade jurídica no ordenamento jurídico brasileiro sob a égide do Código Civil de 2002. **Contribuciones a Las Ciencias Sociales**, São José dos Pinhais, v. 18, n. 1, p. 01-20, 2025.

CERTISIGN. Assinaturas eletrônicas e digital: o que são e quais os tipos. **Blog Certisign**, [s. d.]. Disponível em: https://blog.certisign.com.br/simples-avancada-e-qualificada-conheca-as-diferencas-entre-os-tipos-de-assinaturas-eletronicas/. Acesso em: 13 nov. 2025.

AZEVEDO, Antônio Junqueira de. **Negócio jurídico**: existência, validade e eficácia. 4. ed. atual. São Paulo: Saraiva, 2008.

BASHIR, Imran. **Mastering Blockchain**. Birmingham: Packt Publishing Ltd, 2017.

BASSO, Maristela. **Contratos internacionais do comércio**: negociação, conclusão, prática. 3. ed. Porto Alegre: Livraria do Advogado, 2002.

BATISTA, Vera. Golpes financeiros contra idosos aumentaram 60% durante a quarentena. **Correio Braziliense**, Brasília, 6 dez. 2020. Economia. Disponível em: https://www.correiobraziliense.com.br/economia/2020/12/4893412-golpes-financieiros-contra-idosos-aumentaram-60--durante-a-quarentena.html. Acesso em: 13 nov. 2025.

BERTINI PASQUOT POLIDO, Fabrício; SÁVIO OLIVEIRA DA SILVA, Lucas. Contratos internacionais eletrônicos e o direito brasileiro: entre a insuficiência normativa doméstica e as soluções globais. **Sequência**: Estudos Jurídicos e Políticos, Florianópolis, v. 38, n. 75, p. 157–188, maio 2017. DOI: 10.5007/2177-7055.2017v38n75p157. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2017v38n75p157. Acesso em: 24 jul. 2025.

BOIAGO JÚNIOR, J. **Contratação eletrônica**: aspectos jurídicos. Curitiba: Juruá, 2005.

BOLZAN, Fabrício. **Direito do consumidor esquematizado**. 2. ed. São Paulo: Saraiva, 2014.

BRAGA, Alexandre Melo. **Tecnologia Blockchain**: fundamentos, tecnologias de segurança e desenvolvimento de software. Campinas: CPQD, 2019. Disponível em: https://www.cpqd.com.br/wp-content/uploads/2017/09/whitepaper_blockchain_fundamentos_tecnologias_de_seguranca_e_desenvolvimento_de_softwar_FINALpdf. Acesso em: 13 nov. 2025.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 maio 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 6 ago. 2025.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 13 nov. 2025.

BRASIL. **Lei n.º 9.099, de 26 de setembro de 1995.** Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Brasília, DF: Presidência da República, [1995]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9099.htm. Acesso em: 20 nov. 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 24 jul. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 18 maio 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 maio 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 maio 2025.

BRASIL. Lei nº 13.874, de 20 de setembro de 2019. Institui a Declaração de Direitos de Liberdade Econômica; estabelece garantias de livre mercado […]. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13874.htm. Acesso em: 24 jul. 2025.

BRASIL. Lei nº 14.063, de 23 de setembro de 2020. Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos […]. Brasília, DF: Presidência da República, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14063.htm. Acesso em: 13 nov. 2025.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil […]. Brasília, DF: Presidência da República, [2001]. Disponível em: http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm. Acesso em: 1 abr. 2025.

BRASIL. Resolução nº 4.283, de 4 de novembro de 2013. Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições financeiras […]. Banco Central do Brasil. Disponível em: https://www.bcb.gov.br/pre/normativos/res/2013/pdf/res_4283_v1_o.pdf. Acesso em: 18 maio 2025.

BRASIL. Superior Tribunal de Justiça (STJ). Recurso Especial nº 1.495.920/DF. Relator: Ministro Paulo de Tarso Sanseverino. Terceira Turma, julgado em 15 de maio de 2018, DJe 7

de junho de 2018. Disponível em: https://www.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1698344&num_registro=201402953009&data=20180607&formato=PDF. Acesso em: 24 jul. 2025.

BRASIL. Superior Tribunal de Justiça (STJ). Recurso Especial nº 1.997.175/SP. Relator: Ministro Luis Felipe Salomão, [S. l.], 15 mar. 2021.

BRASIL. Superior Tribunal de Justiça (STJ). 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. Segunda Seção, julgado em 27/06/2012, DJe 01/08/2012. Disponível em: http://www.coad.com.br/busca/detalhe_16/2409/Sumulas_e_enunciados. Acesso em: 2 out. 2025.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 10. ed. São Paulo: Atlas, 2012.

CERT.BR. **Estatísticas Mantidas pelo CERT.br**. NIC.br – Núcleo de Informação e Coordenação do Ponto BR. [S. l.: s. n.], [s. d.]. Disponível em: https://stats.cert.br/. Acesso em: 18 maio 2025.

CGI.BR. **Pesquisa sobre o uso das TIC no Brasil**. São Paulo: CGI.br, 1995.

CLICKSIGN. STJ reafirma os entendimentos acerca da validade jurídica das assinaturas eletrônicas. **Blog Clicksign**, 29 nov. 2024. Disponível em: https://www.clicksign.com/blog/stj-reafirma-os-entendimentos-acerca-da-validade-juridica-das-assinaturas-eletronicas/. Acesso em: 2 nov. 2025.

COELHO, Fábio Ulhoa. **Curso de Direito Civil**. 8. ed. São Paulo: Saraiva, 2016.

COELHO, Fábio Ulhoa. **Curso de direito comercial**: direito de empresa. 20. ed. São Paulo: Revista dos Tribunais, 2016.

COMISSÃO DAS NAÇÕES UNIDAS PARA O DIREITO COMERCIAL INTERNACIONAL (UNCITRAL). **Model Law on Electronic Commerce**. Nova York: United Nations, 1996. Disponível em: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce. Acesso em: 24 jul. 2025.

CONTRATOS Digitais: Validade Jurídica de Contratos Eletrônicos. **Sotto Maior & Nagel Advogados Associados**, [s. d.]. Disponível em: https://smnadv.com.br/contratos-digitais-validade-juridica-de-contratos-eletronicos. Acesso em: 13 nov. 2025.

CONTRATOS ELETRÔNICOS E A VALIDADE JURÍDICA DAS ASSINATURAS DIGITAIS NO BRASIL. **Revista FT**, [s. d.]. ISSN 1678-0817. Disponível em: https://revistaft.com.br/contratos-eletronicos-e-a-validade-juridica-das-assinaturas-digitais-no-brasil. Acesso em: 13 nov. 2025.

CONTRATOS inteligentes (Smart Contracts): O uso da tecnologia blockchain e a validade jurídica no Brasil. **Editora OAB Digital**, [s. d.]. Disponível em: https://editoraoabdigital.org.br/contratos-inteligentes-smart-contracts-o-uso-da-tecnologiablockchain-e-a-validade-juridica-no-brasil. Acesso em: 13 nov. 2025.

CORRÊA, Daniel Marinho; AMARAL, Ana Cláudia Corrêa Zuin Mattos do. Diálogo das Fontes: análise acerca da (in)aplicabilidade das normas relativas ao plano da validade dos negócios jurídicos aos contratos eletrônicos. **Cadernos do Programa de Pós-Graduação em Direito - PPGDir./UFRGS**, v. 17, n. 1, p. 151-174, 2022.

DINIZ, Maria Helena. **Curso de Direito Civil brasileiro**: teoria das obrigações contratuais e extracontratuais. 19. ed. São Paulo: Saraiva, 2003.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro 1**: Teoria Geral do Direito Civil. 35. ed. São Paulo: Saraiva, 2017.

DINIZ, Maria Helena. **Tratado Teórico e Prático dos Contratos**. São Paulo: Saraiva, 2010.

DOCUSIGN. Saiba como o clique no botão "aceite" pode ter validade jurídica com o Docusign Click. **Blog DocuSign**, [s. d.]. Disponível em: https://www.docusign.com/pt-br/blog/docusign-click-aceite. Acesso em: 2 nov. 2025.

DONEDA, Danilo C. M. **Criptografia no Direito**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo C. M. **Da privacidade à proteção de dados pessoais**: direito, tecnologia e inovação. Ed. rev., atual. e ampl. São Paulo: Thomson Reuters - Revista dos Tribunais, 2021.

DYKSTRA, M. M.; MORAES, M. H.; MORAES, R. M. **Smart Contracts**: Potencialidades e Limites no Direito Brasileiro. [S. l.]: TST, 2023. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/215794/2023_dykstra_mayna_smart_contracts.pdf?sequence=1&isAllowed=y. Acesso em: 13 nov. 2025.

FERRAZ, Robertson Novellino. **As tecnologias envolvendo os contratos inteligentes (Smart Contracts) e alguns dos impactos nos contratos**. 2019. Monografia (Bacharelado em Direito) – Centro de Ciências Jurídicas, Universidade Federal de Pernambuco, Recife, 2019.

FIGUEIRA, Hector Luiz Martins; COUTO, Luciane de França. A (Hiper) vulnerabilidade do consumidor idoso nos contratos eletrônicos: desafios e perspectivas. **Revista Veritas de Difusão Científica**, v. 5, n. 2, p. 1078–1111, 2024. Disponível em: https://revistaveritas.org/index.php/veritas/article/view/138/242. Acesso em: 24 jul. 2025.

FRAUDE. *In*: MICHAELIS Dicionário Brasileiro de Língua Portuguesa. São Paulo: Editora Melhoramentos Ltda., 2020. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/fraude. Acesso em: 13 nov. 2025.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**: contratos. 2. ed. São Paulo: Saraiva Educação, 2019.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GOMES, Orlando. **Contratos**. Rio de Janeiro: Forense, 1997.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**. 12. ed. São Paulo: Saraiva, 2015.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**: contratos e atos unilaterais. 13. ed. São Paulo: Saraiva, 2019. v. 3.

GUELFI, Airton Roberto. **Análise de elementos jurídico-tecnológicos que compõem a assinatura digital certificada digitalmente pela Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil)**. 2007. Dissertação (Mestrado em Direito) - Universidade de São Paulo, São Paulo, 2007.

LISBOA, Letícia Lobato Anicet; SANT'ANNA, Leonardo da Silva. A validade dos contratos eletrônicos empresariais Business-to-business (B2B) sob a ótica econômica. **Revista Jurídica UNICURITIBA**, v. 1, n. 63, p. 69-88, 2021.

LÔBO, Paulo. **Contratos**. 6. ed. São Paulo: Saraiva Educação, 2020.

LUCCA, Newton de. **Aspectos jurídicos da contratação informática e telemática**. São Paulo: Saraiva, 2003.

MAIA, Álvaro Marcos Cordeiro. **Disciplina Jurídica dos Contratos Eletrônicos no Direito Brasileiro**. Recife: Nossa Livraria, 2004.

MEIRA, E. A.; PINTO, O. L. S.; TEIXEIRA, J. P. M. Contratos e assinaturas digitais: validade, confecção e jurisprudência. **Revista FT**, São Paulo, v. 15, n. 3, p. 45-67, 2024. Disponível em: https://revistaft.com.br/contratos-e-assinaturas-digitais-validade-confeccao-e-jurisprudencia/. Acesso em: 21 jul. 2025.

MELO, Gilberto. **Enunciado 297 – CJF**. [S. l.], 22 jan. 2008. Disponível em: https://gilbertomelo.com.br/enunciado-297-cjf/. Acesso em: 2 nov. 2025.

NUNES, Luiz Antônio Rizzato. **Curso de direito do consumidor**. 7. ed. São Paulo: Saraiva, 2012.

PAES, André Berto. Crime de Estelionato – Artigo 171 do Código Penal Brasileiro. **Âmbito Jurídico**, 17 jul. 2019. Disponível em: https://ambitojuridico.com.br/crime-de-estelionato-artigo-171-do-codigo-penal-brasileiro/. Acesso em: 7 maio 2025.

PAIXÃO, Marcelo Barros Falcão. **Contratos eletrônicos de consumo**: os novos paradigmas da teoria contratual e a proteção do consumidor. 2019. Dissertação (Mestrado) – Universidade Federal de Pernambuco, Recife, 2019.

PEDROSA, Leyberson; FERREIRA, Luiz Cláudio. Como era a Internet no Brasil antes da comercialização. **Agência Brasil**, Brasília, DF, 4 maio 2021. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-04/como-era-internet-no-brasil-antes-da-comercializacao. Acesso em: 13 nov. 2025.

PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil**. 3. ed. Rio de Janeiro: Forense, 1975. v. 3.

PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil**. 12. ed. Rio de Janeiro: Forense, 2006.

PINHEIRO, Patrícia Peck. **Direito digital**. 4. ed. São Paulo: Saraiva, 2010.

PINHEIRO, Patricia Peck. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

RAMOS, W. **A validade dos contratos firmados via WhatsApp e os documentos assinados eletronicamente**. Migalhas, 12 set. 2023. De peso. Disponível em: https://www.migalhas.com.br/depeso/394185/a-validade-dos-contratos-firmados-via-whatsapp. Acesso em: 13 nov. 2025.

REALE, Miguel. **A teoria tridimensional do Direito**. 5. ed. São Paulo: Saraiva, 2002.

REBOUÇAS, Rodrigo Fernandes. **Contratos Eletrônicos**: Formação e Validade - Aplicações Práticas. São Paulo: Almedina, 2018.

ROCHA, Renata Vieira. A evolução do Direito Digital e suas implicações legais. **Revista FT**, Ciências Humanas, v. 28, ed. 139, out. 2024. DOI: 10.69849/revistaft/ch10202410281448. Disponível em: https://revistaft.com.br/a-evolucao-do-direito-digital-e-suas-implicacoes-legais/. Acesso em: 19 ago. 2025.

SCHREIBER, Anderson. **Os contratos eletrônicos no direito brasileiro**. [S. l.: s. n.], [s. d.]. Disponível em: http://www.schreiber.adv.br/downloads/artigo-contratos-eletronicos.pdf. Acesso em: 30 mar. 2025.

SILVA, Roberta. **As fraudes bancárias e a responsabilidade civil das instituições financeiras**. 2020. 69 f. Monografia (Bacharel em Direito) - Faculdades Integradas de Bauru, Bauru, 2020.

SOARES, Gabriela Vitória Alves. **Da (in)segurança jurídica dos contratos eletrônicos**. 2022. Artigo Científico (Graduação em Direito) - Pontifícia Universidade Católica de Goiás, Goiânia, 2022.

SOUZA, Ysis Lorenna da Cruz. Os contratos eletrônicos e o ordenamento jurídico brasileiro. **Brasil Escola**, 2013. Disponível em: http://monografias.brasilescola.com/direito/os-contratos-eletronicos-ordenamento-juridico-brasileiro.htm. Acesso em: 13 nov. 2025.

SUPERSIGN. **Validade jurídica da assinatura digital gratuita (análise técnica 2026)**. Blog SuperSign, 11 maio 2025. Disponível em: https://supersign.com.br/blog/assinatura-digital-gratuita-validade-juridica-supersign/. Acesso em: 2 nov. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Citação por aplicativo de mensagem pode ser válida se der ciência inequívoca da ação judicial**. Brasília, DF: STJ, 22 ago. 2023. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/22082023-Citacao-por-aplicativo-de-mensagem-pode-ser-valida-se-der-ciencia-inequivoca-da-acao-judicial.aspx. Acesso em: 2 nov. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Falta de credenciamento da entidade certificadora na ICP-Brasil, por si só, não invalida assinatura eletrônica**. Brasília, DF: STJ, 3 dez. 2024. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/03122024-Falta-de-credenciamento-da-entidade-certificadora-na-ICP-Brasil--por-si-so--nao-invalida-assinatura-eletronica-.aspx. Acesso em: 2 nov. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Instituição financeira é responsável por provar autenticidade de assinatura em contrato questionado pelo cliente**. Brasília, DF: STJ, 4 fev. 2022. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04022022-Instituicao-

financeira-e-responsavel-por-provar-autenticidade-de-assinatura-em-contrato-questionado-pelo-cliente-.aspx. Acesso em: 2 nov. 2025.

TAVARES, Beatriz Cal. A validade dos novos contratos eletrônicos bancários. **Revista Eletrônica da Faculdade de Direito de Franca**, v. 17, n. 2, p. 91-111, dez. 2022.

TJ-SP valida empréstimo feito por meio digital com selfie e biometria. **Migalhas**, 18 jul. 2023. Quentes. Disponível em: https://www.migalhas.com.br/quentes/389933/tj-sp-valida-emprestimo-feito-por-meio-digital-com-selfie-e-biometria. Acesso em: 13 nov. 2025.

TONOLI, Marcus Rogério. **Contratos Eletrônicos e Assinatura Digital Conjunta**. 2013. 117 f. Dissertação (Mestrado em Direito) – Centro Universitário Eurípedes de Marília, Marília, 2013.

VENOSA, Sílvio de Salvo. **Direito Civil**. São Paulo: Atlas, 2003. v. 3.

FACULDADE
ViaSapiens
A IDENTIDADE DO CONHECIMENTO

DECLARAÇÃO DE CORREÇÃO GRAMATICAL

DECLARAÇÃO

Eu, LUCIANA MARA BRAGA AGUIAR, CPF 98202260310, formada em Letras pela Universidade Estadual do Ceará - UECE, sob número de registro 54.908, livro GC61, folha 381, **DECLARO**, para os devidos fins, que realizei a revisão ortográfica e gramatical da MONOGRAFIA intitulada como "**CONTRATOS ELETRÔNICOS: SEGURANÇA E VALIDADE JURÍDICA**" de autoria de "**NATANIEL TOMAZ DA SILVA**".

Por ser a verdade, firmo a presente.

Tianguá, Ceará.

05 de dezembro de 2025.

39528eed-cc22-4127-a1a4-41626a287403

Assinado de forma digital por 39528eed-cc22-4127-a1a4-41626a287403
Dados: 2025.12.05 10:48:07 -03'00'

LUCIANA MARA BRAGA AGUIAR