Volume 4 - Número 7 - janeiro a junho 2025

ISSN 2675-7125

Revista da esmape online

VALIDADE E EFICÁCIA DA ASSINATURA DIGITAL EM CONTRATOS ELETRÔNICOS:

uma análise da manifestação de vontade no ambiente virtual

Haroldo Carneiro Leão Sobrinho

Edição especial em homenagem aos 37 anos da Esmape

Volume 4 - Número 7 - janeiro a junho 2025

ISSN 2675-7125

Revista da esmape online

VALIDADE E EFICÁCIA DA ASSINATURA DIGITAL EM CONTRATOS ELETRÔNICOS:

uma análise da manifestação de vontade no ambiente virtual

Haroldo Carneiro Leão Sobrinho

Edição especial em homenagem aos 37 anos da Esmape

Recife, 2024

Coordenação Técnica e Editorial: Joseane Ramos Duarte Soares
Projeto gráfico: TL Publicidade e Assessoria Ltda / Joseane Ramos Duarte Soares
Revisão: Autor

A Revista da Esmape online divulga assuntos de interesse jurídico pedagógico. Os artigos são de total responsabilidade dos respectivos autores, sendo resguardada pluralidade de pensamento. Os conceitos emitidos não expressam, necessariamente, a opinião do Conselho Editorial.

Sítio: https://www.tjpe.jus.br/web/escolajudicial/revista-da-esmape/edicoes

Revista da Esmape online / Escola Judicial de Pernambuco (Esmape).
Ano I, n. 1, (2022-). – Recife: Esmape, 2022- .

Semestral
ISSN 2675-7125

1. Direito – Periódico. I. Escola Judicial de Pernambuco. II. Esmape

CDD 340.05

Correspondências:

Escola Judicial de Pernambuco (ESMAPE)
Rua Des. Otílio Neiva Coelho, s/n – bairro Ilha Joana Bezerra Recife – PE
Biblioteca Jarbas Maranhão - CEP 50.080-900
E-mail: revista.esmape@tjpe.jus.br

TRIBUNAL DE JUSTIÇA DE PERNAMBUCO
BIÊNIO 2024/2026

PRESIDENTE

Desembargador Ricardo de Oliveira Paes Barreto

1º VICE-PRESIDENTE

Desembargador Fausto de Castro Campos

2º VICE-PRESIDENTE

Desembargador Eduardo Sertório Canto

CORREGEDOR-GERAL DA JUSTIÇA

Desembargador Francisco José dos Anjos Bandeira de Mello

ESCOLA JUDICIAL DE PERNAMBUCO
BIÊNIO 2024/2026

DIRETOR-GERAL

Desembargador Jorge Américo Pereira de Lira

VICE-DIRETORA-GERAL

Desembargadora Daisy Maria de Andrade Costa Pereira

SUPERVISOR

Juiz Sílvio Romero Beltrão

CONSELHO EDITORIAL

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Católica de Pernambuco (UNICAP), em 2024, para obtenção do título de mestre. Linha de Pesquisa: Processo, Hermenêutica e Efetividade dos Direitos. Orientação: Profº Dr. Lúcio Grassi de Gouveia.

Também este trabalho, como uma parte de tudo que sou, dedico à minha guia, àquela que nunca soltou minha mão, Maria Amélia.

AGRADECIMENTOS

Gostaria de expressar minha mais profunda gratidão à Profa. Dra. Erica Babini Lapa do Amaral Machado pelo excelente trabalho desempenhado como coordenadora do curso de pós-graduação da Universidade Católica de Pernambuco. Sua liderança, competência e dedicação não só elevaram o padrão de excelência do programa, mas também criaram um ambiente acadêmico estimulante e inclusivo. A atenção meticulosa da Professora Erica aos detalhes, seu comprometimento em promover um ensino de qualidade e sua capacidade de inspirar alunos e professores refletem verdadeiramente seu profissionalismo e paixão pela educação. Seu trabalho incansável e visão inovadora têm sido fundamentais para o sucesso e o desenvolvimento contínuo do curso, beneficiando a todos nós que fazemos parte desta comunidade acadêmica.

Minha sincera gratidão ao Prof. Dr. João Paulo Fernandes de Souza Allain Teixeira, pelos valiosos ensinamentos e orientações providos na disciplina Lógica do Pensamento Jurídico. Sua dedicação e profundidade de conhecimento não apenas enriqueceram meu aprendizado, mas também ampliaram minha perspectiva sobre o campo jurídico, instigando-me a uma reflexão crítica e aprofundada sobre os diversos temas abordados. Da mesma forma, sou extremamente grato ao Prof. Dr. José Mário Wanderley Gomes Neto, cuja expertise e metodologia de ensino na disciplina de Metodologia se mostraram fundamentais para o meu desenvolvimento acadêmico e profissional. A abordagem rigorosa e ao mesmo tempo acessível do professor José Mário permitiu-me compreender melhor as complexidades da pesquisa jurídica, fornecendo-me as ferramentas necessárias para explorar o direito de maneira mais eficaz e inovadora. A ambos, meu profundo respeito e agradecimento por contribuírem significativamente para minha jornada acadêmica.

Quero expressar minha sincera gratidão ao Prof. Dr. Glauco Salomão Leite, cujos ensinamentos na área da Teoria do Direito Constitucional foram de imenso valor e profundidade. A paixão e o conhecimento que o Professor Glauco transmite em suas aulas enriqueceram significativamente minha compreensão dos princípios constitucionais, inspirando-me a buscar sempre a excelência e a justiça em minha carreira jurídica. Da mesma forma, sou extremamente grato ao Prof. Dr. Raymundo Juliano Rego Feitosa, um profundo conhecedor e excelente professor de Direito Financeiro e Tributário. A clareza com que transmite seus vastos conhecimentos e sua capacidade de tornar acessíveis temas complexos contribuíram significativamente para o meu desenvolvimento acadêmico e profissional. A

ambos os professores, meu mais profundo respeito e apreço por sua dedicação e pelo impacto positivo que tiveram em minha jornada educacional.

Minha profunda gratidão ao Prof. Dr. Alexandre Freire Pimentel pelos valiosos ensinamentos proporcionados na disciplina de Big Data. Sua habilidade em transmitir conhecimentos complexos e inovadores de maneira clara e envolvente não apenas aprofundou meu entendimento sobre o assunto, mas também inspirou uma admiração crescente não só pelo estudo teórico da matéria, mas principalmente pela sua aplicação prática no ambiente de trabalho. As diversas citações de suas obras neste trabalho são o testemunho disso. A paixão e o entusiasmo do Professor Alexandre pelo campo de Big Data são contagiantes e têm sido uma fonte de motivação para mim, incentivando-me a explorar novas possibilidades e a aplicar o conhecimento adquirido de maneira inovadora em minha carreira. Seu compromisso em promover uma aprendizagem significativa e sua capacidade de conectar teoria e prática de maneira eficaz têm sido essenciais para a minha formação e desenvolvimento profissional.

Gostaria de expressar minha sincera gratidão ao Prof. Dr. Fábio Túlio Barroso pelos inestimáveis ensinamentos na disciplina de Direito Jurisdicional Social e Coletivo. A profundidade de seu conhecimento e a paixão com que aborda os temas foram fundamentais para o meu desenvolvimento acadêmico e profissional. Além disso, sou profundamente grato pelo incentivo e orientação durante o processo de elaboração do artigo científico ("Relações de trabalho e o uso da inteligência artificial como controle das atividades: estudo comparado entre o Brasil e a Alemanha"), do qual tive a honra de ser seu coautor. A sua orientação foi essencial para que o nosso trabalho alcançasse o reconhecimento merecido, culminando na aprovação e publicação do artigo. O apoio e a confiança do Professor Fábio em minha capacidade de contribuir para o debate acadêmico foram, sem dúvida, um marco significativo em minha carreira e um grande impulso para o meu crescimento intelectual. Suas orientações não apenas me guiaram durante o processo, mas também instigaram em mim um desejo ainda maior de perseguir a excelência no campo do Direito. Por tudo isso, minha gratidão é imensa.

É com grande estima e gratidão que expresso meus sinceros agradecimentos ao Prof. Dr. Sérgio Torres Teixeira, cujos ensinamentos na Teoria do Processo não só enriqueceram profundamente meu conhecimento jurídico, mas também fortaleceram minha paixão pela área. Sua dedicação exemplar e abordagem pedagógica inspiradora já haviam capturado minha admiração desde os tempos de graduação, estabelecendo uma base sólida para o meu desenvolvimento acadêmico. Além disso, sou extremamente grato pelo incentivo e apoio inestimável na elaboração do artigo científico ("Efetividade das decisões na era digital: legitimidade passiva dos provedores de aplicação no combate à

desinformação"), do qual tive a honra de ser seu coautor. A orientação precisa e motivadora do Professor Sérgio foi crucial para a aprovação e publicação de nosso trabalho, representando um marco significativo em minha carreira e um testemunho do seu compromisso com a excelência e a formação de seus alunos. A confiança depositada em minha capacidade de contribuir para o debate acadêmico e sua orientação incansável foram fundamentais para o sucesso deste empreendimento, inspirando-me a continuar buscando o aprimoramento intelectual e a excelência profissional. Por tudo isso, minha gratidão ao Professor Sérgio é imensa e profundamente sentida.

Quero expressar minha mais profunda gratidão aos Professores Dr. Breno Duarte Ribeiro de Oliveira e Dr. Roberto Campos Gouveia, cujo incentivo e revisão crítica do meu projeto foram indispensáveis para a criação do estímulo necessário ao início do meu trabalho acadêmico. O apoio e a orientação sábia de ambos não apenas contribuíram significativamente para o refinamento das minhas ideias, mas também forneceram a motivação essencial para embarcar com confiança nesta jornada intelectual. A dedicação dos professores em examinar detalhadamente o projeto, oferecendo insights valiosos e direcionamentos precisos, foi um fator chave para o desenvolvimento de um trabalho acadêmico sólido e coerente. Este estímulo inicial desempenhado por eles foi crucial, marcando o começo de um empenho que se mostrou tanto desafiador quanto extremamente gratificante. Sua disposição em compartilhar conhecimento, juntamente com o compromisso em fomentar o desenvolvimento acadêmico de seus alunos, reflete uma genuína paixão pelo ensino e pela pesquisa. Por todo o suporte, confiança e sabedoria compartilhada, minha gratidão a ambos é imensurável.

Minha gratidão ao Prof. Dr. Teodomiro Noronha Cardozo é imensa e vai além das palavras, pela orientação, incentivo e revisões meticulosas tanto do projeto quanto da dissertação, que foram fundamentais para a realização deste trabalho. O Professor Teodomiro não apenas dedicou tempo e esforço para garantir a qualidade e profundidade acadêmica de minha pesquisa, mas também foi uma fonte constante de motivação em minha carreira acadêmica. Seu apoio incansável e fé inabalável em minha capacidade foram essenciais para superar os desafios e obstáculos ao longo deste percurso. A generosidade com que compartilhou seu conhecimento, a precisão de suas revisões e o constante encorajamento são aspectos que destacaram sua contribuição como decisiva para o sucesso deste empreendimento. Sem a sua orientação experta e o constante incentivo, a conclusão deste trabalho não seria possível. Estou profundamente grato por ter tido a honra de contar com sua valiosa orientação e apoio, que me inspiraram a perseguir a excelência e a manter a dedicação inabalável à minha jornada acadêmica.

Estou profundamente grato aos meus colegas do curso de mestrado por terem sido uma parte essencial desta jornada acadêmica. As inúmeras discussões e debates em que participamos juntos foram fundamentais para o enriquecimento do meu aprendizado e desenvolvimento intelectual. A troca de ideias, o compartilhamento de diferentes perspectivas e o incentivo mútuo criaram um ambiente estimulante e colaborativo, que não só desafiou minhas concepções, mas também ampliou significativamente minha compreensão sobre os temas estudados. A solidariedade e o apoio que recebemos uns dos outros nos momentos de desafios e incertezas foram inestimáveis, proporcionando a força necessária para perseverarmos em nossos objetivos acadêmicos. A cada um de vocês, minha sincera gratidão por tornarem esta experiência não apenas educacional, mas também profundamente gratificante e enriquecedora. A camaradagem e o companheirismo que compartilhamos serão sempre lembrados como elementos chave para o sucesso desta etapa de nossas vidas.

Meu profundo agradecimento ao Prof. Dr. Antônio Carlos Ferreira de Souza Júnior. É com imenso respeito que vejo suas excelentes observações sobre segurança jurídica, as quais se destacaram não apenas pela profundidade e relevância, mas também pelo seu aguçado e preciso apreço pelo rigor da pesquisa científica. Sua capacidade de concisão e objetividade na discussão dos temas abordados nos capítulos contribuiu de maneira significativa para enriquecer a pesquisa proposta, evidenciando seu comprometimento inigualável com a excelência acadêmica e o desenvolvimento intelectual de seus interlocutores. Suas contribuições não apenas elevaram o nível da discussão, mas também me proporcionaram insights valiosos que serão fundamentais para o aprimoramento contínuo do meu trabalho.

Minha família, o pilar fundamental da minha vida, merece um agradecimento especial por todo o apoio incondicional durante esta jornada. À minha amada esposa, Marlene, cuja força, cujo vigor intelectual, vontade de aprender e ensinar, amor e compreensão foram a luz que me guiou nos momentos mais desafiadores, minha eterna gratidão. Suas palavras de encorajamento e sua presença serena foram essenciais para manter minha determinação e foco. Às minhas filhas, Maria Regina e Helena, que me enchem de orgulho e servem como constante fonte de inspiração, o meu mais profundo agradecimento. Vocês trazem alegria e significado à minha vida, incentivando-me a ser a melhor versão de mim mesmo, não só como acadêmico, mas também como pai. Cada sacrifício, cada hora de estudo e cada desafio superado foram sustentados pela força e pelo amor que recebo de vocês. Esta conquista é também sua, compartilhada com todo o amor e gratidão que tenho por cada um de vocês. Vocês são minha motivação e meu maior tesouro.

Meu mais profundo e sincero agradecimento é dirigido ao Prof. Dr. Lúcio Grassi de Gouveia, cujo papel como orientador transcendeu o acadêmico, tornando-se um pilar essencial em minha formação. Seu estímulo inabalável para com a academia foi um fator decisivo em minha jornada, enquanto seu exemplar desempenho como magistrado e professor serviram como fontes de inspiração incomparáveis. A paixão e dedicação do Professor Lúcio ao direito processual iluminaram o caminho para minha carreira, tanto acadêmica quanto profissional, fornecendo-me um guia valioso em cada passo. Em momentos de adversidade, especialmente quando enfrentamos a necessidade de alterar o projeto, seu incentivo e confiança foram fundamentais para a continuidade e sucesso de meu trabalho. A confiança pessoal que depositou em mim é motivo de profundo orgulho e gratidão, e suas lições e apoio serão sempre lembrados como elementos decisivos para as conquistas que pude alcançar.

É com profundo respeito e admiração que dedico este agradecimento especial ao Professor Emérito da UFRJ, Dr. Emmanuel Carneiro Leão. A sua recente passagem não marca o fim de seus ensinamentos, que continuam a ecoar em mim e em muitos que tiveram a honra de conhecê-lo. Desde minha mais tenra idade, o Professor Emmanuel esteve presente como uma referência intelectual luminosa e privilegiada, instilando em mim um amor profundo pelo estudo da filosofia, pela aprendizagem de novos idiomas e, mais fundamentalmente, pela arte de pensar.

Cada encontro familiar em sua companhia foi uma lição inesquecível, repleto de diálogos que despertavam em mim a ânsia por mais conhecimento, mais compreensão. A expectativa por esses momentos era sempre imensa, e eles nunca decepcionaram, deixando-me sempre com a sensação enriquecedora de ter aprendido algo valioso e com o desejo fervoroso de continuar aprendendo.

Guardo com imenso carinho cada livro e artigo de sua autoria que consegui reunir ao longo dos anos. Estes textos não são apenas obras para serem admiradas em uma estante, mas sim fontes ricas de sabedoria, que continuam a me oferecer conhecimento e inspiração. O legado do Professor Emmanuel Carneiro Leão permanece vivo em seus escritos e na memória daqueles que tiveram o privilégio de serem tocados por sua mente brilhante e coração generoso. Ele sempre trazia consigo histórias dos antigos, que iluminavam a compreensão dos desafios do conhecimento.

> “De repente Aristóteles notou que um ancião tinha cavado um enorme buraco na areia e, com uma colher de chá, ia buscar água do mar e vinha para encher o buraco. Aproximando-se do velho, quis saber o que pretendia todo aquele esforço. - O ancião respondeu que ia transferir o mar para o buraco. - Aristóteles revoltou-se: você está maluco? Este é um esforço

> de Sísifo num trabalho de Tântalo! Você não está vendo o tamanho do buraco e a imensidão do mar? Será que pode haver alguma proporção entre o volume das águas e as dimensões de uma colher de chá? Antes de calar-se, o velho ainda perguntou: e a sua cabeça será maior que o buraco na areia? E o ser será menos vasto do que a imensidão do mar? E num conceito poderá caber tudo que é o ser de uma colherinha de chá?" (CARNEIRO LEAO, 1997. p. 114)

Tal com um simples buraco na areia da praia, reconhece-se as limitações desta dissertação, onde não comporta, por maior que seja o esforço de Sísifo, o agrupamento de todos os problemas e aspectos relacionados ao tema, trazendo com a colher cada parte desta vasta intercessão. Mas com a mesma esperança de Albert Camus, fazemos a escolha de enfrentar o desafio na busca de um significado. O foco é delinear e se aprofundar em aspectos específicos, escolhidos pela sua relevância e pertinência ao escopo definido, reconhecendo a colaboração de todos, visando proporcionar, assim, uma contribuição, ainda que parcial, para o entendimento e a discussão acadêmica aqui proposta.

PREFÁCIO

Este livro corporifica a exitosa conclusão do Curso de Mestrado, do Programa de Pós-Graduação Stricto Sensu em Direito, da UNICAP (Universidade Católica de Pernambuco), do talentoso jurista Haroldo Carneiro Leão Sobrinho. A obra constitui-se pela íntegra de sua Dissertação, cujo título, a "**Validade e Eficácia da Assinatura Digital em Contratos Eletrônicos: Uma Análise da Manifestação de Vontade no Ambiente Virtual**", já antecipa fielmente a latitude do problema de pesquisa, que entrelaça tecnologia, direito contratual e direito digital.

Adotando uma metodologia de pesquisa preponderantemente qualitativa e dogmática, associada a uma criteriosa revisão de literatura, a qual vem edificada a partir de um alicerce bibliográfico de School e de um arguto estudo da jurisprudência de regência, que servem de argamassa teórica para legitimar suas conclusões, o autor nos apresenta uma obra densa, concretada sob uma perspectiva crítica transdisciplinar, no sentido de Edgar Morin, que perpassa distintas áreas do conhecimento jurídico, como o Direito Constitucional e Contratual, sob o fio condutor das TICs, para desaguar no Direito que resulta desse amálgama, o Direito Digital ou Tecnológico, como prefiro, e, pontuar os problemas derivados da (in)segurança das assinaturas eletrônicas e sua validade e eficácia.

É nessa ambiência que o autor constrói sua compreensão, abrangente e aprofundada, sobre a validade e eficácia das assinaturas eletrônicas em documentos digitais e suas implicações no recortado âmbito dos contratos nas relações de consumo.

Com notável domínio da matéria, após um diagnóstico abrangente, porém preciso, dos desafios e das oportunidades que a era digital apresenta à segurança do direito contratual, Haroldo conduz-nos para uma reflexão sobre um fenômeno sem volta: o da tecnologização das relações negociais.

A obra se estrutura em quatro capítulos, cada qual explorando de forma satisfatoriamente abrangente, diante do corte epistemológico que serve de premissa para a pergunta e resposta de pesquisa, as nuances e complexidades do tema.

Pois bem, o primeiro capítulo, "A Assinatura Eletrônica e Sua Função Jurídica", estabelece as bases para a compreensão do tema e para o arremate, que vem ao final na conclusão, explorando o conceito de segurança jurídica e sua importância fundamental para a estabilidade e previsibilidade das relações contratuais. Aqui, o autor evidencia como a segurança jurídica, longe de ser um obstáculo à inovação trazida pelas TICs, se apresenta como um pilar dúctil,

rectius, adaptável e compossível com a Revolução 4.0, acolhendo as transformações tecnológicas, com o escopo de garantir a justiça e a equidade nas relações contratuais digitais.

Ainda no primeiro capítulo, são apresentados e contextualizados os princípios contratuais clássicos, com destaque para a autonomia da vontade, a vinculação contratual (*pacta sunt servanda*), a boa-fé objetiva e o consentimento livre e esclarecido dos contraentes, e sobre como estes se imbricam e se aplicam ao contexto digital.

Com sutil perspicácia, o autor analisa os desafios específicos da expressão da vontade em ambientes digitais, abordando questões como a autenticidade, a identificação do declarante e a compreensão dos termos contratuais pelos consumidores, especialmente em face do uso de interfaces de usuário e sistemas automatizados. A profundidade da análise sobre a lesão subjetiva, particularmente no que tange à inexperiência ou vulnerabilidade do consumidor no mundo digital, demonstra a sensibilidade do autor para com as assimetrias típicas do tecnopoder que permeiam as relações de consumo no ciberespaço.

O segundo capítulo, epigrafado como a "Regulação dos Documentos Digitais e a Manifestação de Vontade no Ambiente Digital", nos convida a uma imersão no panorama normativo internacional e nacional que regulamenta as assinaturas eletrônicas. O autor ostenta o seu conhecimento da legislação comparada, o que se justifica e se explica pelo domínio dos idiomas inglês e alemão, e, assim, examina as normas do Mercosul, dos Estados Unidos, da Europa e a Lei Modelo da UNCITRAL (United Nations Commission On International Trade Law), isto é, sobre a regulamentação do Comércio Eletrônico, contextualizando, criticamente, nessa seara, a legislação brasileira, em especial a Medida Provisória nº 2.200-2/2001, com enfoque para a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

A análise meticulosa da Lei Modelo da UNCITRAL, com sua abordagem baseada em princípios, manifesta a busca por um equilíbrio entre a segurança jurídica e a flexibilidade necessária para acompanhar a constante evolução tecnológica. A discussão sobre a MP nº 2.200-2/2001 e a ICP-Brasil revela a preocupação do autor com a segurança e a validade jurídica dos documentos eletrônicos no Brasil, destacando a importância da conformidade com os padrões internacionais de segurança digital.

Com elogiável acuidade, ainda examina os desafios da adaptação da teoria geral da vontade ao meio digital, explorando as nuances da manifestação volitiva em ambientes virtuais, a função das assinaturas digitais como meio de expressão da vontade, e a complexa temática dos smart contacts (contratos inteligentes). A análise da manifestação de vontade no ambiente de telemarketing e

os desafios da prova dos vícios de consentimento em ambiente virtual descortina uma inquietação com a proteção do consumidor e a necessidade de se garantir a justiça e a equidade nas relações contratuais digitais.

O terceiro capítulo, designado "A Validade e Eficácia dos Contratos Digitais", concentra a análise dos elementos essenciais para a validade contratual no contexto digital, aprofundando a discussão sobre a equivalência e a fusão funcional entre documentos tradicionais e digitais. Guiado por um rigor técnico típico da verticalidade de um produto de um curso de mestrado acadêmico, Haroldo examina os requisitos da capacidade, objeto, causa, consenso e forma dos negócios jurídicos, demonstrando como estes se aplicam aos contratos digitais, considerando as peculiaridades e os desafios inerentes ao ambiente virtual.

A investigação sobre a jurisprudência acerca da validade das assinaturas digitais em contratos eletrônicos, com a inclusão de casos concretos, revela uma inquietação humanista que objetiva conectar a teoria à prática, oferecendo ao leitor uma visão completa e contextualizada da latitude do tema. A discussão sobre os fatores de eficácia do negócio jurídico, indo além da mera validade formal, ratifica que o livro detém, também, um viés prático-jurídico para com a efetiva irradiação dos efeitos jurídicos pretendidos pelas partes, no contexto digital.

O quarto e último capítulo, "Proteção ao Consumidor na Assinatura dos Contratos Digitais", se debruça sobre a necessidade da proteção consumerista no ambiente digital, explorando os riscos e as salvaguardas existentes nas transações eletrônicas. Enfoca-se aqui a vulnerabilidade do consumidor no ciberespaço, e são examinados os desafios da efetiva proteção de dados pessoais, sobretudo no contexto da Lei nº 13.709/ 2018 (Lei Geral de Proteção de Dados Pessoais (LGPD).

Igualmente, expõe-se o papel das agências reguladoras e órgãos de proteção do consumidor, como a ANEEL, a ANATEL, o Conselho Monetário Nacional e o PROCON, demonstrando-se a importância da 'autorregulação', da 'regulação', da 'regulamentação' e da fiscalização para se garantir a segurança e a justiça nas relações de consumo no ambiente digital. A discussão sobre as políticas de compliance e os aperfeiçoamentos de práticas de mercado, com a inclusão de exemplos de empresas que se destacam na proteção do consumidor, demonstra a importância da responsabilidade corporativa e da ética nos negócios digitais.

Ao cabo do último capítulo são exploradas as novas tecnologias e as perspectivas de ambientação social do consumidor na ágora cibernética, analisando-se o impacto da Internet das Coisas, da inteligência artificial, da criptografia quântica e do blockchain na esfera dos contratos digitais. Aqui o autor foca na necessidade de se promover a inclusão digital do consumidor por meio de sua alfabetização tecnológica, revelando sua preocupação com a

democratização do acesso às novas tecnologias e com a garantia de que todos os indivíduos possam participar de forma plena e consciente na sociedade digital.

Em suma, pode-se arrematar que o presente livro constitui uma valiosa contribuição para o debate acadêmico e profissional sobre a validade e a eficácia das assinaturas digitais em contratos eletrônicos, especialmente nas relações de consumo. A obra, com sua linguagem clara e precisa, de leitura leve e fluída, destina-se não apenas a juristas e acadêmicos, mas a todos aqueles que buscam compreender os desafios e as oportunidades que a era digital apresenta ao direito contratual.

Recife, 30 de julho de 2024.

ALEXANDRE FREIRE PIMENTEL
Professor da Linha de Cidadania Digital do Programa de Pós-Graduação em Direito da Universidade Católica de Pernambuco (PPGD-UNICAP). Professor da Faculdade de Direito do Recife da Universidade Federal de Pernambuco (FDR-UFPE). Desembargador do Tribunal de Justiça do Estado de Pernambuco.

RESUMO

Esta dissertação investiga a validade e eficácia das assinaturas eletrônicas em contratos de consumo digitais, enfatizando a necessidade de segurança jurídica e a equivalência funcional com as assinaturas tradicionais. Revelou que, embora haja um reconhecimento jurídico crescente das assinaturas digitais, ainda existem lacunas significativas na proteção ao consumidor, especialmente em relação à privacidade de dados e acesso à tecnologia. Identificou-se a necessidade de atualizações legislativas para abordar integralmente os desafios da manifestação de vontade e dos vícios de consentimento no ambiente digital. A pesquisa destaca a importância de um marco regulatório adaptativo e atualizado, capaz de enfrentar os desafios trazidos pela evolução tecnológica, oferecendo diretrizes para futuras discussões sobre a interseção entre direito, tecnologia e proteção ao consumidor.

Palavras-chave: Assinaturas eletrônicas. Segurança jurídica. Contratos de consumo digitais. Proteção ao consumidor. Legislação adaptativa.

ABSTRACT

This dissertation investigates the validity and effectiveness of electronic signatures in digital consumer contracts, emphasizing the need for legal security and the functional equivalence with traditional signatures. It revealed that, although there is a growing legal recognition of digital signatures, there still are significant gaps in consumer protection, especially regarding data privacy and access to technology. The need for legislative updates to fully address the challenges of will manifestation and consent defects in the digital environment was identified. The research highlights the importance of an adaptive and updated regulatory framework, capable of facing the challenges brought by technological evolution, offering guidelines for future discussions on the intersection between law, technology, and consumer protection.

Keywords: Electronic signatures. Legal security. Digital Consumer contracts. Consumer protection, Adaptive legislation.

SUMÁRIO

INTRODUÇÃO

Na era digital em que vivemos, as transações eletrônicas se tornaram um meio consolidado, remodelando a maneira como contratos são formulados e assinados. A adoção crescente de assinaturas eletrônicas em contratos de consumo não é apenas uma consequência dessa transformação digital (Pinheiro; Weber; Neto, 2022), mas também um catalisador para novas formas de expressão da vontade jurídica. Este cenário apresenta um desafio jurídico significativo: como as assinaturas eletrônicas, enquanto manifestações de vontade no ambiente digital, são regulamentadas e reconhecidas para garantir a validade e eficácia dos contratos nas relações de consumo? Este problema multifacetado engloba a segurança jurídica proporcionada por essas assinaturas, a adequação das normativas vigentes e as práticas de proteção ao consumidor diante dos riscos do ambiente digital.

A presente dissertação de mestrado se propõe a investigar uma questão de crescente relevância no cenário jurídico e tecnológico contemporâneo: a validade e eficácia das assinaturas eletrônicas em documentos digitais, sobretudo no contexto das relações de consumo, especialmente nos contratos de adesão. Este estudo surge em resposta ao aumento exponencial de transações digitais e à adesão generalizada às assinaturas eletrônicas em contratos de consumo, elementos que moldam significativamente o panorama legal e comercial atual.

O cerne da problemática abordada reside na questão de como as assinaturas eletrônicas, enquanto manifestações de vontade no ambiente digital, são regulamentadas e reconhecidas juridicamente. A relevância deste estudo é amplificada pela necessidade de assegurar a validade e eficácia dos contratos digitais, considerando as peculiaridades e desafios inerentes ao ambiente virtual. Esta análise abrange aspectos de segurança jurídica, adequação das normativas vigentes e as práticas de proteção ao consumidor no contexto digital, que são marcados por riscos e vulnerabilidades específicos.

Para abordar esta temática complexa e multifacetada, foram estabelecidas hipóteses que orientam a investigação: a equivalência jurídica entre assinaturas eletrônicas e tradicionais, a eficácia das normativas atuais na regulação da manifestação de vontade em ambientes digitais, a dependência da validade dos contratos digitais na equivalência funcional com documentos tradicionais, e as lacunas existentes na proteção ao consumidor em transações eletrônicas.

O objetivo geral deste estudo é analisar a validade e eficácia das assinaturas eletrônicas em documentos digitais, com um foco particular na manifestação

de vontade no ambiente virtual, para determinar a validade dos contratos nas relações de consumo. Para alcançar tal objetivo, propõe-se quatro objetivos específicos, incluindo a investigação da regulação jurídica da assinatura eletrônica, a avaliação do panorama normativo nacional e internacional, a análise dos elementos essenciais para a validade contratual no contexto digital, e o exame dos riscos e proteções ao consumidor em transações eletrônicas, como os contratos de consumo por adesão estão sendo formalizados.

A metodologia adotada nesta pesquisa é de natureza qualitativa e dogmática, baseada principalmente na análise de fontes bibliográficas, legislações, normativas e jurisprudência relevantes. Esta abordagem interdisciplinar, que incorpora conhecimentos de áreas como Direito Contratual, Direito Digital, Segurança da Informação e Tecnologia da Informação e Comunicação, permite uma compreensão abrangente e aprofundada sobre a validade e eficácia da assinatura eletrônica em documentos digitais e suas implicações para os contratos nas relações de consumo.

O estudo realizado aqui visa contribuir para a compreensão mais ampla da dinâmica entre direito, tecnologia e consumo na era digital, propondo-se a oferecer uma perspectiva informada e atualizada sobre a temática, além de recomendações práticas e propostas de aperfeiçoamento legislativo e regulatório no contexto das relações de consumo digitais.

As hipóteses que norteiam este estudo abrangem desde a equivalência jurídica das assinaturas eletrônicas em relação às tradicionais até os desafios na regulação da manifestação de vontade no ambiente digital, a validade e eficácia dos contratos digitais e as lacunas na proteção ao consumidor.

A análise crítica das fontes permitiu identificar lacunas, inconsistências e pontos de convergência nos estudos existentes, contribuindo para a formulação de conclusões e recomendações informadas.

Esta pesquisa não apenas busca aprofundar o entendimento sobre a validade e eficácia das assinaturas eletrônicas, mas também visa contribuir para o debate sobre a evolução da legislação e práticas no contexto das relações de consumo digitais, reconhecendo a natureza provisória das hipóteses formuladas e abrindo caminho para futuras investigações no campo do Direito Digital e da proteção ao consumidor.

Este estudo busca explorar as complexidades e nuances envolvendo a validade e eficácia das assinaturas digirais nos contratos de consumo. Isso significa que o desafio aqui apresentado envolve a intercessão do Direito e da Tecnologia da Informação e Comunicação. O Direito possui intercessões com diversos ramos do saber, de modo que a abertura deste ponto de contato forma

um novo oceano de conhecimento, desafiando aqueles que se aventuram em navegar por águas inexploradas.

É um campo vasto e multifacetado dentro do domínio do Direito e da Tecnologia da Informação e Comunicação, sendo pretensiosa qualquer tentativa de exaurir a tarefa exploratória em uma simples dissertação.

1 A ASSINATURA ELETRÔNICA E SUA FUNÇÃO JURÍDICA

1.1 RELAÇÕES JURÍDICAS CONTRATUAIS DIGITAIS. NOVOS DESAFIOS PARA A INTERPRETAÇÃO DAS NORMAS

As relações jurídicas e os negócios jurídicos realizados pelo meio digital constituem uma novidade de recente, mas que não escapam da antiga necessidade humana de confiança naquilo que é definido como obrigatório nas relações interpessoais. Está na cultura humana o desenvolvimento de relações baseadas na confiança, pois é da própria interação a realização propósitos específicos (Rapport; Overing, 2000, p. 195). No contexto jurídico, especialmente nas reações contratuais, a segurança jurídica é um conceito essencial, tendo como núcleo a previsibilidade das relações contratuais, a proteção da confiança e boa-fé, a estabilização da relação através das técnicas jurídicas como a irretroatividade e o ato jurídico perfeito, sem olvidar os aspectos instrumentais de realização do direito, como a facilitação do acesso à justiça substantiva em tempo razoável.

Conforme aponta Ellul (1988), dentre os desafios na sociedade contemporânea, revela-se a importância da previsão, destacando que, ao contrário de períodos anteriores, a necessidade de prever eventos e tendências se tornou constante e abrangente em diversos campos, como no automobilismo, no setor de seguros, nas empresas e no Estado. O autor argumenta que *Tout. Tout le temps. Prévoir en auto. Prévoir assurances et risques*[1], enfatizando a urgência e universalidade da previsão em vários regimes.

O autor observa que as previsões afetam a realidade social, influenciando as ações e reações das pessoas, pelo que menciona o fenômeno da *prophétie auto-réalisatrice*[2] e como as previsões moldam as ações dos agentes econômicos. Aborda a complexidade da previsão na era da inovação técnica, onde agricultores dependem de mercados internacionais e a ordem liberal depende da previsão

1 Tradução livre: Tudo. Todo o tempo. Prever no automóvel. Prever seguros e riscos.

2 Tradução livre: profecia autorrealizável.

para funcionar efetivamente, inobstante a possibilidade de imprecisão e falhas das previsões, destacando como previsões erradas podem ter consequências enormes, especialmente em uma era dominada pela tecnologia. Ellul analisa as metodologias de previsão e suas falhas, mesmo quando se baseiam em dados e parâmetros abundantes. Ele menciona a crítica de Edgar Morin à prospectiva dos anos 1960 e destaca que, mesmo diante da necessidade, as previsões econômicas e técnicas são frequentemente inexatas, levantando questões sobre a imprevisão e a imprevisibilidade[3].

As relações contratuais estão submetidas a esta necessidade de previsibilidade, em que pese os diversos estudos associados à teoria da imprevisão, afetando a segurança jurídica diretamente. O conforto da segurança jurídica nas relações contratuais, nas transações comerciais e consumeristas em especial, favorece um ambiente no qual os sujeitos envolvidos, assim como terceiros afetados, possam antever as consequências de seus atos. As disposições claras, as obrigações assumidas pelos sujeitos, estabilizam as expectativas futuras, de modo que o ordenamento jurídico, tanto nacional quanto estrangeiros, possuem diversas normas que abordam o assunto nas mais diversas situações.

Cabral (2021, p. 30-34) aborda a temática da segurança jurídica, destacando sua relevância e complexidade no contexto jurídico contemporâneo. Salienta que "todos os institutos relacionados à estabilidade dos atos processuais são reconduzidos, pela doutrina tradicional, à necessidade de segurança jurídica", evidenciando a centralidade deste conceito no direito. Ele observa que, não obstante sua importância, a segurança jurídica raramente é explicitada em termos gerais nas legislações, tanto nacionais quanto internacionais, e geralmente é protegida apenas em disposições específicas.

Afirma Cabral que a natureza polissêmica do termo "segurança" gera incertezas sobre seu significado exato. Distingue entre "segurança através do direito" (proteção contra violações à vida e integridade física) e "segurança do

3 Sobre o problema da complexidade, refuta Morin (2005, p. 12-13) uma visão fragmentada do conhecimento, investindo na busca por uma compreensão multidimensional e integrada da realidade. Ressalta que nunca conseguiu separar um objeto de estudo de seu contexto mais amplo, incluindo seu passado e futuro, e sempre se viu atraído por pensamentos que englobam múltiplas dimensões, reconhecendo a existência de verdades profundas e opostas, considerando-as complementares, apesar de suas contradições. Foi apenas no final dos anos 1960, influenciado por campos como a teoria da informação, cibernética, teoria dos sistemas e o conceito de auto-organização, que ele começou a usar o termo complexidade. Esta passou de uma noção de confusão e complicação para uma que unifica ordem, desordem, e organização. Dentro dessa organização, explora Morin a relação entre o uno e o diverso, considerando essas ideias tanto complementares quanto antagonistas. Essas noções interagiram e formaram um "macro-conceito" central em seus pensamentos, abordando o nó górdio das relações entre o empírico, o lógico e o racional.

direito" (referente à cognoscibilidade, aplicabilidade e previsibilidade do direito). Na Constituição Brasileira de 1988, a segurança é mencionada no preâmbulo e em diversos dispositivos, mas foi apenas com a Emenda Constitucional nº 45 de 2004 que a ideia de "segurança jurídica" foi expressamente incorporada ao texto constitucional, além do que, embora haja escassez de previsão expressa da segurança jurídica na legislação ordinária, o Código de Processo Civil de 2015 trouxe avanços significativos nesse aspecto (Cabral, 2021, p. 34). No que diz respeito aos fundamentos normativos da segurança jurídica, a doutrina tem buscado diversas bases, como o princípio da dignidade humana e o Estado de Direito. Indica Cabral que o entendimento majoritário é de que a segurança jurídica deriva da cláusula do Estado de Direito, que exige regras gerais, claras, conhecidas, constantes no tempo e não incoerentes entre si.

Entende Cabral que para compreender a operacionalização da segurança jurídica em institutos específicos como a coisa julgada, é necessário examinar as dimensões da segurança incorporadas contemporaneamente à ideia do *Rechtsstaat*, ressaltando a importância de se adaptar a compreensão da segurança jurídica aos desafios e realidades do mundo jurídico atual.

A segurança jurídica se ergue como um dos pilares centrais do direito, lado a lado com a justiça, em uma simbiose que busca garantir a estabilidade das relações jurídicas e a concretização de um sistema legal justo e eficaz. Sua relevância se intensifica no contexto jurídico contemporâneo, marcado por constantes transformações tecnológicas e sociais.

Oferece a segurança jurídica previsibilidade e estabilidade às relações jurídicas, permitindo que os indivíduos planejem suas vidas e negócios com confiança. Ela se traduz na certeza de que as leis e normas serão aplicadas de forma justa e imparcial, protegendo os direitos e interesses de todos. Sem segurança jurídica, reina a incerteza e a insegurança, fragilizando o Estado de Direito e impedindo o desenvolvimento social e econômico.

Em casos difíceis, a segurança jurídica e a justiça podem colidir, gerando dilemas para o intérprete do direito. A fórmula de Gustav Radbruch oferece uma solução ponderada para tais situações. Radbruch (2006) propõe que, em regra, a segurança jurídica deve prevalecer, mesmo que isso resulte em decisões injustas. No entanto, em casos extremos, quando a injustiça se torna intolerável, a justiça deve ser priorizada, mesmo que isso implique em sacrificar a segurança jurídica.

A relativisação ou flexibilização da segurança jurídica não deve ser banalizada. É preciso cautela para evitar que sua verga excessiva fragilize o sistema legal e gere insegurança jurídica. A relatividade da segurança jurídica deve ser utilizada com parcimônia, em situações excepcionais e devidamente justificadas.

O estudo dos aspectos de validade e eficácia de negócios jurídicos frente às novas tecnologias, como os contratos digitais, busca preservar a segurança jurídica como valor essencial do direito. É fundamental analisar as especificidades das novas tecnologias para garantir a autenticidade das manifestações de vontade dos sujeitos na era digital.

Reconhece-se que a segurança jurídica é um valor fundamental para o direito, mas não absoluto. Em um mundo em constante transformação, é preciso encontrar um equilíbrio entre a segurança jurídica e a justiça, buscando soluções que preservem a estabilidade das relações jurídicas sem comprometer a busca por um sistema legal justo e eficaz. As novas tecnologias trazem novos desafios para a segurança jurídica, mas também oportunidades para aprimorar o sistema legal e garantir a justiça para todos. Neste contexto, o presente estudo tem sua atenção para esta nova realidade da virtualização na formação das relações jurídicas, onde um dos seus elementos essenciais, a manifestação de vontade, assume novas feições.

A proteção da confiança e boa-fé constitui um dos elementos da segurança jurídica, especialmente diante das funções verificadas com a confiança legítima das partes em razão das suas expectativas e o dever de honestidade e lealdade.

Segundo Huber (2008, p. 132-134), ao abordar a confiança (ou lealdade) e boa-fé no contexto da relação obrigacional fundado no Código Civil alemão, são apontadas quatro funções principais do princípio da *Treu und Glauben*[4], evidenciando sua importância e aplicabilidade no sistema jurídico.

1. Função Reguladora (Concretização de Deveres), que consiste em regular modalidades de desempenho estabelecidas, conforme expresso na § 242 do Código Civil Alemão (BGB). Este princípio orienta a forma como uma obrigação deve ser cumprida, complementando disposições legais específicas. Um exemplo citado é a dívida em dinheiro, que no BGB é regulamentada apenas fragmentariamente, e a aplicação do princípio *Treu und Glauben* ajuda a preencher essas lacunas.

2. Função de Suplementação (Fundamentação de Deveres), originária do Direito Romano, é a de fundamentação de deveres. Este uso histórico do princípio servia para estabelecer obrigações em relações contratuais não regulamentadas especificamente pelas leis, preenchendo lacunas legais. Atualmente, além de seu significado textual, o princípio é utilizado para fechar lacunas em

4 Tradução livre: Lealdade e Boa Fé.

acordos contratuais ou complexos de regulamentação legal, especialmente em relação à definição de deveres de proteção.

3. Função de Limitação, frequentemente aplicada na prática, servindo para prevenir o exercício abusivo de direitos, comportamento contraditório e a preclusão. Huber enfatiza que *„jedes subjektive Recht unter dem Vorbehalt der Ausübung nach Treu und Glauben steht"* [5].

4. Função de Correção de Conteúdos Contratuais e Normas Legais, sendo destacado que originalmente, o § 242 do BGB servia para preencher lacunas legais, mas logo foi utilizada para deixar de aplicar a lei existente em nome da justiça. Atualmente, ela é primordialmente utilizada para controlar e corrigir resultados percebidos como injustos, sejam eles baseados em acordos contratuais ou em disposições legais.

Conclui Huber que, não obstante as várias tentativas de fundamentar a segurança jurídica, e sendo majoritário o entendimento de que a cláusula do Estado de Direito é a sede normativa da qual deriva, é necessário examinar quais dimensões da segurança são incorporadas contemporaneamente à ideia do *Rechtsstaat* para compreender como outros institutos específicos, como a coisa julgada, devem refletir e operar esta segurança.

Além da regulação da vigência da lei no tempo, conforme preconizado pelo art. 1º da LINDB – Lei de Introdução às Normas do Direito Brasileiro, cuja disposição forma uma relação entre a vigência e o conhecimento (ficção legal decorrente da publicação) da norma pelos seus destinatários, a segurança jurídica também opera nos atos jurídicos aperfeiçoados segundo as normas vigentes, tal como determina o art. 6º da LINDB c.c. art. 5º, inciso XXXVI da Constituição Federal.

Tartuce (2019, p. 74-84) discute a retroatividade das normas jurídicas e sua relação com o direito adquirido, o ato jurídico perfeito e a coisa julgada, com foco especial na questão da ponderação entre esses elementos e outros valores constitucionais, destacando que, por regra, as normas jurídicas são criadas para ter efeito no futuro, mas podem afetar fatos pretéritos respeitando determinados parâmetros legais e constitucionais. Ele reforça essa ideia ao citar o artigo 5º, inciso XXXVI, da Constituição Federal do Brasil, que prescreve que "a lei não prejudicará o direito adquirido, o ato jurídico perfeito e a coisa julgada".

Segundo o autor, o direito adquirido é descrito como um direito material ou imaterial já incorporado ao patrimônio de uma pessoa, enquanto o ato

5 Tradução livre: cada direito subjetivo está sob a condição de ser exercido de acordo com a Lealdade e Boa Fé.

jurídico perfeito é uma manifestação de vontade lícita, já realizada e aperfeiçoada conforme a lei vigente na época. Por sua vez, a coisa julgada é caracterizada como uma decisão judicial da qual não cabe mais recurso.

Salienta que, em que pese a proteção concedida a esses elementos, há uma tendência no Direito de relativizar princípios e regras, inclusive a coisa julgada, especialmente em casos como ações de investigação de paternidade julgadas improcedentes pela falta de provas, quando não disponível o exame de DNA. Este ponto é evidenciado pelo Enunciado nº 109 do CJF/STJ, que admite a relativização da coisa julgada nesses casos.

Avança o autor para o tema da ponderação, citando a obra de Robert Alexy, que defende esta técnica para os direitos fundamentais. O Novo Código de Processo Civil brasileiro expande esse conceito para incluir a ponderação entre normas e regras. O autor menciona casos concretos onde a coisa julgada é relativizada em nome da justiça, particularmente em questões de paternidade.

Também explora a possibilidade de retroatividade das normas relacionadas à função social da propriedade e dos contratos, conforme previsto no Código Civil de 2002. Este ponto é ilustrado pelo artigo 2.035 do Código, que permite a aplicação de novas normas a contratos já celebrados.

Conclui Tartuce que há uma tendência doutrinária e jurisprudencial de relativizar a proteção do direito adquirido, o ato jurídico perfeito e a coisa julgada, argumentando que isso confere ao sistema jurídico maior flexibilidade e capacidade de adaptação às mudanças sociais. Ele afirma que "a tendência doutrinária e jurisprudencial é justamente relativizar a proteção do direito adquirido, o que torna o sistema jurídico de maior mobilidade, de melhor possibilidade de adaptação às mudanças sociais".

Neste ponto, encontramos valiosa contribuição de Cabral (2021, p. 37-40) quanto ao seu estudo sobre as novas funções estatais em face da segurança jurídica no direito, isso no que diz respeito à adaptabilidade e mutabilidade das funções estatais e dos atos jurídicos.

Inicialmente, o autor destaca que a partir do final do século XX, houve uma mudança significativa no papel e nas funções do Estado, motivada pelo aumento do ritmo das mudanças sociais e pela necessidade de relações mais dinâmicas e flexíveis com os cidadãos e outros países. Este novo contexto exigiu que o Estado se tornasse mais aberto a inovações, levando a uma revisão da cláusula do *Rechtsstaat*. Argumenta que "se o ordenamento jurídico possui não só elementos estáticos, mas também componentes dinâmicos, e, portanto, deve ter espaço para inovações, para alteração de conteúdo dos atos praticados e sua

adaptação, deveriam ser repensados os esquemas e arranjos normativos para garantir segurança e estabilidade".

Além dessa maior abertura à mudança, continua, o Estado assumiu novas funções, passando de um mero sancionador para um indutor de comportamentos, o que implica em uma maior interação com a sociedade e uma abordagem mais proativa e indutiva em suas atividades. Como resultado, a vida diária das pessoas passou a ser mais dependente dos indicadores políticos e econômicos, e suas decisões estão cada vez mais conectadas às funções estatais.

Sustenta Cabral, o Estado do século XXI tem que lidar simultaneamente com o passado, o presente e o futuro, para assegurar a segurança jurídica em todos esses espaços temporais, destacando que, com o aumento da alterabilidade dos atos estatais e sua maior influência na vida individual, é necessário respeitar os atos anteriormente praticados e as programações que os cidadãos realizaram com base nas condutas estatais passadas.

Argumenta Cabral que a segurança jurídica não deve ser uma barreira à mudança. Ele afirma que "a maior alterabilidade dos atos estatais, somada à crescente ingerência e influência do Estado na vida individual, exige o indispensável respeito aos atos anteriormente praticados e às programações que os cidadãos tivessem empreendido com base nas condutas estatais passadas". A proteção tradicional do direito adquirido e da coisa julgada, baseada na ideia de *res finitae* (coisas finalizadas), não se adequa mais a um contexto de constante mutabilidade e necessidade de adaptabilidade.

Assim, conclui que em um ambiente onde a mudança é a regra e o ritmo das alterações aumenta constantemente, não é possível aplicar modelos rígidos de segurança jurídica. Em vez disso, o Estado deve garantir que as mudanças ocorram dentro do direito, e não à margem dele. Isso implica numa reavaliação da abordagem tradicional da segurança jurídica, que deve ser adaptada para refletir a natureza dinâmica da sociedade moderna.

Exemplo atual destas transformações são as alterações das relações jurídicas realizadas em ambiente digital, onde a execução de tarefas por algoritmos, no ambiente do ciberespaço, empreende novos contornos e desafios para o direito, moldando e influindo nos princípios contratuais tradicionais, além de criar notáveis transformações nas estruturas dos contratos.

A presente pesquisa sobre a validade do contrato digital mediante assinatura eletrônica se propõe a discutir a questão em uma nova realidade social marcada pelas novas tecnologias. A pesquisa não se debruça sobre o tema especificamente sobre as interessantes discussões sobre a flexibilização da segurança jurídica, mas busca, ao invocar tais discussões, apenas ilustrar como o

impacto das mudanças sociais deve ser considerado diante do novo fenômeno social decorrente dessa técnica. Procura-se um alicerce que garanta a validade das relações jurídicas por meio da compreensão do fenômeno, favorecendo a própria segurança jurídica.

A pesquisa sobre a validade do contrato digital mediante assinatura eletrônica reconhece a importância da segurança jurídica, mas também reconhece a necessidade de adaptação do sistema jurídico às novas realidades sociais. Além da necessidade de regulamentação específica, a pesquisa discute a ponderação e a reinterpretação das normas existentes podem ser ferramentas úteis para lidar com os desafios da era digital.

1.2 PRINCÍPIOS CONTRATUAIS

Antes de procedermos com a investigação do impacto que as novas tecnologias apresentam nos negócios jurídicos, especialmente na forma contratual, há a necessidade de apresentar a sua essência na forma de princípios reconhecidos pela tradição jurídica. Sua relevância e compreensão são aspectos fundamentais na formação, execução e interpretação dos contratos.

Cabe esclarecer que ao adentrarmos no universo dos contratos digitais, é determinante analisar os princípios que regem a formação e a execução desses instrumentos. Diversos princípios se aplicam a esse contexto, mas neste estudo, focaremos naqueles que se relacionam diretamente com a manifestação de vontade das partes, observando as especificidades do ambiente digital.

Os mais destacados pela doutrina são o princípio da autonomia da vontade, o princípio da vinculação do contrato (*pacta sunt servanda*), o princípio da boa-fé objetiva e o princípio do consentimento livre e esclarecido. Alguns podem compreender que determinado princípio seria um desdobramento de outro princípio, como por exemplo o consentimento livre e esclarecido que seria uma decorrência da autonomia da vontade. Entretanto, ao examinarmos mais a frente, algumas particularidades daquele pode ter uma importância significativa para a relação contratual que mereça um estudo específico.

Em se tratando de princípios clássicos, muitos estudiosos já tiveram a oportunidade de discorrer longos trabalhos sobre cada um destes princípios, cada qual oferecendo uma contribuição sobre sua importância para a relação contratual, especialmente por destacar o aspecto teleológico e o interesse subjacente. Isso favorece a integralização das regras em um sistema jurídico e sua adaptação ao longo do tempo e em diferentes culturas.

Watson (1981, p. 14) apresenta uma análise profunda sobre a natureza e o impacto do Direito Romano nos diversos sistemas legais ao redor do mundo. Destaca a capacidade de adaptação e aplicabilidade do Direito Romano em diferentes contextos sociais, econômicos e políticos. Como merciona, "*its legal rules and institutions can to an extent unequaled by other major legal systems operate in societies of very different types*" [6]. E enfatiza que o Direito Romano não foi apenas adotado em diferentes regiões geográficas, mas também se adaptou a variadas formas de organização social e política. Cita exemplos de como o Direito Romano foi aplicado em sistemas econômicos baseados na escravidão, em sociedades feudais e em países capitalistas, bem como em estados com uma variedade de orientações políticas e religiosas, incluindo ditaduras, monarquias, oligarquias e repúblicas, sejam elas pagãs, católicas, calvinistas ou luteranas. Assim, destaca a "transplantabilidade" do Direito Romano, ou seja, sua capacidade de ser transferido e adaptado a diferentes contextos sem perder sua essência. Isso é evidenciado pelo fato de que, embora o que foi emprestado do Direito Romano possa variar de lugar para lugar, com modificações importantes, a essência do sistema legal romano permanece influente e relevante em diferentes culturas e épocas.

Caio Mário da Silva Pereira (1999, p. 302-306) aborda a complexidade e as nuances dos conceitos de ato jurídico e negócio jurídico. O autor inicia a discussão diferenciando fatos humanos voluntários e involuntários, indicando que os primeiros podem se constituir em atos jurídicos quando alinhados com o direito positivo. A distinção é essencial: "Não são todas as ações humanas que constituem atos jurídicos, porém apenas as que traduzem conformidades com a ordem jurídica".

Pereira diferencia ato jurídico e negócio jurídico. O negócio jurídico, segundo a doutrina moderna, é uma declaração de vontade direcionada para a obtenção de um resultado específico, enquanto o ato jurídico em sentido estrito também implica uma manifestação de vontade, mas os efeitos jurídicos decorrem independentemente da intenção direta do agente. Ele destaca que "os 'negócios jurídicos' são, portanto, declarações de vontade destinadas à produção de efeitos jurídicos queridos pelo agente".

O autor ressalta a contribuição da doutrina alemã na formação do conceito de negócio jurídico, valorizando a vontade que atua em conformidade com a

6 Tradução livre: suas regras e instituições legais podem, em uma extensão incomparável por outros grandes sistemas legais, operar em sociedades de tipos muito diferentes.

ordem legal. Este aspecto é central, pois, como Pereira afirma, "o fundamento e os efeitos do negócio jurídico assentam então na vontade, não uma vontade qualquer, mas aquela que atua em conformidade com os preceitos ditados pela ordem legal".

Pereira analisa a evolução desses conceitos no direito brasileiro, especialmente no contexto do Código Civil de 1916. Ele sugere que o legislador brasileiro conceituou o ato jurídico de maneira abrangente, incluindo tanto os negócios jurídicos quanto outras formas de manifestação de vontade.

A questão da autonomia da vontade é destacada pelo civilista quando afirma que, embora o indivíduo seja livre para criar direitos e obrigações através de sua vontade, esta liberdade está sujeita às restrições da ordem pública. Pereira observa que "por amor à regra da convivência social, este princípio da autonomia da vontade subordina-se às imposições da ordem pública".

A importância da vontade e da lei na constituição do negócio jurídico, concluindo que ambos são componentes essenciais que se complementam. Ele afirma que "o negócio jurídico é uma função da vontade e da lei, que procedem na sua criação, completando-se reciprocamente". Essa interação entre vontade e lei é fundamental para a compreensão da natureza e dos efeitos dos negócios jurídicos no âmbito do direito.

Esta construção dialógica que se apresenta na vontade manifestada livremente permite a criação de direitos e obrigações e tem por fundamento a comunhão de interesses. A existência de um interesse comum que resulta na manifestação livre da vontade de acordo com a lei realiza a formação de um vínculo entre os sujeitos.

Ruggiero (1999, p. 354-346), foca na natureza obrigatória dos contratos e no princípio da obrigatoriedade contratual. Faz uma comparação elucidativa entre contrato e lei, afirmando que "nada pode exprimir melhor a virtude vinculativa da relação contratual do que igualar o contrato a uma lei", destacando a força coativa dos preceitos contratuais, que são específicos para as partes envolvidas.

Tanto o Código Civil brasileiro de 1916, art. 1.079, quanto o Código Civil brasileiro de 2002, art. 421, não falam expressamente na força de lei dos contratos, tal como citado por Ruggiero e ilustrado pelo civilista italiano ao invocar normas do Código Civil italiano.

A doutrina brasileira infere este vínculo diante da consequência do inadimplemento da obrigação em geral, tal como preconizado pelo art. 389 do Código Civil brasileiro de 2002, que dispõe: "Não cumprida a obrigação, responde o devedor por perdas e danos, mais juros e atualização monetária segundo índices oficiais regularmente estabelecidos, e honorários de advogado".

Stolze e Pamplona Filho (2020), abordam o inadimplemento de obrigações, com foco particular no inadimplemento culposo e suas consequências jurídicas. Observam que o desfecho esperado de uma obrigação é seu cumprimento voluntário. No entanto, o foco se desloca para situações em que a obrigação não é cumprida devido à culpa do devedor, o que faz incidir o art. 389 do Código Civil de 2002.

Destacam que essa regra legal está mais alinhada com a realidade econômica atual, ao contrário do Código anterior, elaborado em uma época de economia estável e rudimentar, visto que abordam tanto a questão da perda de valor da moeda em razão da corrosão inflacionária quanto o pagamento dos honorários advocatícios.

Diferenciam entre inadimplemento absoluto e relativo. O inadimplemento absoluto ocorre quando o credor é impedido de receber a prestação devida, total ou parcialmente, por causa da conduta do devedor, como no exemplo dado da destruição de um cereal a ser entregue. Esse tipo de inadimplemento, na falta de tutela jurídica específica, converte-se em obrigação de indenizar. Já o inadimplemento relativo, ou mora, ocorre quando a prestação ainda é possível, mas não foi cumprida no tempo, lugar e forma acordados. Neste caso, o credor pode exigir o cumprimento com uma compensação pelo atraso.

Por fim, lembram que o art. 389 do CC/2002 é a base legal da responsabilidade civil contratual, enquanto a responsabilidade civil extracontratual ou aquiliana encontra fundamento em outras disposições, como o artigo 927 do CC/2002. Este ponto de vista sublinha a distinção entre responsabilidades decorrentes de relações contratuais e aquelas que surgem independentemente de um contrato.

Esta questão do inadimplemento que revela, segundo o ordenamento jurídico brasileiro, o vínculo necessário entre os sujeitos que manifestam uma vontade para satisfazer um interesse individual, traz à tona novamente a questão da boa-fé. A segurança jurídica tem a boa-fé em termos genéricos um ponto de apoio, mas que deve ser analisada de forma mais aprofundada em razão de suas raízes não só jurídicas, mas também por estar impregnada de significado moral.

Gonçalves (2008, p. 130-135) fez um interessante estudo sobre o princípio da boa-fé, suas perspectivas e aplicações, oferecendo uma análise abrangente sobre a boa-fé, explorando suas dimensões morais, éticas e jurídicas. Apresenta várias conclusões de seu estudo, destacando a origem pré-jurídica da boa-fé, imbuída de significado moral, referindo-se à verdade, não-contradição, sinceridade, honestidade, fidelidade à palavra e manutenção da promessa. Ela enfatiza que a boa-fé se relaciona com a pessoa como um todo, abrangendo tanto aspectos

internos quanto externos: "A boa-fé é identificada no contexto pré-jurídico impregnada de carga moral".

Distingue entre boa-fé subjetiva e objetiva. A boa-fé subjetiva diz respeito à intenção interna e sincera da pessoa, enquanto a boa-fé objetiva se relaciona com um padrão de conduta externa baseado no comportamento de um indivíduo honesto e leal. Ela argumenta que, do ponto de vista ético, apenas a boa-fé objetiva pode ser considerada, pois a ética lida com ações ordenadas a um fim, enquanto a moral envolve uma avaliação mais ampla do caráter.

Gonçalves também aborda a relação entre boa-fé e confiança, destacando que a confiança é um elemento essencial nas relações humanas e serve como ponte entre os aspectos interno e externo da boa-fé. Ela explica que a boa-fé subjetiva representa a essência da confiança, enquanto a boa-fé objetiva fornece um meio legal para sua proteção.

Destaca a autora a relevância da boa-fé no Direito, afirmando que, apesar de sua origem pré-jurídica, ela é essencial para a interpretação e aplicação justa das leis. A boa-fé guia os operadores do Direito contra injustiças, permitindo decisões que levem em conta a finalidade da ação e o dever de orientação para o bem comum: "seu caráter ético guia o intérprete contra injustiças".

Gonçalves discute a importância da boa-fé na estrutura da sociedade e no convívio entre os indivíduos. Ela realça a necessidade de conciliar os aspectos formais do ordenamento jurídico com as demandas sociais por justiça material, destacando o papel dos princípios como veículos de valores no sistema jurídico: "o desafio atual consiste em conciliar a formalidade do ordenamento com as exigências sociais".

As relações jurídicas baseadas em ambiente virtual também merecem a atenção da boa-fé, especialmente diante da ausência de elementos físicos desta interrelação, onde os elementos da linguagem corporal, as trocas de impressões interpessoais são mitigadas, o que eleva a importância da boa-fé objetiva na interpretação da vontade manifestada.

Gonçalves (2008, p. 135-139) enfatiza a natureza humana e sua importância para a formação de relações confiáveis e a construção de uma comunidade sólida. A autora destaca que a boa-fé é fundamental para a afirmação do ser humano e sua singularidade, citando Hannah Arendt: a necessidade do espaço coletivo para a afirmação do ser humano "denota a suma importância das normas de caráter agregador".

Gonçalves aborda as bases constitucionais do princípio da boa-fé, que se encontram na dignidade da pessoa humana e na solidariedade. Ela argumenta que a boa-fé, como tratamento probo, veraz e leal, é um corolário dos direitos

da personalidade, e que seu descumprimento fere a dimensão moral desses direitos e a dignidade humana. A solidariedade, por sua vez, envolve a disposição de cooperação e vai além do âmbito individual em prol do social, influenciando a concepção atual da boa-fé.

Ao longo da história, continua, o sentido e a extensão da boa-fé variaram, adaptando-se aos valores preponderantes de cada época. No Direito romano, a boa-fé tinha um caráter objetivo, centrado na conduta e nas expectativas razoáveis de diligência e probidade. O Direito Canônico, acrescenta a autora, enfatizou o aspecto subjetivo e íntimo da boa-fé, alinhado com a concepção religiosa da ausência de pecado. No período germânico, a boa-fé foi associada à confiança e aos ideais de honra e lealdade da cavalaria medieval.

Traz a autora a questão da boa-fé objetiva ao contexto brasileiro, visto que ganhou destaque com o advento do Código de Defesa do Consumidor, embora sua concepção como princípio e cláusula geral seja mais recente. Gonçalves ressalta que a introdução do valor da solidariedade na Constituição e a visão objetiva dos direitos resultaram em uma ordem jurídica que limita os direitos subjetivos individuais em favor de deveres objetivos e cooperação social.

Discute a autora o papel das cláusulas gerais, como a da boa-fé, que permitem ao intérprete avaliar o comportamento das partes diante das circunstâncias do caso concreto, estendendo os valores de solidariedade, justiça e confiança para além das situações especificamente regulamentadas. Ela argumenta que, embora as cláusulas gerais ofereçam ampla margem de interpretação, elas são instrumentos legais que expressam princípios e mantêm o Direito alinhado com as mudanças sociais e as peculiaridades dos casos individuais.

Gonçalves conclui enfatizando a importância de operar com princípios e valores contidos em cláusulas gerais, apesar das dificuldades que isso possa acarretar. Ela defende que a positivação dos valores nos princípios autoriza sua observância pelo uso da força do Estado, além de destacar a relevância da solidariedade, da dignidade humana e da confiança inerentes à boa-fé, enriquecendo o papel do Direito na regulação das relações sociais.

Isso revela a importância da manifestação de vontade consciente e esclarecido, visto que a definição das cláusulas gerais servirá de fonte para a interpretação dos contratos. A questão da falta de correspondência entre a vontade conscientemente manifestada e a obrigação assumida é um problema jurídico da maior relevância, especialmente agravado na proporção da complexidade das relações sociais.

Ao discutirem as condições e consequências do desejo de se desvincular unilateralmente de um negócio jurídico após sua conclusão, Schwab e Löhnig

(2012, p. 267-270) explicam que a legislação geralmente não permite a desvinculação unilateral de um acordo legalmente válido, que possui efeito vinculativo. Como dizem *„[d]as gültig zustande gekommene Geschäft hat bindende Wirkung“* [7]. Todavia, abordarem os mecanismos legais disponíveis no Código Civil Alemão (BGB) para dissolver unilateralmente um acordo jurídico, destacando quatro meios principais: impugnação, resolução por inadimplência, resilição do contrato e revogação, situações que se assemelham ao Código Civil brasileiro.

Na impugnação, ocorre a invalidação retroativa de uma declaração de vontade inicialmente válida. É permitida se a declaração foi feita sob um erro ou transmissão defeituosa que, embora não grave o suficiente para tornar a declaração inválida desde o início, torna injusto exigir que a pessoa permaneça vinculada a ela. Em certos casos, a pessoa que anula sua declaração pode ser responsável por compensar os danos sofridos pela outra parte devido à confiança na validade da declaração.

A resolução por inadimplência permite a dissolução unilateral de um contrato em certas circunstâncias, como o não cumprimento das obrigações contratuais por uma das partes. A resolução não invalida o contrato, mas transforma o relacionamento em uma obrigação de restituição. O contrato permanece válido, mas não é executado; quaisquer benefícios já recebidos devem ser devolvidos.

Por sua vez, a resilição é aplicável a contratos de longo prazo, como locações ou contratos de trabalho. Tem efeito a partir do momento em que é declarada ou de um momento futuro específico, mas não afeta a validade do contrato antes desse ponto.

A revogação ou arrependimento permite ao consumidor cessar a validade unilateralmente uma declaração de intenção de celebração de contrato em determinadas circunstâncias, como vendas porta a porta ou contratos à distância. As consequências da revogação são tratadas da mesma forma que as da rescisão.

Os institutos da anulação por impugnação podem ter causas diversas: por erro e por dolo ou coerção[8]. Schwab e Löhnig apontam que a anulação por erro é limitada no direito alemão a erros significativos e pode acarretar a obrigação de

7 Tradução livre: o negócio jurídico validamente concluído tem efeito vinculativo.

8 Neste ponto, as expressões alemãs no livro foram traduzidas na forma seguinte para a compreensão do texto: impugnação (Anfechtung); resolução por inadimplência (Rücktritt); resilição (Kündigung); revogação ou arrependimento (Widerruf); institutos da anulação por impugnação por ter causas diversas: por erro (Anfechtung wegen Irrtums) e por dolo ou coerção (Anfechtung wegen arglistiger Täuschung oder widerrechtlicher Drohung).

indenização, enquanto a anulação por dolo ou coerção não implica tal obrigação, pois a influência indevida na formação da vontade é atribuída à outra parte.

Segundo Lamy e Akaoui (2018), algumas nuances fundamentais devem ser compreendidas para a validade dos atos jurídicos quanto aos vícios da manifestação de vontade, visto que comprometem a liberdade ou a racionalidade, tendo o potencial de invalidar o negócio jurídico, uma vez que não refletem a verdadeira intenção das partes envolvidas.

Destacam os autores que entre o erro próprio e o dolo, ambos implicam uma vontade viciada pela carência de racionalidade. No erro próprio, a pessoa é levada a erro por uma concepção equivocada da realidade, enquanto no dolo, o engano é induzido por outra parte. Em ambos os casos, é necessário que o vício seja essencial e escusável para que invalide o negócio jurídico. A principal distinção reside na origem do engano. No erro, o equívoco é espontâneo e não provocado intencionalmente por terceiros; já no dolo, existe uma manipulação intencional da realidade por parte de outro indivíduo com o objetivo de induzir alguém a erro. Além disso, no dolo, é necessário que haja consciência da indução ao engano.

No caso da coação e do estado de perigo, apontam Lamy e Akaoui que nos dois casos os vícios se relacionam com a carência de liberdade na manifestação de vontade. A coação envolve uma ameaça externa que induz ao temor de um dano, levando a pessoa a agir sob pressão, enquanto o estado de perigo se caracteriza por um temor espontâneo diante de uma situação de risco iminente que exige ação para salvaguarda própria ou de outrem. A coação pressupõe uma violência ou ameaça injusta vinda de terceiros que resulta em um temor iminente e considerável, exigindo uma relação de causalidade direta entre a ameaça, o temor e a declaração viciada. Já o estado de perigo deriva de uma situação objetiva de risco, não necessariamente provocada por terceiros, e a pessoa, diante do temor grave e iminente, aceita condições excessivamente onerosas para evitar o perigo.

A lesão subjetiva, possui segundo Lamy e Akaoui peculiaridades que a distingue dos demais vícios. Esta envolve uma situação de necessidade ou inexperiência que leva a pessoa a aceitar uma prestação desproporcionalmente onerosa. É marcada pela carência de liberdade ou consciência na avaliação do negócio, podendo ser exacerbada por uma relação de vulnerabilidade evidente entre as partes. Difere dos outros vícios principalmente pela ênfase na desproporcionalidade do negócio e na condição subjetiva de necessidade ou inexperiência. Enquanto outros vícios se concentram mais diretamente na maneira pela qual a vontade é formada ou distorcida (por erro, engano, coação ou

perigo), a lesão subjetiva enfoca as condições desvantajosas que exploram a condição de uma das partes.

A lesão subjetiva, especialmente considerando a inexperiência no contexto dos contratos digitais, levanta questões importantes sobre a validade desses contratos diante dos desafios inerentes ao ambiente digital. A evolução tecnológica e a digitalização das transações comerciais expandiram o alcance e a complexidade dos contratos eletrônicos, colocando os usuários, muitas vezes inexperientes, diante de termos e condições que podem não compreender totalmente, especialmente na interação direta entre o homem e a máquina. Esta situação é exacerbada pela facilidade com que as assinaturas eletrônicas podem ser implementadas, muitas vezes com um simples clique ou aceitação de termos sem a leitura adequada.

O direito contratual tradicionalmente protege as partes contra a exploração em virtude de sua vulnerabilidade, seja por necessidade, inexperiência ou por uma significativa disparidade de poder e informação. A lesão subjetiva, como vício, reflete essa preocupação ao invalidar contratos nos quais uma parte aceita condições desproporcionalmente onerosas devido à sua inexperiência ou necessidade. Usuários podem não estar plenamente cientes das implicações de seus atos no ambiente digital, especialmente em relação à adesão a termos e condições complexos ou ao uso de assinaturas eletrônicas. A inexperiência com a natureza e o funcionamento de contratos digitais pode levar a uma aceitação inadvertida de termos desfavoráveis. A apresentação de termos contratuais em plataformas digitais nem sempre é feita de maneira transparente ou compreensível, podendo dificultar que usuários, especialmente os inexperientes, tenham pleno conhecimento dos compromissos que estão assumindo.

A facilidade com que uma assinatura eletrônica pode ser fornecida – muitas vezes sem uma compreensão clara de que um contrato está sendo formalizado – aumenta o risco de adesões não intencionais a termos não compreendidos ou não lidos. A validade dos contratos digitais tem relação direta com o vício de consentimento, podendo ser questionada sob a alegação de lesão subjetiva quando se demonstra que a inexperiência ou a falta de compreensão por parte do usuário resultou na aceitação de termos desproporcionalmente onerosos ou prejudiciais. O reconhecimento jurídico dessa vulnerabilidade requer uma análise detalhada das circunstâncias de cada caso, considerando a adequação das informações, seja através de aplicativos, plataformas digitais, telemarketing, especialmente em termos de consentimento para a formação do contrato.

Deve-se examinar a forma como o consentimento é obtido, principalmente de usuários inexperiente, especialmente em relação ao uso de assinaturas

eletrônicas, para assegurar que houve uma manifestação de vontade livre e esclarecida. A legislação de proteção ao consumidor desempenha um papel crucial, impondo obrigações aos fornecedores de serviços digitais para garantir a justiça e a equidade nas práticas contratuais e na obtenção do consentimento.

1.3 TRANSFORMAÇÕES DOS CONTRATOS: DO PAPEL AO DIGITAL

A manifestação de vontade na forma de assinatura digital representa uma das várias formas de demonstração desta vontade que foram aceitas ao logo dos anos, não constituindo a única possível para atribuição de validade jurídica. A evolução histórica dos contratos reflete as mudanças nas formas de comércio e comunicação, sendo que o caminho do papel ao digital é apenas uma de suas etapas.

A forma manuscrita para a contratação é uma etapa relativamente recente. Garbi (2020) apresentou breve estudo sobre a evolução do contrato e o seu controle judicial, destacando como principais argumentos o fato de inicialmente o contrato ter um papel secundário em relação à propriedade, de modo que a evolução para o papel acompanhou uma mudança central na economia e na sociedade, sendo que "no direito romano a figura central era a propriedade... Ao contrato se reservava a função de aquisição e disposição da propriedade."

A revolução francesa e o Código de Napoleão trouxeram um novo significado à importância do contrato mediante a valorização da autonomia da vontade, servindo o contrato como uma garantia da conservação da propriedade. Já no século XX, inicia-se o período que o autor entende como a modernização e objetivação do contrato, mediante a diminuição da ênfase na vontade subjetiva, pois "nos Novecentos se acentua a tendência de objetivar o contrato, reduzindo o valor subjetivo da vontade das partes." (Garbi, 2020).

Esta exposição evolutiva do contrato leva à discussão a respeito da teoria do contrato, sendo relevante a tese de sua reabsorção na teoria geral do delito, feita por Gilmore (1974, p. 87-101), que entende que as teorias clássicas do contrato estão se desintegrando por razões diversas, como a do enriquecimento ilícito, a aproximação da responsabilidade contratual da delitual, a responsabilidade por vícios nos produtos, com a erosão do conceito tradicional

de negligência, distanciando-se claramente da teoria clássica do *laissez-fair*[9], da teoria individualista do século XIX. Todavia, embora tentador, o tema vai além do que é proposto na presente pesquisa, que trata da dogmática a respeito da validade da manifestação de vontade no contexto digital.

Ainda sobre o aspecto evolutivo, Garbi (2020) aponta que a jurisprudência moderna assume um papel ativo no controle do contrato, equilibrando autonomia contratual e justiça, pois "em favor da equidade e da justiça contratual, o juiz se habilita a corrigir o ato de autonomia contratual.". Acrescenta que a crise do Estado moderno reflete na compreensão do contrato, com Keynes negando o direito absoluto no contrato, sendo que nesta fase pós-industrial, o contrato se adapta à economia financeira, ganhando complexidade técnica, inclusive citando a ênfase de Miguel Reale sobre a necessidade de equilíbrio entre autonomia individual e valor coletivo nos contratos. Conclui que o controle judicial do contrato é amplo, porém limitado pela jurisprudência e ordem jurídica, sendo que a jurisprudência, especialmente no Brasil, desempenha um papel crucial na estabilidade e racionalidade do Direito Privado, pois "as normas decorrentes da jurisprudência, pela sua concretude e historicidade, podem ser mais estáveis e racionais", de modo que o controle judicial busca equilibrar o individualismo do poder negocial com a promoção dos valores sociais.

O impacto da revolução industrial na formação dos contratos foi considerável, emergindo a padronização não só na produção, mas também das relações jurídicas. Hobsbawm (2000, p. 38-41), destaca que a revolução industrial representou não apenas como o capital necessário para a Revolução Industrial foi acumulado, mas principalmente como essa "explosão" econômica foi efetivamente iniciada e o que a sustentou. Hobsbawn afirma que ao contrário da crença popular, as economias de iniciativa privada não tendem automaticamente à inovação; elas visam principalmente o lucro. A inovação ocorre quando é vista como um meio de aumentar os lucros. Em vista disso, acrescenta, a industrialização trouxe a padronização de produtos, diferentemente das economias

9 Keynes (1926) questiona a eficácia do laissez-faire em promover o bem-estar social, ressaltando a necessidade de uma ação coordenada e deliberada em áreas como controle monetário, investimento e população. Ele sugere que o progresso residiria no reconhecimento de entidades semi-autônomas dentro do Estado, que atuariam pelo bem público, e na distinção entre os serviços sociais e individuais. Keynes defende uma abordagem mais pragmática e menos dogmática na economia, que levasse em conta tanto o papel do Estado quanto o da iniciativa privada. Segundo Kaynes, "a cura [dos males econômicos] reside fora das atividades dos indivíduos; pode até ser do interesse destes o agravamento da doença". Keynes enfatiza a importância de entender a relação entre os motivos monetários individuais e a organização social, propondo uma reflexão sobre como administrar o capitalismo de forma eficiente sem comprometer um modo de vida satisfatório.

pré-industriais que focavam em bens de luxo para os ricos e bens simples para os pobres. Esta padronização permitiu a expansão de mercados e a criação de demanda para produtos em massa. Revelou-se a importância dos mercados internos e externos na Revolução Industrial, sugerindo que ambos foram cruciais para o seu desenvolvimento, junto com o papel do governo, exemplificando o autor ao afirmar que "*when Henry Ford produced his Model-T, he also produced what had not existed before, namely a vast number of buyers for a cheap, standardized, and simple car*" [10], o que revela uma fundamental trazida pela Revolução Industrial: a criação de mercados de massa para produtos padronizados, algo que não era concebível nas economias pré-industriais.

Com efeito, a forma impressa dos contratos ganha relevância, carecendo da assinatura dos contratantes para que a manifestação de vontade para a criação de obrigações seja claramente delineada. Algumas variações para a contratação em massa emergiram, como é o caso dos contratos de adesão, onde, na forma clássica, as disposições são previa e unilateralmente estabelecidas, cabendo ao interessado apenas assinar em aderência aos seus termos.

Este aspecto jurídico é um reflexo da política desenvolvida em apoio à revolução industrial. Conforme demonstra Hobsbawm (2000, p. 49) o governo britânico desempenhou um papel crucial na gênese da Revolução Industrial, subordinando a política externa a objetivos econômicos, incluindo a conquista de mercados através da guerra e da colonização. Diferentemente de outros países europeus, a Grã-Bretanha estava disposta a alinhar sua política externa, incluindo atividades bélicas e coloniais, com os interesses econômicos, especialmente os dos manufatureiros britânicos, protegendo os produtores nacionais contra a concorrência externa, primeiro no mercado interno e, posteriormente, no externo, exemplificado pela restrição de importações de têxteis indianos.

A era digital representou uma mudança significativa nesta estrutura pós-revolução industrial, pois o padrão de contratação em papel assumiu a forma computacional, por meio de sistemas informáticos, representando também na adaptação das disposições legais com novos desafios.

Petrillo et al. (2018) discutem a transformação da indústria em direção à completa digitalização e inteligência dos processos de produção, visando maior eficiência, destacando a necessidade de implementar novas tecnologias para automatizar processos industriais, fundamentais para a Indústria 4.0, que se baseia

10 Tradução livre: quando Henry Ford produziu seu Modelo-T, ele também produziu o que antes não existia, ou seja, um enorme número de compradores para um carro barato, padronizado e simples.

no conceito de fábrica inteligente, onde as máquinas são integradas com os seres humanos através de sistemas ciber-físicos. Esta revolução, argumentam, abrange a digitalização e a integração aumentada das cadeias de valor verticais e horizontais, bem como a digitalização das ofertas de produtos e serviços, com a introdução de modelos de negócios digitais inovadores, com alto nível de interação entre sistemas e oportunidades tecnológicas. A revolução industrial atual se caracteriza pela colaboração de máquinas inteligentes, sistemas de armazenamento e sistemas de produção em redes inteligentes, fundindo os mundos real e virtual. A Indústria 4.0 é vista como um salto disruptivo no processo industrial, com mudanças fundamentais na sociedade e na economia.

Reed (2019, p. 2-9) apresenta uma análise profunda sobre como a era digital e as tecnologias de informação e comunicação (TICs) têm remodelado a cultura, o poder e as dinâmicas sociais em escala global. O autor destaca como a Internet revolucionou a comunicação humana, tornando-a mais acessível e instantânea. Argumenta que diferentes meios de comunicação, como correspondência, telefonemas, cinema e música, foram digitalizados, alterando a forma como nos conectamos globalmente. Questiona a novidade real das mídias digitais, indagando sobre a profundidade das mudanças nas relações interpessoais, na informação política, na economia e no entretenimento causadas por essas tecnologias, sendo percebida a cultura digital onde a tecnologia molda as relações sociais. Ele aborda como experiências online influenciam o mundo offline e vice-versa, destacando a fluidez e a constante evolução das culturas digitais. "*Culture is one of the most complicated words in the English language, but for our purposes we can simplify it to mean the values, beliefs and behaviors that are typical and defining of a group*" [11].

Argumenta como as tecnologias digitais são fundamentais na atual fase da globalização, facilitando o movimento transnacional de dinheiro, dados e conhecimento, em que pese reconhecer contradições na cultura digital, como na promoção da justiça social versus a disseminação de ódio, o empoderamento de minorias versus a marginalização, e a criação de espaços para novas vozes versus a dominância de culturas majoritárias. Um aspecto crucial abordado é a "divisão digital", destacando as disparidades no acesso e uso da Internet globalmente, influenciadas por diferenças econômicas e sociais. Ainda segundo o autor, faz-se necessário compreender s dimensões culturais e sociais das tecnologias digitais,

11 Tradução livre: A cultura é uma das palavras mais complicadas da língua inglesa, mas para nossos fins, podemos simplificá-la para significar os valores, crenças e comportamentos que são típicos e definidores de um grupo.

quem se beneficia delas e como podem ser usadas para promover a justiça social e mudanças progressistas. Reed adota uma abordagem de conhecimento situado, reconhecendo as limitações e os vieses inerentes à análise cultural e buscando uma compreensão mais objetiva das dinâmicas de poder nas culturas digitais, não deixando de reconhecer a quadra atual como uma revolução digital que está transformando nossas formas de conhecer o mundo e a nós mesmos, alterando significativamente identidades e práticas culturais.

A exemplo, uma das formas desenvolvidas para validação das relações digitais nesta nova cultura foi com o desenvolvimento do blockchain. Como apresentação neste trabalho, é suficiente destacar neste capítulo que esta tecnologia foi originalmente desenvolvida para o funcionamento do protocolo Bitcoin, um sistema descentralizado onde os membros permanecem anônimos. As transações são controladas para prevenir o *Double Spending*, um fenômeno em que informações digitais podem ser usadas simultaneamente por vários usuários. Um aspecto distintivo da blockchain é sua natureza descentralizada, permitindo comunicação direta entre os usuários sem intermediários. Isso torna o sistema imune a controles externos. A blockchain consiste em uma rede de usuários que interagem entre si, com todas as transações sendo publicamente auditáveis. O sistema não se limita apenas à transferência de criptomoedas, mas também pode representar propriedade de bens físicos ou direitos legais. As transações são armazenadas e gerenciadas em nós (nodes), que mantêm um histórico imutável de todas as transações (Hein; Hein; Wellbrock, 2019, p. 5-14).

Até este ponto, vimos os fundamentos teóricos essenciais sobre o tema, como a questão da segurança jurídica, os princípios contratuais e da manifestação de vontade, bem como as transformações culturais, sociais, econômicas e jurídicas da predominância dos contratos escritos em papel para o formato digital. É necessário, a seguir, abordar não só os elementos constitutivos da assinatura digital, mas também seus aspectos técnicos e como a sua importância vem sendo tratada nos primeiros ensaios regulatórios.

1.4 DEFINIÇÃO E ELEMENTOS CONSTITUTIVOS DA ASSINATURA DIGITAL

As assinaturas digitais são vistas como uma das invenções mais fundamentais e úteis da criptografia moderna. Seu esquema permite que cada usuário assine mensagens de maneira que as assinaturas possam ser verificadas por qualquer pessoa. Especificamente, cada usuário cria um par de chaves, privada

e pública, de tal forma que apenas ele pode criar uma assinatura para uma mensagem usando sua chave privada, mas qualquer pessoa pode verificar a assinatura usando a chave pública do remetente (GOLDWASSER; BELLARE, 2008, p. 168). Segundo os autores, "*the verifier can convince himself that the message contents have not been altered since the message was signed. Also, the signer can not later repudiate having signed the message, since no one but the signer possesses his private key*" [12], o que ressalta a segurança proporcionada pela assinatura digital, garantindo a integridade da mensagem e a impossibilidade de o signatário negar a autoria da assinatura.

Goldwasser e Bellare fazem uma analogia com o mundo físico, onde se pode assinar uma carta e selá-la em um envelope. De maneira semelhante, pode-se assinar uma mensagem eletrônica usando a chave privada e depois selar o resultado criptografando-a com a chave pública do destinatário. O destinatário, então, realiza as operações inversas para abrir a "carta" e verificar a assinatura, usando sua chave privada e a chave pública do remetente, respectivamente. Esta aplicação da tecnologia de chave pública para o correio eletrônico já é bastante difundida. Se o diretório de chaves públicas for acessado pela rede, é necessário proteger os usuários de mensagens fraudulentas que alegam ser chaves públicas do diretório. Uma solução elegante, acrescentam, é o uso de um certificado - uma cópia da chave pública do usuário assinada digitalmente pelo gerente do diretório de chaves públicas ou outra parte confiável. Se o usuário mantiver localmente uma cópia da chave pública do gerente do diretório, ele pode validar todas as comunicações assinadas vindas do diretório de chaves públicas e evitar ser enganado ao usar chaves fraudulentas. Apontam que cada usuário pode transmitir o certificado de sua chave pública com qualquer mensagem que assine, eliminando a necessidade de um diretório central e permitindo verificar mensagens assinadas sem informações adicionais além da chave pública do gerente do diretório.

12 Tradução livre: o verificador pode convencer-se de que o conteúdo da mensagem não foi alterado desde que a mensagem foi assinada. O signatário não pode posteriormente repudiar ter assinado a mensagem, já que ninguém além do signatário possui sua chave privada.

1.5 ASPECTOS TÉCNICOS: CRIPTOGRAFIA E CHAVES PÚBLICAS

Uma visão técnica a respeito da criptografia se faz necessária para a compreensão do fenômeno jurídico, mesmo que não se adentre nas métricas e tecnologias matemáticas para a realização da certificação digital[13].

Katz e Lindell (2015, p. 441-443) abordam a definição e a segurança de esquemas de assinaturas digitais, destacando seu papel crucial na criptografia moderna. As assinaturas digitais são vistas como o equivalente, no mundo das chaves públicas, aos códigos de autenticação de mensagens. Elas possuem uma sintaxe e garantias de segurança análogas, com a diferença de que o algoritmo usado pelo remetente para assinar uma mensagem é chamado de "Sign" (em vez de "Mac") e seu resultado é conhecido como uma assinatura (e não uma etiqueta). Tanto o "Mac" quanto o "Sign" possuem a finalidade de garantir a integridade e autenticidade de uma mensagem digital através da criptografia. No entanto, o "Mac" não garante a identidade do remetente, o que é feito pela autenticação "Sign". Katz e Lindell apontam que o esquema de assinatura digital consiste em três algoritmos: geração de chaves (Gen), assinatura (Sign) e verificação (Vrfy). A Geração de Chaves (Gen) cria um par de chaves, pública (pk) e privada (sk), a partir de um parâmetro de segurança. A Assinatura (Sign) usa a chave privada (sk) e uma mensagem para produzir uma assinatura. A assinatura é única para cada mensagem e apenas o detentor da chave privada pode gerá-la. A Verificação (Vrfy) consiste em algoritmo determinístico que verifica a validade de uma assinatura usando a chave pública (pk), a mensagem e a assinatura. Ele retorna um bit indicando se a assinatura é válida (1) ou inválida (0).

Por trás dos esquemas de assinaturas digitais temos a teoria da criptografia. Katz e Lindell (2015, p. 3-4) lembram que a criptografia é tradicionalmente definida como a arte de escrever ou resolver códigos, tendo evoluído significativamente ao longo do tempo. Historicamente, a criptografia estava centrada em códigos secretos para comunicação, mas hoje seu escopo é muito mais amplo, incluindo mecanismos para garantir a integridade dos dados, técnicas de troca de chaves secretas, protocolos de autenticação de usuários, leilões eletrônicos, eleições, dinheiro digital e muito mais. A criptografia moderna envolve o estudo

13 A questão regulatória, como a UNCITRAL e a Medida Provisória nº 2.200/2001 serão abordadas a seguir, no capítulo que trata da regulação dos documentos digitais.

de técnicas matemáticas para proteger informações digitais, sistemas e computações distribuídas contra-ataques adversários.

Antigamente, acrescentam os autores, a criptografia era mais uma arte do que uma ciência, baseada na criatividade e no entendimento prático de como os códigos funcionavam, sem uma teoria sólida ou definição de um bom código. Contudo, a partir das décadas de 1970 e 1980, o campo passou por uma transformação radical, desenvolvendo uma teoria rica e se estabelecendo como uma disciplina científica e matemática rigorosa, influenciando também a forma como pesquisadores veem a segurança da computação como um todo.

Enquanto historicamente seu uso principal era em organizações militares e governamentais, hoje ela está presente em quase todos os aspectos da vida cotidiana, como na autenticação de senhas, compras com cartão de crédito pela internet e atualizações verificadas de sistemas operacionais. Programadores, muitas vezes sem grande experiência, são solicitados a incorporar mecanismos criptográficos em suas aplicações.

Katz e Lindell (2015, p. 4-6) anotam que a criptografia clássica focava no design e uso de códigos (ou cifras) que permitiam a comunicação secreta entre duas partes na presença de um observador externo. Nos termos modernos, esses códigos são chamados de esquemas de criptografia, e a segurança de todos esses esquemas clássicos dependia de uma chave secreta compartilhada antecipadamente pelas partes e desconhecida pelo observador. Esse cenário é conhecido como configuração de **chave privada** (ou chave compartilhada/segredo), e a criptografia de chave privada é apenas um exemplo de um primitivo criptográfico usado nesse contexto.

Na criptografia de chave privada, duas partes compartilham uma chave e a utilizam para se comunicar secretamente. Uma parte pode enviar uma mensagem, ou texto puro, para a outra, usando a chave compartilhada para criptografar (ou "embaralhar") a mensagem e obter um texto cifrado que é transmitido ao receptor. O receptor usa a mesma chave para descriptografar (ou "desembaralhar") o texto cifrado e recuperar a mensagem original. Observam os autores que "*the same key is used to convert the plaintext into a ciphertext and back; that is why this is also known as the symmetric-key setting*". Neste contexto, diante do uso de uma mesma chave entre o emissor e o recebedor da mensagem, temos a **criptografia simétrica**.

Essa configuração é contrastada com a **criptografia assimétrica**, ou criptografia de **chave pública**, onde chaves diferentes são usadas para criptografar e descriptografar. Segundo Katz e Lindell, existem duas aplicações canônicas da criptografia de chave privada. A primeira envolve duas partes distintas separadas

espacialmente, como um trabalhador em Nova York se comunicando com um colega na Califórnia. Esses usuários devem ter compartilhado uma chave de forma segura antes de sua comunicação. A segunda aplicação envolve a mesma parte se comunicando consigo mesma ao longo do tempo, como na criptografia de disco, onde um usuário criptografa um texto puro e armazena o texto cifrado no disco rígido, para depois descriptografar e recuperar os dados originais.

A introdução da criptografia de chave pública, segundo Katz e Lindell (2015, p. 375-377), representou uma revolução na área, permitindo que as partes se comuniquem privadamente sem ter acordado previamente qualquer informação secreta. Esta abordagem é notavelmente surpreendente e contra-intuitiva, pois "duas pessoas de lados opostos de uma sala que só podem se comunicar gritando uma com a outra, e não têm nenhum segredo inicial, podem falar de uma maneira que ninguém mais na sala aprenda nada sobre o que estão dizendo!"

Na criptografia de chave privada, as partes concordam com uma chave secreta para criptografar e descriptografar mensagens. Em contraste, a criptografia de chave pública é **assimétrica**: uma parte (o receptor) gera um par de chaves, a chave pública (pk) e a chave privada (sk), com a chave pública usada para criptografar e a privada para descriptografar mensagens.

Existem duas maneiras de como o remetente pode aprender pk. Uma abordagem é o receptor gerar (pk, sk) e enviar pk ao remetente, que então usa pk para criptografar sua mensagem. Alternativamente, o receptor pode gerar suas chaves com antecedência e amplamente disseminar sua chave pública, permitindo que qualquer um que deseje se comunicar com ele possa usar essa chave pública. Segundo os autores, "*note that pk is inherently public—and can thus be learned easily by an attacker*".

A segurança da criptografia de chave pública depende da manutenção do segredo de sk, sendo crucial que "*Alice not reveal her private key to anyone, including the sender Bob*". A principal diferença entre a criptografia de chave privada e a pública é que a primeira exige total segredo de todas as chaves criptográficas, enquanto a última requer segredo apenas para a chave privada sk. Isso, segundo os autores, tem implicações enormes: na criptografia de chave pública, a chave pública pode ser enviada de uma parte para outra por um canal público sem comprometer a segurança.

Como já apontado pelos autores, a distinção importante é que os esquemas de criptografia de chave privada usam a mesma chave para criptografia e descriptografia, enquanto os de chave pública usam chaves diferentes para cada operação. Isso significa que a criptografia de chave pública é inerentemente assimétrica e "*a single key-pair allows communication in one direction only*".

Entre as vantagens da criptografia de chave pública em relação à chave privada, destacam-se a resolução parcial do problema de distribuição de chaves e a conveniência para um receptor que se comunica com vários remetentes, conforme os autores. No entanto, a criptografia de chave pública tem a desvantagem de ser significativamente mais lenta do que a de chave privada, o que pode ser um desafio em dispositivos com recursos limitados. Segundo afirmam, "*when private-key encryption is an option, then it typically should be used*". Na prática, argumentam, a criptografia de chave privada é frequentemente usada em conjunto com a de chave pública para melhorar a eficiência.

A infraestrutura para as chaves públicas é explicada por Malone (2023), que apresenta uma visão geral e simplificada sobre certificados e a Infraestrutura de Chave Pública (PKI – Public Key Infrastructure). O autor reconhece a complexidade do tema, mas enfatiza a importância e a utilidade da PKI em estabelecer sistemas seguros e universais para a comunicação criptografada. Reconhece o autor que a PKI é poderosa e interessante, em que pese sua matemática complexa e padrões complicados. Ele ressalta que "*PKI lets you define a system cryptographically*" ("PKI permite que você defina um sistema criptograficamente"), sublinhando sua universalidade e flexibilidade. Um ponto-chave discutido é a autenticação de mensagens usando MACs (Códigos de Autenticação de Mensagem) e assinaturas digitais. Enquanto os MACs utilizam uma senha compartilhada para autenticar mensagens, as assinaturas digitais usam um par de chaves, sendo a chave privada usada para gerar a assinatura e a chave pública para verificá-la. Isso leva ao conceito de não-repúdio, onde o titular da chave privada não pode negar a autoria dos dados assinados. Malone aborda a criptografia de chave pública (ou assimétrica), explicando que ela usa pares de chaves para criptografar dados e assinar digitalmente, permitindo que computadores e códigos autentiquem suas identidades de maneira segura através de redes. O autor compara certificados digitais a licenças de motorista ou passaportes para computadores e códigos, ligando chaves públicas a nomes e assegurando a autenticidade. O autor aborda ainda a complexidade técnica de representar certificados como bits e bytes, detalhando padrões como X.509, ASN.1, OIDs,

DER, PEM e PKCS[14]. Ele lamenta a confusão e frustração que muitas vezes acompanham a aprendizagem e a aplicação de PKI, devido à sua natureza esotérica e mal definida, mas enfatiza que, no fundo, um certificado é simplesmente "*a thing that binds a public key to a name*".

1.6 ABORDAGEM EUROPEIA SOBRE A IMPORTÂNCIA DA IDENTIFICAÇÃO DIGITAL

Sobre a validade jurídica e probatória das assinaturas digitas, podemos extrair da exposição dos fundamentos normativos que o Parlamento Europeu apresentou para a edição do Regulamento nº 910/2014[15] sobre identificação eletrônica e serviços confiáveis para transações eletrônicas no mercado interno.

14 Existem vários protocolos de segurança que são utilizados para garantir a eficácia das assinaturas digitais, destacando-se: 1. Padrão de Assinatura Digital (DSS - Digital Signature Standard): Desenvolvido pelo Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA. Baseia-se no algoritmo de assinatura digital (DSA - Digital Signature Algorithm). Utiliza a criptografia assimétrica, onde a assinatura é gerada usando uma chave privada e pode ser verificada por qualquer pessoa com a chave pública correspondente. Oferece validação da origem da mensagem e integridade dos dados. 2. Secure Hash Algorithm (SHA): Uma família de funções hash criptográficas projetadas pelo NIST. SHA-1, SHA-256 e SHA-512 são as variantes mais comuns, com SHA-256 e SHA-512 sendo mais seguras e amplamente usadas. As funções hash transformam uma mensagem de comprimento variável em um resumo de mensagem de comprimento fixo, um processo essencial nas assinaturas digitais. Um hash seguro garante que a mensagem não foi alterada, pois qualquer modificação na mensagem resultaria em um hash diferente. 3. RSA (Rivest-Shamir-Adleman): Um dos primeiros sistemas de criptografia de chave pública e ainda amplamente utilizado para assinaturas digitais. Baseia-se na dificuldade de fatorar números grandes compostos por dois primos. RSA permite que a chave privada crie uma assinatura que pode ser verificada por qualquer pessoa com a chave pública correspondente. 4. Elliptic Curve Digital Signature Algorithm (ECDSA): Uma variante do DSA que usa criptografia de curva elíptica. Oferece um nível mais alto de segurança com chaves menores comparado a algoritmos não baseados em curvas elípticas, como o RSA. É eficiente e rápido, tornando-o adequado para dispositivos com recursos limitados. 5. PGP (Pretty Good Privacy) e GPG (GNU Privacy Guard): PGP é um programa de criptografia que fornece assinaturas digitais em comunicações eletrônicas. GPG é uma versão de código aberto do PGP. Ambos utilizam uma combinação de criptografia simétrica e assimétrica, incluindo RSA e DSA, para assinatura e criptografia de e-mails. 6. X.509 Certificados Digitais: Um padrão para certificados digitais que usa RSA ou DSA para assinaturas digitais. X.509 é fundamental para TLS/SSL, o protocolo por trás da segurança HTTPS na Web.

15 A União Europeia (UE) utiliza diversos tipos de atos legislativos para alcançar os objetivos traçados em seus tratados. Estes atos podem ser vinculativos ou não, e podem ser aplicados a todos os países da UE ou apenas a alguns. Principais diferenças: **Regulamento**: Ato vinculativo que deve ser aplicado integralmente em toda a UE. Exemplo: Tarifas de itinerância. **Diretiva**: Ato que define um objetivo que os países da UE devem alcançar, mas cabe a cada país definir suas leis para tal. Exemplo: Redução do impacto de plásticos de utilização única. **Decisão**: Ato vinculativo apenas para seus destinatários específicos (país da UE, empresa) e é diretamente aplicável. Exemplo: Adoção do euro pela Croácia. **Recomendação**: Ato não vinculativo que sugere uma linha de conduta, sem impor obrigações legais. Exemplo: Transparência na propriedade de serviços de comunicação social. **Parecer**: Declaração não vinculativa que permite às instituições da UE se manifestarem sobre um determinado assunto. Exemplo: Estratégia de nova geração para as PME. (https://european-union.europa.eu/institutions-law-budget/law/types-legislation_pt).

O Regulamento enfatiza a importância da confiança no ambiente online para o desenvolvimento econômico e social. A falta de confiança, especialmente devido à falta de certeza legal, faz com que consumidores, empresas e autoridades públicas hesitem em realizar transações eletrônicas e adotar novos serviços.

A regulamentação busca aprimorar a confiança nas transações eletrônicas no mercado interno europeu, fornecendo uma base comum para interações eletrônicas seguras entre cidadãos, empresas e autoridades públicas. Isso visa aumentar a eficácia dos serviços online públicos e privados, do comércio eletrônico e dos negócios eletrônicos na União Europeia.

A Diretiva 1999/93/CE, que abordava assinaturas eletrônicas, não fornecia um quadro abrangente para transações eletrônicas seguras e confiáveis. O novo Regulamento expande e aprimora as diretrizes dessa Diretiva. Problemas como fragmentação do mercado digital, falta de interoperabilidade e aumento do cibercrime foram identificados como obstáculos ao desenvolvimento da economia digital.

O Conselho Europeu e a Comissão Europeia incentivaram a criação de um mercado único digital e a promoção de um mercado digital totalmente integrado, com atenção especial à identificação eletrônica segura e autenticação. A resolução do Parlamento Europeu de 21 de setembro de 2010 sobre o mercado interno de comércio eletrônico enfatizou a importância da segurança dos serviços eletrônicos, especialmente das assinaturas eletrônicas. Já a Diretiva 2006/123/CE exige que os Estados-membros estabeleçam 'pontos de contato únicos' para facilitar procedimentos e formalidades por meios eletrônicos. Muitos serviços online acessíveis através desses pontos exigem identificação eletrônica, autenticação e assinatura.

Por sua vez, a Diretiva 2011/24/UE estabeleceu uma rede de autoridades nacionais responsáveis pela e-saúde, enfatizando a necessidade de reconhecimento mútuo da identificação eletrônica e autenticação para facilitar o cuidado de saúde transfronteiriço.

O novo Regulamento deve ser aplicadao em total conformidade com os princípios de proteção de dados pessoais, processando apenas os dados de identificação necessários e respeitando a confidencialidade e segurança do processamento. Um dos objetivos é eliminar barreiras ao uso transfronteiriço de meios de identificação eletrônica, sem interferir nos sistemas de gestão de identidade eletrônica dos Estados-membros. Os Estados-membros têm liberdade para usar ou introduzir meios de identificação eletrônica e decidir sobre o envolvimento do setor privado.

A obrigação de reconhecer meios de identificação eletrônica se aplica apenas a esses meios cujo nível de garantia de identidade corresponde ou é superior ao nível exigido para o serviço online em questão. Os níveis de garantia devem caracterizar o grau de confiança nos meios de identificação eletrônica, assegurando que a pessoa que reivindica uma identidade é de fato a pessoa a quem essa identidade foi atribuída. O nível de garantia depende da confiança que os meios de identificação eletrônica proporcionam na identidade reivindicada, considerando processos, atividades de gestão e controles técnicos. Os requisitos estabelecidos devem ser neutros em relação à tecnologia.

Os Estados-membros devem incentivar o setor privado a usar voluntariamente meios de identificação eletrônica em um esquema notificado para fins de identificação em serviços online ou transações eletrônicas. Isso permitirá que o setor privado confie na identificação eletrônica e autenticação já amplamente utilizadas para facilitar o acesso a serviços online além das fronteiras.

O novo Regulamento estabelece a responsabilidade dos Estados-membros notificantes, da parte que emite os meios de identificação eletrônica e da parte que opera o procedimento de autenticação por não cumprimento das obrigações relevantes. No entanto, deve ser aplicada de acordo com as regras nacionais de responsabilidade.

A segurança dos esquemas de identificação eletrônica é fundamental para o reconhecimento mútuo confiável. Os Estados-membros devem cooperar quanto à segurança e interoperabilidade desses esquemas a nível da União. A cooperação entre os Estados-membros deve facilitar a interoperabilidade técnica dos esquemas de identificação eletrônica notificados, visando fomentar um alto nível de confiança e segurança.

O novo Regulamento estabelece um quadro legal geral para o uso de serviços de confiança, mas não cria obrigação geral de usá-los ou instalar um ponto de acesso para todos os serviços de confiança existentes. Os serviços de confiança devem ser utilizáveis como evidência em processos legais em todos os Estados-membros. O direito nacional define o efeito legal dos serviços de confiança, exceto se previsto de outra forma nesta Regulamentação. A obrigação de reconhecer um serviço de confiança só pode ser rejeitada por razões técnicas fora do controle imediato do destinatário da obrigação. Os Estados-membros podem manter ou introduzir disposições nacionais relativas a serviços de confiança, desde que esses serviços não sejam totalmente harmonizados pela Regulamentação europeia.

Permanecem os Estados-membros livres para definir outros tipos de serviços de confiança, além daqueles listados na Regulamentação, para

reconhecimento a nível nacional. Devido ao rápido avanço tecnológico, a nova Regulamentação adota uma abordagem aberta à inovação, sem renunciar à neutralidade em relação à tecnologia, e os efeitos legais que concede devem ser alcançáveis por qualquer meio técnico.

Para aumentar a confiança de pequenas e médias empresas (PMEs) e consumidores no mercado interno, são introduzidos os conceitos de serviços de confiança qualificados e provedor de serviços de confiança qualificados. Em conformidade com a Convenção das Nações Unidas sobre os Direitos das Pessoas com Deficiência, os serviços de confiança e os produtos finais usados na prestação desses serviços devem ser acessíveis para pessoas com deficiência.

Cabe aos Estados-membros designar um ou mais órgãos de supervisão para realizar as atividades de supervisão sob esta Regulamentação e podem decidir designar um órgão de supervisão em outro Estado-membro mediante acordo mútuo. Os órgãos de supervisão devem cooperar com autoridades de proteção de dados, como informar sobre resultados de auditorias de provedores de serviços de confiança qualificados, especialmente em casos de violação de proteção de dados pessoais.

Segundo a Regulação, a norma sobre identificação eletrônica emitida pelo Parlamento Europeu abrange diversos aspectos regulatórios focados em serviços de confiança. Todos os provedores de serviços de confiança são obrigados a aplicar práticas de segurança adequadas aos riscos relacionados às suas atividades, a fim de fortalecer a confiança dos usuários no mercado único. Eles devem estar sujeitos aos requisitos da Regulamentação, especialmente em termos de segurança e responsabilidade, sendo importante diferenciar entre provedores qualificados e não qualificados.

A Regulamentação estabelece um regime de responsabilidade, segundo o qual os provedores de serviços de confiança são responsáveis por danos causados por não cumprimento das obrigações estabelecidas. É essencial a notificação de violações de segurança e avaliações de risco para informar adequadamente as partes interessadas em caso de incidentes.

Órgãos de supervisão devem fornecer informações resumidas à Comissão e à ENISA (*European Union Agency for Network and Information Security*) para avaliar a eficácia dos mecanismos de notificação de violações. Devem relatar suas atividades para facilitar a troca de boas práticas e garantir a implementação eficiente dos requisitos de supervisão.

Para garantir a sustentabilidade e durabilidade dos serviços de confiança qualificados, os órgãos de supervisão devem verificar a existência e a correta aplicação de planos de término quando provedores cessam suas atividades.

Um sistema de assistência mútua entre órgãos de supervisão é estabelecido para facilitar a supervisão de provedores qualificados. É necessário realizar uma avaliação de conformidade por um órgão de avaliação de conformidade, com relatórios submetidos pelos provedores ao órgão de supervisão.

A Regulamentação visa garantir um quadro coerente para fornecer alto nível de segurança e certeza legal dos serviços de confiança, levando em conta padrões e especificações técnicas de organizações de padronização. Há um incentivo para interações preliminares entre potenciais provedores de serviços de confiança qualificados e o órgão supervisório competente.

Aspectos adicionais incluem a criação de um selo de confiança da UE para identificar serviços de confiança qualificados, a aceitação de assinaturas eletrônicas com menor garantia de segurança em casos específicos, e a definição de que documentos eletrônicos não devem ser negados efeito legal por serem eletrônicos. Selos eletrônicos servem para autenticar documentos emitidos por pessoas jurídicas e outros ativos digitais. A Regulamentação também aborda a autenticação de websites, estabelecendo obrigações mínimas de segurança e responsabilidade para os provedores desses serviços.

2 REGULAÇÃO DOS DOCUMENTOS DIGITAIS E A MANIFESTAÇÃO DE VONTADE NO AMBIENTE DIGITAL

2.1 PANORAMA NORMATIVO INTERNACIONAL

Em que pese diversas regulações surgirem a cada dia, a presente pesquisa sobre a regulação da assinatura eletrônica, quanto ao aspecto internacional, está focada no Mercosul, Estados Unidos e Europa, isso em razão da relevância econômica destas regiões e da sua proximidade e interação com o Brasil, tanto em termos geográficos quanto econômicos e tecnológicos.

O Mercosul, como bloco econômico regional, desempenha um papel crucial na economia brasileira. A integração econômica e a facilitação do comércio entre seus membros requerem uma infraestrutura digital robusta e harmonizada, da qual a certificação digital e a assinatura eletrônica são componentes essenciais. O estudo da regulação neste âmbito visa aprimorar a eficiência do comércio intrarregional, reduzir barreiras burocráticas e fortalecer a segurança jurídica nas transações eletrônicas. Considerando as recentes iniciativas de reconhecimento mútuo de assinaturas digitais no Mercosul, é fundamental compreender como essas regulamentações se integram e se alinham com as práticas internacionais.

Os Estados Unidos, por seu turno, como uma das maiores economias do mundo e um parceiro comercial significativo para o Brasil, representam um campo de estudo importante. As regulamentações estadunidenses sobre certificação digital e assinatura eletrônica têm grande influência global, e sua compreensão é vital para empresas brasileiras que operam no mercado internacional ou que buscam expansão nos EUA. A dinâmica tecnológica e as inovações advindas dos Estados Unidos impõem a necessidade de atualização e compatibilidade regulatória para facilitar as relações comerciais e proteger os interesses dos consumidores e empresas brasileiras.

A Europa, por sua vez, é um líder reconhecido em regulamentações de proteção de dados e segurança digital, como evidenciado pelo Regulamento para identificação eletrônica e serviços de confiança para as transações eletrônicas. Estudar a regulação europeia em certificação digital e assinatura eletrônica não só fornece perspectivas sobre práticas avançadas de segurança e privacidade, mas também é essencial para empresas brasileiras que atuam ou pretendem atuar no mercado europeu. A compatibilidade regulatória é uma questão chave para garantir a fluidez nas transações comerciais e a confiança nas relações digitais.

2.1.1 REGULAÇÃO NO MERCOSUL

Recentemente, surgiram acordos internacionais assinados com certificação digital, o que levanta a questão da sua regulação além dos países e blocos econômicos. Conforme noticiado pelo Serasa (2020), foi assinado o primeiro acordo internacional pelo Brasil realizado inteiramente através de Certificação Digital, em 2 de setembro de 2020, em que autoridades aduaneiras do Brasil e Peru, representadas pela Receita Federal do Brasil e a Superintendencia Nacional de Aduanas y de Administración Tributaria do Peru (SUNAT), assinaram digitalmente o "Acordo de Reconhecimento Mútuo sobre Operador Econômico Autorizado (OEA)". Este acordo, fruto de 22 meses de colaboração técnica, tem o objetivo de facilitar a logística e o comércio bilateral, garantindo padrões internacionais, intercâmbio de informações e redução de custos, beneficiando o crescimento e desenvolvimento regional. Em 2019, o comércio entre Brasil e Peru ultrapassou US$ 3,8 bilhões, indicando a importância dessa parceria.

O acordo também destaca a eficácia dos Certificados Digitais emitidos pelas infraestruturas oficiais de ambos os países: a Infraestrutura de Chaves-Públicas (ICP-Brasil) no Brasil e a Infraestructura Oficial de Firma Electrónica (IOFE) no Peru. Estas infraestruturas aderem aos mesmos padrões técnicos e

normas internacionais, permitindo o reconhecimento mútuo e ilustrando as vantagens do uso de assinatura eletrônica qualificada.

Em 2023, a Câmara dos Deputados aprovou o PDL – Projeto de Decreto Legislativo nº 929/21, que contempla um acordo de reconhecimento mútuo de certificados de assinatura digital no âmbito do Mercosul, assinado em 2019 pelos países do bloco. Este acordo permite o uso de certificados emitidos por certificadores habilitados em cada Estado parte do Mercosul tanto em transações particulares quanto com governos, conferindo-lhes o mesmo valor jurídico de assinaturas manuscritas. No entanto, certificados emitidos por certificadores licenciados fora do Mercosul, mesmo que aceitos em algum Estado membro, não estarão abrangidos pelo acordo.

Segundo noticiado pela Câmara dos Deputados (2023), a assinatura digital, utilizada em transações eletrônicas, garante a autenticidade do signatário por meio de procedimentos de segurança avançados. No Brasil, a assinatura digital qualificada utiliza a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), dependente de certificadores credenciados pelo Instituto Nacional de Tecnologia da Informação.

O acordo estabelece que cada certificador digital só pode emitir certificados no território onde foram credenciados ou licenciados, embora possam operar escritórios em outros países do Mercosul para atender cidadãos do Estado ao qual estão vinculados. Os certificados emitidos em um país do Mercosul terão validade jurídica em outro país membro, desde que emitidos por um prestador de certificação credenciado seguindo padrões internacionais.

Os certificados devem conter dados precisos para identificar o titular e o certificador, período de validade, informações para verificação de revogação, dados verificados no certificado digital, acessibilidade para verificação da assinatura e política de certificação aplicável. O acordo também prevê a harmonização das práticas de certificação, incluindo controle de acesso, separação de tarefas, segurança de dados e informações sensíveis, e integridade de dados e processos críticos.

Segundo o texto aprovado, os países signatários se comprometem a garantir um sistema de credenciamento e controle dos prestadores de serviços de certificação, incluindo auditorias e sanções. O tratamento de dados pessoais pelos certificadores deve respeitar a legislação de proteção do país onde têm sua licença ou credenciamento.

Conforme notícia divulgada pelo Mercosul (2019), a digitalização da economia tem transformado a maneira como cidadãos, empresas e governos interagem, especialmente com a crescente realização de serviços e negócios via

internet. Documentos tradicionalmente físicos, como a CNH – Carteira Nacional de Habilitação, Título de Eleitor, diplomas acadêmicos e certidões de nascimento, estão sendo substituídos por versões digitais, trazendo mais comodidade e segurança. Essa transição para o digital demanda mecanismos de segurança robustos para assegurar autenticidade, confidencialidade, integridade e validade jurídica dos documentos, o que é alcançado através da certificação digital.

Acrescenta que o certificado digital atua como uma identidade digital, ligando dados de verificação de assinatura a informações biográficas do titular. Ele utiliza algoritmos e técnicas criptográficas para garantir a relação incontestável entre o documento assinado e seu signatário, assegurando também a integridade do documento. Além de ser praticamente impossível de decifrar ou falsificar, a certificação digital oferece vários benefícios, como veracidade jurídica, agilidade e segurança nos processos, redução de custos administrativos e burocráticos, viabilização de comércio eletrônico seguro, implementação de políticas de governo digital e rastreabilidade eletrônica de transações.

O acordo de reconhecimento mútuo de assinaturas digitais no Mercosul permite o intercâmbio de documentos eletrônicos entre governos, empresas e cidadãos dos países membros. Esse acordo viabiliza a validação de documentos como diplomas acadêmicos digitais em todos os países do bloco, facilitando relações transfronteiriças e o reconhecimento de documentos oficiais.

Com esse acordo, será possível a troca de documentos fiscais e aduaneiros, assinatura de contratos entre empresas de diferentes países do bloco, rastreabilidade de produtos de livre comércio e reconhecimento automático de documentos eletrônicos emitidos a partir de certificados digitais das infraestruturas oficiais de cada país. Documentos assinados com certificado digital de uma infraestrutura credenciada nos países membros serão validados, simplificando processos e eliminando burocracias.

Segundo o Mercosul, para empresários brasileiros que atuam ou planejam atuar no mercado comum, isso representa uma facilitação substancial em negócios, validação de propostas comerciais e assinatura de contratos, garantindo a autenticidade e integridade de transações e documentos eletrônicos. Assim, a digitalização nas relações comerciais e sociais no Mercosul se torna uma realidade mais palpável e eficiente.

2.1.2 REGULAÇÃO ESTADUNIDENSE

Os Estados Unidos editaram o Electronic Signatures in Global and National Commerce Act (PUBLIC LAW 106–229 - E-Sign Act), promulgado em 30 de junho

de 2000, estabelecendo uma regra geral de validade para registros eletrônicos e assinaturas em transações que afetam o comércio interestadual ou internacional. Este ato permite o uso de registros eletrônicos para satisfazer qualquer estatuto, regulamento ou regra de direito que exija que tais informações sejam fornecidas por escrito, desde que o consumidor tenha consentido afirmativamente a tal uso e não tenha retirado tal consentimento (Estados Unidos: FDIC, 2023).

As disposições substanciais da Lei entraram em vigor em 1º de outubro de 2000, e os requisitos de retenção de registros se tornaram efetivos em 1º de março de 2001. O E-Sign Act considera válidos os acordos existentes entre um consumidor e uma instituição para entrega de informações eletronicamente.

Antes de obter o consentimento do consumidor, as instituições financeiras devem fornecer uma declaração clara e visível, informando sobre o direito de obter o registro em papel ou forma não eletrônica, o direito de retirar o consentimento e as condições, consequências e taxas em caso de tal retirada. Devem esclarecer se o consentimento se aplica apenas à transação específica que gerou a divulgação ou a categorias identificadas de registros que podem ser fornecidos no decorrer do relacionamento entre as partes.

Os consumidores devem ser informados sobre os requisitos de hardware e software necessários para acessar e reter registros eletrônicos. Se houver mudança nesses requisitos, criando um risco material de que o consumidor não possa acessar ou reter registros eletrônicos subsequentes, a instituição financeira deve fornecer uma declaração revisada dos requisitos de hardware e software e o direito de retirar o consentimento sem imposição de condições, consequências ou taxas.

Segundo a norma estadunidense, comunicações orais ou gravações de comunicações orais não se qualificam como registros eletrônicos. O *E-Sign Act* exige que as instituições financeiras mantenham registros eletrônicos que reflitam com precisão as informações contidas nos contratos aplicáveis, avisos ou divulgações, e que permaneçam acessíveis a todas as pessoas legalmente autorizadas a acessar pelo período exigido por lei em uma forma que possa ser reproduzida com precisão para referência posterior.

O *E-Sign Act* também estabelece definições para termos como "consumidor", "eletrônico", "agente eletrônico", "registro eletrônico", "assinatura eletrônica", "agência reguladora federal", "informação", "pessoa", "registro" e "transação". Segundo o Manual divulgado pelo FDIC - *Federal Deposit Insurance Corporation* sobre os direitos do consumidor de seguros, as regras finais adotadas pelo Federal Reserve Board em 2007 estabeleceram padrões uniformes para a entrega eletrônica de divulgações obrigatórias federalmente sob cinco

regulamentações de proteção ao consumidor. Estas regras finais fornecem orientações sobre o momento e a entrega de divulgações eletrônicas.

Além do *E-Sign Act*, o Título 21 CFR Parte 11 é uma seção do Código de Regulamentações Federais dos Estados Unidos que estabelece as normas da *Food and Drug Administration* (FDA) sobre registros eletrônicos e assinaturas eletrônicas. Comumente referido como Parte 11, define os critérios sob os quais registros e assinaturas eletrônicas são considerados confiáveis, seguros e equivalentes a registros em papel (ESTADOS UNIDOS: FDA, 2023).

Na prática, a Parte 11 é aplicável a fabricantes de medicamentos, fabricantes de dispositivos médicos, empresas de biotecnologia, desenvolvedores de produtos biológicos, Organizações de Pesquisa Clínica (CROs) e outras indústrias reguladas pela FDA, com algumas exceções específicas. Exige que essas entidades implementem controles, incluindo auditorias, validações de sistemas, trilhas de auditoria, assinaturas eletrônicas e documentação para softwares e sistemas envolvidos no processamento de dados eletrônicos que as regras de premissas da FDA exigem que sejam mantidos. Uma regra de premissa é qualquer requisito estabelecido no *Federal Food, Drug and Cosmetic Act, no Public Health Service Act* ou em qualquer regulamentação da FDA, excluindo a Parte 11.

A regra também se aplica a submissões feitas à FDA em formato eletrônico, mas não a submissões em papel por métodos eletrônicos. Especificamente, não exige a retenção de registros conforme a Parte 21 CFR 11 para rastreamentos por fabricantes de alimentos. A maioria dos fabricantes de alimentos não é explicitamente obrigada a manter registros detalhados, mas a documentação eletrônica mantida para HACCP[16] e requisitos semelhantes deve atender a essas normas.

Em 1999, a *Uniform Law Commission* editou o *Uniform Electronic Transactions Act* (UETA) pelo qual 49 estados, o Distrito de Columbia e as Ilhas Virgens dos EUA adotaram o UETA. Seu objetivo é harmonizar as leis estaduais relativas à retenção de registros em papel (especialmente cheques) e a validade das assinaturas eletrônicas. A *Uniform Law Commission*, também conhecida como *National Conference of Commissioners on Uniform State Laws*, formada em 1892, é uma associação não incorporada sem fins lucrativos, composta por advogados

16 Hazard analysis and critical control points (análise de perigos e pontos críticos de controle), ou HACCP, é uma abordagem sistemática preventiva para a segurança alimentar contra perigos biológicos, químicos e físicos nos processos de produção que podem tornar o produto final inseguro, e projeta medidas para reduzir esses riscos a um nível seguro.

nomeados por cada estado, pelo Distrito de Columbia, pelo *Commonwealth* de Porto Rico e pelas Ilhas Virgens dos EUA.

A UETA define, em sua Seção 2, "registro eletrônico" como um registro criado, gerado, enviado, comunicado, recebido ou armazenado por meios eletrônicos e "assinatura eletrônica" como um som, símbolo ou processo eletrônico associado a um registro e executado ou adotado por uma pessoa com a intenção de assinar o registro.

Pelas seções seguintes, o objetivo do ato se limita a transações relacionadas a negócios, comerciais (incluindo consumidores) e governamentais. Aplica-se a qualquer registro eletrônico ou assinatura eletrônica criada, gerada, enviada, comunicada, recebida ou armazenada, além de declarar que as transações não precisam estar em forma eletrônica, enquanto também afirma que o Ato se aplica apenas a transações entre partes que concordaram em conduzir transações por meios eletrônicos.

Também tem por objetivo facilitar e promover o comércio e as transações governamentais validando e autorizando o uso de registros e assinaturas eletrônicas, dando o reconhecimento legal a assinaturas eletrônicas, registros e contratos, afirmando que um registro ou assinatura não pode ser negado em eficácia legal ou aplicabilidade somente porque está em forma eletrônica. Exige que as informações estejam disponíveis para todas as partes, dando efeito aos registros eletrônicos e assinaturas eletrônicas.

A Seção 11 permite que um tabelião público e outros oficiais autorizados ajam eletronicamente, removendo efetivamente os requisitos de selo/carimbo, ressalvando que, em um processo, a evidência de um registro ou assinatura não pode ser excluída apenas porque está em forma eletrônica.

Segundo o American Bar Association (2020), ao abordar a utilização de assinaturas eletrônicas sobre acordos de negócios assinados eletronicamente, lembram que tradicionalmente, as partes envolvidas em transações comerciais e seus advogados raramente se reúnem no mesmo local para trocar acordos e documentos assinados manualmente; os fechamentos virtuais têm sido a norma. O *Uniform Electronic Transactions Act* (UETA) é lei na maioria das jurisdições dos Estados Unidos, e o *Electronic Signatures in Global and National Commerce Act* (E-SIGN) é uma lei federal. Ambas as leis estabelecem que uma assinatura não pode ser negada em efeito legal apenas por ser eletrônica.

O UETA e o E-SIGN são aplicáveis quando as partes de um contrato comercial sujeito a uma dessas leis concordam em usar uma assinatura eletrônica, que normalmente terá efeito legal. As assinaturas eletrônicas incluem assinaturas em e-mails, PDFs e faxes, e assinaturas fornecidas por processos de empresas

comerciais, como *DocuSign e Adobe Sign*, desde que sejam afixadas ou associadas ao acordo relevante com a intenção de assinar pelas pessoas que as fornecem.

Exceto para acordos regidos pelos Artigos 2 (vendas de mercadorias) e 2A (locações de mercadorias) do *Uniform Commercial Code* (UCC), o UETA e o E-SIGN não se aplicam a acordos na medida em que são regidos pelo UCC. O UCC rege apenas certos aspectos das transações dentro de seu escopo, deixando as demais questões a serem regidas por outras leis. As definições de "assinatura" no Artigo 1 e "autenticação" no Artigo 9 do UCC fornecem regras substancialmente iguais às do UETA e E-SIGN para o uso de assinaturas eletrônicas.

Às vezes, os acordos exigem que sejam assinados manualmente, assim como quaisquer emendas. Ao emitir um parecer devidamente executado sobre um acordo ou emenda assinada eletronicamente, o parecerista deve confirmar que o acordo não proíbe assinaturas eletrônicas.

Como prática habitual, os parecerem devidamente executados podem ser baseadas na suposição, que pode ser não declarada, de que todas as assinaturas são genuínas. Essa presunção de legitimidade se aplica tanto a assinaturas eletrônicas quanto manuais.

2.1.3 REGULAÇÃO EUROPEIA - EIDAS

Inicialmente abordada na parte teórica para justificar a importância das assinaturas eletrônicas como uma realidade jurídica, o Regulamento europeu (Regulation EU nº 910/2014, do Parlamento Europeu), merece ter a questão dogmática analisada neste capítulo.

A norma traz diversas definições envolvendo a identificação eletrônica, além de apresentar disposições gerais, identificação eletrônica e níveis de garantia associados a esquemas de identificação eletrônica. O objetivo principal é garantir o funcionamento adequado do mercado interno, estabelecendo um nível adequado de segurança para meios de identificação eletrônica e serviços de confiança. Isso inclui:

1. Estabelecer condições sob as quais os Estados-Membros reconhecem meios de identificação eletrônica de pessoas naturais e jurídicas sob um esquema de identificação eletrônica notificado de outro Estado-Membro.

2. Definir regras para serviços de confiança, particularmente para transações eletrônicas.

3. Criar um quadro legal para assinaturas eletrônicas, selos eletrônicos, carimbos de tempo eletrônicos, documentos eletrônicos, serviços de entrega registrada eletrônica e serviços de certificados para autenticação de sites.

O Regulamento é aplicável a esquemas de identificação eletrônica notificados por um Estado-Membro e provedores de serviços de confiança estabelecidos na União. Não se aplica a serviços de confiança usados exclusivamente dentro de sistemas fechados decorrentes da lei nacional ou acordos entre um conjunto definido de participantes, nem afeta a lei nacional ou da União relacionada à conclusão e validade de contratos ou outras obrigações legais ou processuais relacionadas à forma.

Quando a identificação eletrônica é necessária sob a lei nacional para acessar um serviço fornecido online por um órgão do setor público em um Estado-Membro, os meios de identificação eletrônica emitidos em outro Estado-Membro devem ser reconhecidos no primeiro Estado-Membro para fins de autenticação transfronteiriça para esse serviço online, desde que certas condições sejam atendidas. Essas condições incluem que os meios de identificação eletrônica sejam emitidos sob um esquema de identificação eletrônica incluído na lista publicada pela Comissão e que o nível de garantia dos meios de identificação eletrônica corresponda a um nível de garantia igual ou superior ao exigido pelo órgão do setor público relevante.

Um esquema de identificação eletrônica é elegível para notificação desde que atenda a várias condições, incluindo que os meios de identificação eletrônica sob o esquema possam ser usados para acessar pelo menos um serviço fornecido por um órgão do setor público que requer identificação eletrônica no Estado-Membro notificador, e que o esquema e os meios de identificação eletrônica emitidos atendam aos requisitos de pelo menos um dos níveis de garantia estabelecidos.

Os níveis de garantia de esquemas de identificação eletrônica notificados devem especificar os níveis baixos, substancial e/ou alto. Esses níveis de garantia devem atender a critérios específicos relacionados à confiança na identidade reivindicada ou afirmada de uma pessoa, caracterizados com referência a especificações técnicas, padrões e procedimentos relacionados, incluindo controles técnicos. A Comissão deve estabelecer especificações técnicas mínimas, padrões e procedimentos para esses níveis de garantia.

Os serviços de confiança tratam da supervisão e requisitos específicos para assinaturas eletrônicas. Os provedores de serviços de confiança são responsáveis por danos causados intencional ou negligentemente devido ao não cumprimento das obrigações sob o Regulamento. A intenção ou negligência de um provedor de serviços de confiança qualificado é presumida, a menos que ele prove o contrário. No entanto, os provedores não são responsáveis por danos resultantes do uso de serviços que excedam as limitações indicadas, se

essas limitações forem informadas antecipadamente aos clientes e reconhecíveis por terceiros.

Os Estados-Membros devem designar um órgão de supervisão responsável por supervisionar os provedores de serviços de confiança qualificados para garantir que eles e os serviços de confiança qualificados que fornecem atendam aos requisitos do regulamento. Esse órgão deve ter os poderes e recursos necessários para exercer suas tarefas e cooperar com outras entidades de supervisão.

Em relação às assinaturas eletrônicas, o regulamento estabelece que uma assinatura eletrônica não deve ser negada em efeito legal e admissibilidade como prova em processos legais apenas por ser eletrônica. Uma assinatura eletrônica qualificada tem o mesmo efeito legal de uma assinatura manuscrita e deve ser reconhecida em todos os Estados-Membros. O regulamento define requisitos específicos para assinaturas eletrônicas avançadas, incluindo a necessidade de estar vinculada de forma única ao signatário e ser capaz de identificar o signatário.

Os Estados-Membros não podem exigir, para uso transfronteiriço em um serviço online oferecido por um órgão do setor público, uma assinatura eletrônica em um nível de segurança mais alto do que a assinatura eletrônica qualificada. O Regulamento também detalha os requisitos para dispositivos de criação de assinatura eletrônica qualificados, a certificação desses dispositivos e o processo de validação de assinaturas eletrônicas qualificadas.

O Regulamento aborda serviços de preservação qualificados para assinaturas eletrônicas qualificadas, que devem ser fornecidos por provedores de serviços de confiança qualificados capazes de estender a confiabilidade da assinatura eletrônica além do período de validade tecnológica.

Segundo Turner (2016), o eIDAS foi criado para facilitar transações eletrônicas seguras e contínuas em toda a União Europeia (UE), fornecendo um ambiente regulatório que promove seu uso. O propósito do eIDAS é permitir que cidadãos e empresas usem seus esquemas nacionais de identificação eletrônica (eIDS) ao acessar serviços públicos em outros Estados-Membros da UE que utilizam eIDS. Ele define as condições sob as quais os Estados-Membros reconhecerão a identificação eletrônica dos usuários. O regulamento criou um padrão para assinaturas eletrônicas, carimbos de tempo, selos eletrônicos e outros meios de autenticação, incluindo certificação eletrônica e serviços de entrega registrada, conferindo a essas transações eletrônicas o mesmo status legal que se fossem realizadas em papel.

Afirma Turner que o escopo do eIDAS abrange esquemas de identificação eletrônica identificados pelo Estado-Membro e provedores de serviços de

confiança estabelecidos na UE. O regulamento não substitui disposições estabelecidas sob leis nacionais ou acordos legais entre partes definidas para serviços de confiança usados apenas em sistemas fechados, nem tem jurisdição sobre leis nacionais ou da UE relacionadas à validade e conclusão de contratos ou outras obrigações legais relacionadas à forma. Sob o eIDAS, uma assinatura eletrônica qualificada tem o mesmo efeito legal de uma assinatura manuscrita e pode ser usada como evidência em processos legais, desde que atenda aos requisitos para ser reconhecida como uma assinatura eletrônica qualificada. Todos os Estados-Membros devem reconhecer uma assinatura eletrônica qualificada como válida se ela for baseada em um certificado qualificado emitido por um dos Estados-Membros.

Para garantir sua validade, aponta Turner, as assinaturas eletrônicas avançadas devem atender a vários requisitos para provar sua autenticidade. A assinatura deve ser vinculada de forma única ao signatário, ser capaz de identificá-lo, ser criada usando dados de criação de assinatura eletrônica sob controle do signatário e ser capaz de identificar se os dados foram adulterados após a assinatura. Os Estados-Membros devem reconhecer tanto assinaturas eletrônicas qualificadas quanto avançadas que estejam em conformidade com os padrões exigidos. Eles também devem se abster de solicitar assinaturas de nível superior a uma assinatura eletrônica avançada para uso transfronteiriço de serviços online do setor público.

Complementa Turner que as assinaturas eletrônicas qualificadas são validadas por certificados emitidos por provedores de serviços de confiança qualificados. Ao emitir um certificado qualificado, o provedor de serviços de confiança deve verificar a identidade do signatário. Os provedores de serviços de confiança qualificados devem atender a requisitos rigorosos sob o eIDAS para garantir a validade dos certificados que emitem. Eles devem informar o órgão supervisor sobre quaisquer alterações em seus serviços de confiança, manter recursos financeiros adequados ou seguro de responsabilidade, treinar adequadamente os funcionários em procedimentos de segurança de dados, tomar medidas para prevenir falsificação e roubo de dados e armazenar dados em formato verificável, permitindo sua recuperação apenas com o consentimento da pessoa a quem se relaciona.

2.2 LEI MODELO DA UNCITRAL SOBRE COMÉRCIO ELETRÔNICO

A Assembleia Geral, relembrando sua resolução 2205 (XXI) de 17 de dezembro de 1966, que criou a Comissão das Nações Unidas sobre Direito Comercial Internacional com o mandato de promover a harmonização e unificação progressivas do direito do comércio internacional, enfatizando os interesses de todos os povos, especialmente dos países em desenvolvimento, no desenvolvimento extensivo do comércio internacional, observa o aumento no número de transações no comércio internacional realizadas por meio de intercâmbio eletrônico de dados e outras formas de comunicação, conhecidas como "comércio eletrônico", que envolvem o uso de alternativas aos métodos baseados em papel para comunicação e armazenamento de informações (ONU, 1996).

Recorda a ONU a recomendação sobre o valor legal dos registros de computador adotada pela Comissão em sua décima oitava sessão, em 1985, e a resolução 40/71 de 11 de dezembro de 1985, na qual a Assembleia solicitou aos governos e organizações internacionais que tomassem medidas, conforme apropriado, em conformidade com a recomendação da Comissão, a fim de garantir segurança jurídica no contexto do uso mais amplo possível do processamento automatizado de dados no comércio internacional.

Convencida de que o estabelecimento de uma lei modelo que facilite o uso do comércio eletrônico, aceitável para Estados com diferentes sistemas legais, sociais e econômicos, poderia contribuir significativamente para o desenvolvimento de relações econômicas internacionais harmoniosas, a Assembleia Geral nota que a Lei Modelo sobre Comércio Eletrônico foi adotada pela Comissão em sua vigésima nona sessão, após consideração das observações de governos e organizações interessadas.

Acreditando a ONU que a adoção da Lei Modelo sobre Comércio Eletrônico pela Comissão ajudará significativamente todos os Estados a aprimorarem sua legislação que rege o uso de alternativas aos métodos baseados em papel de comunicação e armazenamento de informações e na formulação de tal legislação onde ela atualmente não existe, a Assembleia Geral expressa seu apreço à Comissão das Nações Unidas sobre Direito Comercial Internacional por completar e adotar a Lei Modelo sobre Comércio Eletrônico, contida no anexo à Resolução nº 51/162, de 16 de dezembro de 1996, data da aprovação pela Assembleia Geral, e por preparar o Guia para a Promulgação da Lei Modelo.

O documento apresenta, como dito, um modelo que pode ser adotado internacionalmente, recomendando que todos os Estados considerem

favoravelmente a Lei Modelo quando promulgam ou revisam suas leis, tendo em vista a necessidade de uniformidade da lei aplicável às alternativas aos métodos baseados em papel de comunicação e armazenamento de informações, e também recomenda que todos os esforços sejam feitos para garantir que a Lei Modelo, juntamente com o Guia, se tornem geralmente conhecidos e disponíveis.

A introdução internacional do modelo da UNCITRAL (Comissão das Nações Unidas para o Direito Comercial Internacional) para a regulação do comércio eletrônico tem um impacto significativo, especialmente no que tange à regulamentação da assinatura eletrônica, visto que o comércio eletrônico é intrinsecamente global, com transações atravessando fronteiras nacionais. O modelo da UNCITRAL fornece uma base comum para os países desenvolverem suas legislações, facilitando assim o comércio internacional ao reduzir barreiras legais e aumentar a previsibilidade e a segurança jurídica nas transações eletrônicas.

A tecnologia está em constante evolução, e a legislação precisa ser suficientemente flexível para se adaptar a novas formas de comércio eletrônico e assinatura eletrônica. O modelo da UNCITRAL, com sua abordagem baseada em princípios, permite essa flexibilidade, adaptando-se às novas tecnologias sem a necessidade de frequentes revisões legislativas.

A Resolução se aplica a qualquer tipo de informação no formato de mensagem de dados utilizada no contexto de atividades comerciais. Ela define "mensagem de dados" como informações geradas, enviadas, recebidas ou armazenadas por meios eletrônicos, ópticos ou similares, incluindo, entre outros, a troca eletrônica de dados (EDI), e-mail, telegrama, telex ou telecópia. Também define termos como "originador" da mensagem de dados, "destinatário", "intermediário" e "sistema de informação".

Valente (2012) aborda a aceitação jurídica dos documentos eletrônicos, especialmente no contexto do comércio eletrônico, destacando iniciativas como a Lei Modelo da UNCITRAL. Explica a importância do documento como prova no Direito, destacando que o documento eletrônico é juridicamente válido, pois pode "ser traduzido por meio de programas de informática, que vai revelar o pensamento e a vontade de quem o formulou". O autor enfatiza a agilidade e a necessidade de registros rápidos nas relações modernas, onde a autenticidade e a comprovação de autoria são cruciais. Ricardo Lorenzetti, citado no artigo, aponta que o principal desafio na aceitação jurídica do documento eletrônico é a incerteza quanto à atribuição da autoria. Para superar essa barreira, setores

específicos da sociedade já estabelecem requisitos para a assinatura eletrônica, o principal meio de identificação do criador do documento eletrônico.

No que diz respeito à interpretação da Resolução, deve-se considerar sua origem internacional e a necessidade de promover uniformidade em sua aplicação, respeitando a boa-fé. As questões não expressamente resolvidas na lei devem ser conformadas com os princípios gerais em que se baseia. Brancer (2018) aponta que esta interpretação abrangente favorece a aplicação dos modelos em várias situações, como o "fornecimento ou troca de produtos ou serviços, distribuição, representação comercial, agência, factoring, leasing, serviços de engenharia e empreitada, licenciamento, investimento, financiamento, serviços bancários em geral".

O Artigo 5 da Resolução estabelece que as informações não devem ser negadas em termos de efeito legal, validade ou aplicabilidade, somente pelo fato de estarem no formato de mensagem de dados. No que se refere à escrita, a lei que exige que as informações estejam nesse formato é atendida por uma mensagem de dados se as informações nela contidas forem acessíveis para uso posterior.

O principal aspecto desta legislação diz respeito à assinatura. Quando a lei exige a assinatura de uma pessoa, esse requisito é atendido em relação a uma mensagem de dados se um método for utilizado para identificar essa pessoa e indicar sua aprovação das informações contidas na mensagem de dados. Esse método deve ser tão confiável quanto apropriado para o propósito pelo qual a mensagem de dados foi gerada ou comunicada, considerando todas as circunstâncias, incluindo qualquer acordo relevante. Este requisito se aplica independentemente de ser uma obrigação ou se a lei simplesmente estabelece consequências para a ausência de uma assinatura.

A assinatura eletrônica é um componente crítico do comércio eletrônico, pois garante a autenticidade e integridade das comunicações e transações eletrônicas. O modelo da UNCITRAL estabelece padrões para reconhecer a validade legal das assinaturas eletrônicas, o que aumenta a confiança dos participantes do mercado e ajuda a garantir a segurança jurídica.

O modelo oferece um guia para os países em desenvolvimento formularem sua legislação sobre comércio eletrônico e assinatura eletrônica[17]. Isso é

17 "A partir de 1997, vários países editaram normas sobre o comércio eletrônico, e adotaram as diretrizes da Lei Modelo, como a Alemanha e Itália em 1997, Espanha em 1999 e a França em 2000" (FERNANDES, 2012, p. 5).

crucial, pois muitos desses países estão em processo de digitalização de suas economias e precisam de um arcabouço legal que apoie esse desenvolvimento.

Uma abordagem excessivamente restritiva pode inibir a inovação, enquanto uma abordagem muito aberta pode levar à insegurança jurídica. O modelo da UNCITRAL busca equilibrar essas preocupações, proporcionando um ambiente regulatório que apoia tanto a segurança jurídica quanto a inovação no comércio eletrônico[18].

Considerando a diversidade dos sistemas jurídicos no mundo, o modelo da UNCITRAL é desenhado para ser compatível tanto com os sistemas de *common law* quanto com os de *civil law*, facilitando assim a sua adoção em diferentes contextos jurídicos.

Segundo Ribeiro (2011), o desafio enfrentado por organismos internacionais como a OMC (Organização Mundial do Comércio) e a UNCITRAL (Comissão das Nações Unidas para o Direito Comercial Internacional) consiste em regulamentar o comércio eletrônico sem infringir as liberdades dos governos locais. O objetivo é evitar que essa regulamentação se torne uma forma de protecionismo, especialmente em países que não são membros da OMC. A criação de regras para o comércio eletrônico poderia trazer vantagens significativas, expandindo o número de participantes nesta modalidade de comércio. No entanto, existem perspectivas, como a apresentada por Spadano, que sugerem que a OMC deveria focar apenas nos aspectos gerais do comércio eletrônico. Questões mais

18 A promulgação da Convenção sobre o Crime Cibernético, conhecida como Convenção de Budapeste, pelo Governo Federal brasileiro, visa combater os crimes cibernéticos no Brasil. Publicada no Diário Oficial da União em 12 de abril de 2023, essa adesão ao tratado internacional multilateral coloca o Brasil em sintonia com os esforços globais para enfrentar tais crimes, fortalecendo os laços de cooperação com parceiros estratégicos. A Convenção de Budapeste, firmada originalmente em 23 de 2001, proporciona às autoridades brasileiras um recurso adicional nas investigações de crimes cibernéticos e outras infrações penais que envolvam a obtenção de provas eletrônicas ou digitais armazenadas em outros países. Espera-se que esta adesão resulte em uma cooperação "mais intensa, rápida e eficaz". André Zaca Furquim, coordenador-geral de Cooperação Jurídica Internacional em Matéria Penal do Ministério da Justiça e Segurança Pública (MJSP), expressa a expectativa de que a Convenção aumentará gradativamente o número de pedidos de cooperação jurídica internacional. Ele destaca que "considerando que as investigações operadas no Brasil demandam, cada vez mais, provas eletrônicas que se encontram em outros países, esta Convenção irá facilitar e, portanto, encorajar os investigadores brasileiros a utilizar tal estratégia". Carolina Yumi, diretora do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do MJSP, afirma que a implementação integral da Convenção no Brasil trará resultados positivos, modernizando normativos e políticas de combate a crimes cibernéticos, além da coleta e preservação de provas digitais. Ela enfatiza que "A integral implementação da Convenção de Budapeste no Brasil trará resultados positivos ao país". A Convenção de Budapeste não apenas aprimora a cooperação internacional na instrução e elucidação de delitos virtuais, mas também impulsiona o Brasil a continuar desenvolvendo seu ordenamento jurídico e políticas relacionadas à criminalidade cibernética. Isso será feito com um equilíbrio entre intensificar a persecução penal e proteger dados pessoais, ressaltando a importância de se adaptar às mudanças trazidas pela era digital no âmbito da segurança e justiça. (BRASIL: Ministério da Justiça, 2023)

específicas, como contratação eletrônica, proteção dos direitos do consumidor e reconhecimento de assinaturas digitais, deveriam ser tratadas por outros organismos internacionais. Neste contexto, a UNCITRAL é mencionada pela autora como uma entidade que tem desenvolvido estudos mais específicos relacionados ao comércio eletrônico, em comparação com a OMC.

Segundo Polido e Silva (2017), reconhece-se a importância da regulação jurídica do comércio eletrônico internacional, enfatizando o papel desempenhado pela UNCITRAL (Comissão das Nações Unidas para o Direito Comercial Internacional) neste processo. Diante do ambiente desmaterializado e deslocalizado da internet, surgem exigências de certeza e segurança que têm sido históricas no Direito do Comércio Internacional. Desde a década de 1980, a UNCITRAL tem se debruçado sobre os desafios jurídicos apresentados pelos negócios realizados através de mensagens eletrônicas.

Entendem que a Comissão tem adotado fontes não vinculantes, como leis modelo e convenções, após estudo, discussão e negociação, buscando conciliar interesses diversos e tradições jurídicas e culturais. Esses esforços demonstram os avanços alcançados na harmonização e uniformização do Direito do Comércio Internacional, adaptando-se às particularidades do comércio eletrônico. A análise da evolução das iniciativas de regulação neste foro internacional é fundamental para compreender as bases jurídicas do comércio eletrônico internacional atual. Isso também oferece a oportunidade de identificar caminhos para suprir lacunas normativas em ordenamentos jurídicos nacionais, como o brasileiro.

Afirmam Polido e Silva que embora o Brasil tenha avançado em áreas como certificação digital e proteção ao consumidor no ambiente virtual, ainda há uma lacuna significativa no que se refere à regulamentação adequada dos contratos comerciais eletrônicos, seja no Código Civil, seja em legislação específica. O estabelecimento de marcos normativos que assegurem que os contratos celebrados eletronicamente tenham o mesmo valor jurídico, validade e eficácia dos contratos impressos, e que não representem barreiras ao desenvolvimento de novas tecnologias, é essencial[19]. Afirmam ser esse passo necessário para que o Brasil promova a confiança e a segurança jurídica no comércio internacional.

19 "No mundo atual, inconcebível a perda de tempo para obtenção de documentos e comprovações, tendo que se dirigir ao órgão ou empresa da qual se necessita a informação. Sua disponibilização já está se tornando imprescindível para a agilidade nos negócios. Por conseguinte, o contrato eletrônico, consequência lógica de toda essa movimentação no mundo da informática, também tem e deve se adaptar às novas regras, e por que não, conceitos" (LIMA, 2007, p. 230)

2.3 A MEDIDA PROVISÓRIA Nº 2.200-2/2001 E A INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA (ICP-BRASIL)

A regulamentação da chave pública para a assinatura de documentos digitais no Brasil passou a ser uma necessidade diante do crescimento rápido da internet nos anos 1990, emergindo diversas formas de negócios pelo meio digital com a expansão da tecnologia da informação e comunicação e o surgimento das questões jurídicas que dele se seguiram.

Apara a segurança jurídica, a implementação de uma chave pública regulamentada para assinaturas digitais proporciona um ambiente essencial para transações digitais. Isso favorece que as assinaturas em documentos eletrônicos sejam reconhecidas legalmente, conferindo-lhes a mesma validade e eficácia jurídica das assinaturas manuscritas.

A chave pública é um componente crucial na infraestrutura de chaves públicas (ICP ou PKI – *Public Key Infrastructure*), assegurando que a identidade do signatário e o conteúdo do documento não sejam alterados após a assinatura. Este é um elemento fundamental para a confiança nas transações digitais. Com a regulamentação adequada e abrangente, as pessoas encontram o necessário apoio jurídico, facilitando a promoção do comércio eletrônico e de serviços digitais, pois as partes envolvidas têm maior confiança na validade legal dos documentos assinados digitalmente, o que é particularmente importante em um mundo cada vez mais digitalizado, onde transações comerciais e interações governamentais estão sendo realizadas online.

A regulamentação brasileira insere o país no mercado global. A regulamentação alinhada com padrões internacionais possibilita a interoperabilidade e o reconhecimento de assinaturas digitais além das fronteiras nacionais. Isso é vital para o comércio internacional e para empresas brasileiras que operam globalmente.

O uso de assinaturas digitais também é visto sobre o aspecto econômico, pois reduz significativamente os custos operacionais relacionados à impressão, envio e armazenamento de documentos físicos. Também aumenta a eficiência dos processos, permitindo a execução e a conclusão de transações de forma mais rápida e eficiente. Deste modo, pode contribuir para a democratização do acesso a serviços digitais, sejam públicos ou privados, uma vez que facilita a realização de procedimentos legais, administrativos e comerciais de maneira digital, acessível a um número maior de cidadãos.

Com uma estrutura regulatória robusta, é possível combater mais eficazmente a fraude e o crime digital, pois a chave pública oferece mecanismos avançados de verificação de autenticidade. Nesta quadra de segurança, cria-se também um estímulo para a inovação e o desenvolvimento tecnológico, incentivando empresas e instituições a investirem em soluções digitais seguras e eficientes.

Em um cenário onde o Brasil está cada vez mais inserido em contextos regulatórios complexos, a regulamentação de chaves públicas realizada pela Medida Provisória nº 2.200-2, de 24 de agosto de 2001[20], assegura que as organizações cumpram com suas obrigações legais e normativas de maneira eficaz, promovendo, em face da base criptográfica, a cidadania digital, capacitando os cidadãos a exercerem seus direitos e deveres em um ambiente digital seguro e confiável.

Esta Medida Provisória representa um ponto de inflexão na legislação brasileira, estabelecendo a estrutura necessária para a segurança e a validade jurídica de documentos eletrônicos e transações online. Com a nova regulação, foi introduzido no ordenamento jurídico a Infraestrutura Brasileira (ICP-Brasil), ou seja, a PKI – *Public Key Infrastructure,* estabelecendo a autenticidade, integridade e validade jurídica de documentos em formato eletrônico. Isto implica que o Brasil reconhece a equivalência jurídica entre documentos eletrônicos e seus equivalentes físicos, desde que respeitadas as normas de segurança e autenticação definidas pela ICP-Brasil, sendo vital para a modernização e digitalização de diversos processos jurídicos e administrativos, permitindo uma maior eficiência e segurança nas transações eletrônicas.

Quanto à composição e organização da ICP-Brasil, foi criada uma estrutura hierárquica composta por várias autoridades. No topo, está a Autoridade Certificadora Raiz (AC Raiz), responsável por credenciar e supervisionar outras Autoridades Certificadoras (ACs) e Autoridades de Registro (ARs). Este sistema hierárquico confere unidade ao sistema, mantendo a segurança e a confiabilidade

20 O uso, por mais de 20 anos, de um instrumento normativo como a Medida Provisória, que até a presente data não foi convertida em Lei, é uma anomalia jurídica criada pela Emenda Constitucional nº 31, de 2001, que limitou o uso abusivo das medidas provisórias pelo Poder Executivo, inclusive na prática até então existente de sucessivas prorrogações, sem aprovação pelo Congresso Nacional. Porém, quando da promulgação da Emenda Constitucional nº 31, de 2001, o seu art. 2º dispunha que as "medidas provisórias editadas em data anterior à da publicação desta emenda continuam em vigor até que medida provisória ulterior as revogue explicitamente ou até deliberação definitiva do Congresso Nacional". Com efeito, no momento da promulgação da Emenda Constitucional nº 31, em setembro de 2001, estava em vigor a Medida Provisória 2.200-2 (já na segunda reedição), de 24 de agosto de 2001, permanecendo em vigor, por força do art. 2º da EC nº 31/2001, até a presente data.

da certificação digital, pois cada nível tem responsabilidades específicas e mecanismos de controle para garantir a autenticidade e a validade dos certificados digitais emitidos.

O Comitê Gestor da ICP-Brasil, como a autoridade gestora de políticas da Infraestrutura Brasileira, fica vinculado à Casa Civil da Presidência da República, tendo uma composição mista, incluindo representantes de vários ministérios e da sociedade civil. A inclusão de membros da sociedade civil, com mandatos de dois anos, permite a participação de diversos setores interessados, garantindo uma perspectiva mais ampla e representativa nas decisões. O Comitê Gestor é encarregado de coordenar a implementação e o funcionamento da ICP-Brasil, estabelecendo políticas, critérios e normas técnicas essenciais para o credenciamento de Autoridades Certificadoras (ACs) e Autoridades de Registro (ARs). O Comitê Gestor tem a função de estabelecer a política de certificação e as regras operacionais da Autoridade Certificadora Raiz (AC Raiz), o órgão no topo da cadeia de certificação. Também está encarregado de homologar, auditar e fiscalizar a AC Raiz e seus prestadores de serviço, favorecendo a manutenção da integridade e confiabilidade do sistema.

Quanto às competências específicas do Comitê Gestor, estas incluem a formulação de políticas e normas técnicas para certificados, credenciamento e autorização de funcionamento de ACs e ARs, bem como a gestão de acordos de certificação internacional, revelando seu papel central na administração e na garantia da interoperabilidade da ICP-Brasil com sistemas de certificação de outros países, o que é essencial para transações eletrônicas internacionais. A capacidade do Comitê Gestor de delegar atribuições à AC Raiz, conforme mencionado no parágrafo único do art. 4º, oferece flexibilidade operacional, permitindo que a AC Raiz desempenhe um papel mais ativo na gestão da ICP-Brasil quando necessário.

Ao delinear as funções e limitações da Autoridade Certificadora Raiz (AC Raiz) e das Autoridades Certificadoras (ACs) dentro da Infraestrutura Brasileira (ICP-Brasil), o art. 5º estabelece a AC Raiz como a autoridade máxima na cadeia de certificação, responsável por emitir e gerenciar os certificados das Autoridades Certificadoras subordinadas. A AC Raiz desempenha um papel fundamental na manutenção da integridade e confiabilidade do sistema de certificação digital, executando políticas, normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Suas funções incluem a emissão, expedição, distribuição, revogação e gerenciamento dos certificados, além de gerenciar listas de certificados emitidos, revogados e vencidos. A AC Raiz também é encarregada de

fiscalizar e auditar as ACs e as Autoridades de Registro (ARs), assegurando a conformidade com as diretrizes estabelecidas.

Importante notar que, conforme o Parágrafo único do art. 5º, é vedado à AC Raiz emitir certificados para o usuário final. Isso implica uma separação clara de responsabilidades dentro da cadeia de certificação, garantindo que a AC Raiz mantenha seu foco na supervisão e gestão das ACs, sem entrar em competição com elas no mercado de emissão de certificados para usuários finais.

O art. 6º especifica as responsabilidades das Autoridades Certificadoras. As ACs são entidades credenciadas para emitir certificados digitais, vinculando pares de chaves criptográficas aos respectivos titulares[21]. Suas funções incluem a emissão, expedição, distribuição, revogação e gerenciamento de certificados, além de disponibilizar listas de certificados revogados e outras informações pertinentes aos usuários. As ACs também são responsáveis por manter registros de suas operações.

O Parágrafo único do art. 6º destaca um aspecto crucial da segurança cibernética, estabelecendo que o par de chaves criptográficas deve ser gerado pelo próprio titular e que a chave privada de assinatura deve estar sob o controle exclusivo, uso e conhecimento do titular. Isso assegura a segurança dos dados e a privacidade do usuário, elementos fundamentais em um ambiente digital cada vez mais vulnerável a ameaças de segurança.

As Autoridades de Registro são fundamentais no processo de certificação digital, pois atuam como intermediárias entre os usuários e as Autoridades Certificadoras. As ARs são encarregadas de identificar e cadastrar usuários, o que inclui a verificação de sua identidade e a coleta de informações necessárias para o processo de certificação. As ARs encaminham solicitações de certificados às ACs e mantêm registros detalhados de suas operações. Este procedimento assegura a confiabilidade e a integridade do processo de emissão de certificados digitais[22].

A modificação introduzida pela Lei nº 14.063, de 2020, uma necessidade em razão do isolamento social provocado pela pandemia COVID-19, especifica que a identificação dos usuários pelas ARs deve ser feita presencialmente ou por meios que garantam um nível de segurança equivalente. Esta exigência de verificação de identidade reforça a segurança do processo de certificação,

21 As cadeias da ICP-Brasil cadastradas até 22 de julho de 2022 estão no endereço https://www.gov.br/iti/pt-br/assuntos/repositorio/cadeias-da-icp-brasil.

22 As Autoridades de Registro são vinculadas às Autoridades Certificadoras, sendo a estrutura disponibilizada no site do ITI – Instituto Nacional de Tecnologia da Informação no endereço https://estrutura.iti.gov.br/.

reduzindo o risco de fraudes e abusos, equilibrando a questão da segurança com a necessidade de isolamento social.

Tanto órgãos e entidades públicos quanto pessoas jurídicas de direito privado podem ser credenciados como ACs e ARs. Isso permite uma ampla gama de entidades para participar do sistema de certificação digital, desde que atendam aos critérios estabelecidos pelo Comitê Gestor da ICP-Brasil. A inclusão de entidades privadas e públicas como potenciais ACs e ARs expande a capacidade do sistema de certificação digital e promove uma maior adoção dessa tecnologia em diferentes setores.

Uma Autoridade Certificadora (AC) só pode certificar entidades no nível imediatamente subsequente ao seu na cadeia de certificação. Esta restrição ajuda a manter a estrutura organizada e segura da cadeia de certificação. Exceções a essa regra, como acordos de certificação lateral ou cruzada, são permitidas, mas apenas com a aprovação prévia do Comitê Gestor da ICP-Brasil. Essa flexibilidade permite adaptações necessárias para a cooperação internacional ou situações específicas, mantendo, no entanto, o controle e a supervisão do Comitê Gestor.

Por disposição expressa contida no art. 10, os documentos eletrônicos têm sua validade reconhecida tal como os documentos públicos ou particulares tradicionais, abrindo caminho para uma maior digitalização de processos administrativos e jurídicos. O artigo estabelece que as declarações feitas em documentos eletrônicos, produzidos com a utilização de certificados da ICP-Brasil, são presumidas verdadeiras em relação aos signatários, em conformidade com o Código Civil, sendo importante para a sua aceitação e confiabilidade no meio jurídico.

O § 2º do art. 10 ainda ressalta a flexibilidade no reconhecimento de documentos eletrônicos, visto que menciona que a utilização de outros meios para comprovar a autoria e a integridade de documentos eletrônicos, mesmo aqueles que não utilizam certificados emitidos pela ICP-Brasil, é permitida desde que as partes envolvidas os aceitem como válidos ou sejam aceitos pela pessoa a quem o documento é oposto. Permite-se certa flexibilidade no uso de tecnologias de certificação digital, adequando-se às necessidades de diferentes contextos e partes.

Sobre a aplicação da norma em contextos tributários, os arts. 11 a 15 da Medida Provisória nº 2.200-2/2001, definem o status e as responsabilidades do Instituto Nacional de Tecnologia da Informação (ITI) e delineiam sua estrutura organizacional. A utilização de documentos eletrônicos em contextos tributários deve estar em conformidade com o Código Tributário Nacional. Tal referência enfatiza a necessidade de alinhar os procedimentos eletrônicos com as normas

tributárias existentes, assegurando que os documentos eletrônicos sejam reconhecidos e tratados adequadamente sob a legislação tributária.

O ITI é como uma autarquia federal vinculada ao Ministério da Ciência e Tecnologia, com sede no Distrito Federal, sendo designado como a Autoridade Certificadora Raiz da ICP-Brasil. Essa configuração formaliza a posição do ITI como uma entidade governamental central na infraestrutura de certificação digital do Brasil, responsável por supervisionar e coordenar a emissão de certificados digitais no país.

É atribuído ao ITI a função de fiscalização dentro do âmbito da ICP-Brasil, incluindo a capacidade de aplicar sanções e penalidades conforme previsto em lei, sendo importante para garantir a conformidade e a integridade do sistema de certificação digital, assegurando que as normas e regulamentos sejam seguidos pelas entidades participantes. O art. 15 detalha a estrutura organizacional do ITI, incluindo uma Presidência, Diretorias de Tecnologia da Informação e de Infraestrutura, além de uma Procuradoria-Geral.

Por fim, é conferida pela norma autonomia ao ITI para contratar serviços de terceiros, uma faculdade importante para complementar suas capacidades internas e assegurar a eficiência operacional. Permite-se ao ITI buscar expertise externa e soluções tecnológicas avançadas, essenciais para a manutenção e o desenvolvimento da infraestrutura de chaves públicas no Brasil.

A Associação dos Magistrados do Estado de Rondônia publicou um artigo sobre a ICP-Brasil (Associação dos Magistrados do Estado de Rondônia, 2010), onde destaca a oferta da segurança e redução de custos com a tecnologia. Inicialmente, discorda da visão de que o certificado digital ICP-Brasil não é uma solução completa para todos os problemas de segurança da informação, citando a Medida Provisória 2.200-2/01, que admite outras formas de comprovação de autenticidade e integridade de documentos eletrônicos. Destaca que o ICP-Brasil, composto por várias autoridades, incluindo o Comitê Gestor da ICP-Brasil e o Instituto Nacional de Tecnologia da Informação (ITI), existe para assegurar a autenticidade, integridade e validade jurídica dos documentos eletrônicos, enfatizando a natureza nacional da Medida Provisória, aplicável a todo o território brasileiro, e não apenas a entidades federais.

Argumenta que apenas o certificado ICP-Brasil garante a validade jurídica de documentos eletrônicos, reconhecendo quem os assinou e garantindo que não sofreram alterações. No entanto, reconhece a existência de outros certificados digitais, cuja eficácia depende da aceitação entre as partes envolvidas, em que pese não estarem respaldados por uma infraestrutura pública.

Todavia, a aceitação de certificados digitais fora da Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil) ou de outra infraestrutura reconhecida pelo Brasil suscita preocupações significativas no que tange à segurança jurídica. Embora a flexibilidade de aceitar certificados não emitidos pela ICP-Brasil possa parecer benéfica em termos de inclusão e diversidade tecnológica, ela introduz incertezas quanto à autenticidade, integridade e validade jurídica dos documentos eletrônicos. Esses certificados, ao não estarem subordinados a uma infraestrutura pública rigorosamente controlada e auditada, como a ICP-Brasil, podem não atender aos mesmos padrões rigorosos de segurança, o que aumenta o risco de fraudes e comprometimentos de dados. A dependência da aceitação mútua entre as partes envolvidas nos torna vulneráveis a disputas e contestações legais, inclusive envolvendo o direito de terceiros, podendo resultar em complexidades processuais adicionais e em uma confiança diminuída no comércio eletrônico e nas transações digitais.

A Associação também aborda a utilização de transações eletrônicas no Brasil sem certificados digitais, como no caso das transações bancárias, argumentando que isso não implica na prescindibilidade do certificado digital ICP-Brasil. Ele menciona o alto custo das fraudes bancárias, que poderiam ser reduzidas com a implementação do certificado digital.

Destaca a utilidade do certificado digital ICP-Brasil em facilitar o acesso a serviços governamentais online, como o Centro Virtual de Atendimento ao Contribuinte da Receita Federal, e menciona sua integração no novo Registro de Identidade Civil (RIC). Também aponta a importância do certificado digital ICP-Brasil no Sistema Público de Escritura Digital (Sped) e no serviço Infojud, que atende solicitações judiciais em tempo significativamente reduzido.

Vê a Associação com criticidade a ideia de que a regulamentação dos certificados digitais pelos tribunais constitua uma delegação da fé pública dos atos judiciais, argumentando que a fé pública permanece com o Judiciário. Lembra que a Lei nº 11.419/2009, que dispõe sobre a informatização do processo judicial, permite duas formas de assinatura eletrônica (art. 1º, § 2º, III), mas o certificado digital ICP-Brasil é preferível devido à sua maior segurança em comparação com sistemas baseados em login e senha.

Ressalta que as deficiências tecnológicas e a incompatibilidade entre sistemas não devem ser vistas como um obstáculo à adoção do certificado digital, mas sim como um incentivo para aprimorar e homogeneizar os sistemas processuais eletrônicos, enfatizando os benefícios do certificado digital ICP-Brasil, como agilidade, redução de custos e menor impacto ambiental.

Entrando no debate sobre a importância do ICP-Brasil, Garcia (2010), em resposta às críticas de Sérgio Tejada sobre a limitada segurança da informação oferecida pelo certificado digital, argumenta a favor da robustez e da validade jurídica do ICP-Brasil, destacando seu papel essencial na garantia de autenticidade e integridade dos documentos eletrônicos.

Garcia refuta a ideia de Tejada de que outras formas de assinatura digital, autorizadas pela MP 2.200-2/2001, sejam tão seguras quanto o ICP-Brasil. Ele afirma, "se outros formatos de assinatura digital fossem inseguros, a norma legal não os autorizaria". Garcia defende que a infraestrutura do ICP-Brasil, composta por diversas autoridades e um modelo administrativo sólido, é crucial para a segurança digital no Brasil. Ele ressalta que a MP é uma norma nacional, aplicável em todo o território brasileiro, e que apenas o certificado ICP-Brasil assegura a validade jurídica dos documentos eletrônicos, pois garante quem os assinou e que não sofreram modificações.

O autor também aborda a questão dos outros certificados digitais, mencionando que sua validade depende da aceitação entre as partes, o que introduz uma insegurança intrínseca e uma natureza mais privada do que pública, ao contrário do ICP-Brasil. Ele argumenta que a dependência da aceitação mútua pode levar a disputas legais e enfraquece a segurança jurídica oferecida por um certificado oficial.

Garcia destaca a utilidade prática do ICP-Brasil, como no acesso a serviços da Receita Federal e em transações bancárias. Ele critica a visão de que certificados digitais são dispensáveis, mencionando os altos custos associados a fraudes bancárias que poderiam ser mitigados com a implementação do ICP-Brasil.

Em seu artigo, enfatiza a integração do ICP-Brasil em sistemas governamentais como o Registro de Identidade Civil (RIC) e o Sistema Público de Escritura Digital (Sped), ressaltando sua eficiência e segurança. Garcia defende que a regulamentação dos certificados digitais pelos tribunais não implica em uma delegação da fé pública judicial, mas sim um cumprimento da MP 2.200-2/01.

Por fim, Garcia aborda a interoperabilidade dos certificados digitais ICP-Br, desmistificando a noção de que os certificados digitais dos advogados devam ser exclusivamente emitidos pela OAB. Ele defende a modernização e homogeneização dos sistemas processuais eletrônicos, enfatizando os benefícios do ICP-Brasil, como agilidade, redução de custos e menor impacto ambiental. Garcia conclui destacando a necessidade de viver com informações apropriadas em uma sociedade da informação.

Seus argumentos são sólidos, visto que se deve observar a importância e a utilidade prática do ICP-Brasil, ressaltando sua contribuição significativa para

a segurança e confiabilidade em diversos setores, especialmente em serviços governamentais e transações bancárias. A implementação do ICP-Brasil poderia mitigar significativamente os custos associados a fraudes bancárias, evidenciando a necessidade de um sistema de certificação digital robusto e confiável. A integração eficiente do ICP-Brasil em sistemas governamentais vitais como o Registro de Identidade Civil (RIC) e o Sistema Público de Escritura Digital (Sped) é importante não apenas em razão da eficiência, mas também a segurança reforçada que o sistema oferece. A questão da regulamentação dos certificados digitais pelos tribunais não deveria ser feita de forma autônoma, desvinculado do sistema da ITI, visto que sua estrutura técnica favorece a integridade e segurança valiosas para a justiça. Adicionalmente, a modernização e a uniformização dos sistemas processuais eletrônicos e a interoperabilidade dos certificados ICP-Br, são medidas que promovem a agilidade, a redução de custos e o menor impacto ambiental, consistindo em passos cruciais para uma adaptação eficiente à crescente sociedade da informação.

2.4 TEORIA GERAL DA VONTADE E SUA ADAPTAÇÃO AO MEIO DIGITAL

Neste subcapítulo, examinaremos a questão da manifestação de vontade no ambiente virtual, fazendo uma exploração meticulosa da interseção entre a teoria jurídica tradicional da vontade e sua aplicação no dinâmico e evolutivo contexto digital.

Para tanto, iniciamos com uma análise da teoria geral da vontade no direito contratual, um pilar fundamental do direito privado. Este estudo revisita os conceitos essenciais como a autonomia da vontade, o consentimento livre e esclarecido, e a intenção das partes, elementos cruciais na formação dos contratos tradicionais. Esta abordagem baseada em princípios serve como alicerce para entender como a vontade é concebida e interpretada no direito contratual e estabelece um ponto de partida para sua adaptação ao meio digital.

Avançamos para os desafios específicos da expressão da vontade em ambientes digitais. Faremos uma abordagem de questões sobre autenticidade e identificação do declarante, compreensão e consentimento em relação aos termos contratuais digitais, especialmente como uso de interfaces de usuário e sistemas na manifestação eletrônicos da vontade. Esta seção é vital para entender as complexidades e nuances que surgem quando a vontade é expressa não mais em papel, mas em bytes e telas.

O papel das assinaturas digitais, como uma forma de manifestação de vontade em contratos digitais, é então examinado. Discutiremos como as assinaturas digitais são tratadas no que diz respeito à validade do consentimento e à formação de contratos, destacando seu papel fundamental na segurança jurídica e na validade contratual no âmbito digital.

Não menos importante como objeto de investigação, temos a questão da adaptação da teoria da vontade às novas tecnologias, como contratos inteligentes, sendo crucial para compreender como os conceitos tradicionais de vontade e consentimento se adaptam (ou enfrentam desafios) diante de tecnologias que automatizam e, em certos aspectos, redefinem a formação e execução de contratos.

Também se focalizam os desafios da formação contratual online, começando com a autenticidade e identificação das partes em contratos online, sendo importante para o entendimento sobre como as tecnologias são empregadas para assegurar que as partes de um contrato sejam autenticamente identificadas, um aspecto crucial para a segurança jurídica do contrato.

A compreensão e o consentimento em acordos digitais são então analisados, destacando os desafios em assegurar que as partes entendam claramente os termos do contrato e concedam um consentimento válido, especialmente em contextos onde os termos são apresentados eletronicamente. Isso leva à necessidade de discussão das interfaces e usabilidade na formação de contratos, enfocando na sua técnica para a formação de contratos, e abordamos os desafios legais e regulatórios enfrentados na formação de contratos online, incluindo a análise das legislações existentes e as lacunas legais.

A detecção de vícios da vontade em contratos digitais é importante para este contexto, devendo-se proceder com a identificação e análise dos vícios da vontade - como erro, dolo, coação, e fraude - no contexto digital. São relevantes os desafios associados à prova de vícios da vontade em ambiente virtual, o impacto das tecnologias e interfaces na manifestação da vontade, e estratégias para prevenir e remediar vícios da vontade em contratos digitais.

Este subcapítulo oferece uma visão abrangente e detalhada dos múltiplos aspectos que compõem a manifestação de vontade no ambiente virtual, estabelecendo um diálogo entre a teoria jurídica tradicional e as inovações e desafios do mundo digital. É uma contribuição essencial para o entendimento e aprimoramento da segurança jurídica na formação de contratos digitais, um tema de importância crescente na era digital, permitindo a continuidade da pesquisa nos capítulos seguintes concernentes à validade dos contratos digitais, a segurança jurídica diante da proteção do consumidor.

2.4.1 FUNDAMENTOS DA TEORIA GERAL DA VONTADE NO DIREITO CONTRATUAL

Sobre a teoria tradicional da vontade no direito contratual, a questão envolve conceitos que podem ser inferidos a partir da legislação brasileira, especialmente quanto à autonomia da vontade, o consentimento livre e esclarecido, bem como a questão da subjetividade concernente à intenção das partes na formação do contrato.

O art. 421 do Código Civil menciona a liberdade contratual quando cita os limites para o seu exercício. Ao que parece, a compreensão da liberdade envolve não apenas a definição dos seus limites como também a investigação do comportamento das partes durante a relação jurídica. Destaca Schreiber (2021, p. 792-800) que a intenção das partes em um contrato não se limita a declarações iniciais, mas se renova continuamente através de ações práticas, defendendo a ideia de que o contrato é uma relação dinâmica, caracterizada por múltiplas ações e atitudes.

Quando analisamos a teoria com base na legislação alemã, verifica-se a importância das declarações de vontade no contexto dos negócios jurídicos, conforme delineado pelo Código Civil Alemão (BGB). Schwab e Löhnig (2012, p. 21), destacam que "*der wesentliche, aber nicht einzige Bestandteil der Rechtsgeschäfte ist die Erklärung einer oder mehrerer Personen*"[23] Esta afirmação sublinha a centralidade das declarações de vontade no direito civil, reconhecendo que, embora sejam fundamentais, não são os únicos elementos constituintes dos negócios jurídicos. De acordo com este paradigma, o BGB estabeleceu regras específicas para as declarações de vontade nos §§ 116 a 144, sendo aplicáveis a todas as declarações no âmbito dos negócios jurídicos, incluindo ofertas de contrato e aceitações de contrato, assim como ofertas de compra e aceitações de compra.

Segundo os autores, o foco nas declarações de vontade reflete uma compreensão de que tais declarações são cruciais para a formação, alteração e dissolução de relações jurídicas. Ao estabelecer regras específicas para elas, o BGB busca garantir clareza e segurança jurídica nos processos que envolvem negócios jurídicos. Esta abordagem é consistente com os princípios gerais do direito civil, que valorizam a autonomia da vontade e a necessidade de expressar

23 Tradução livre: o elemento essencial, mas não único, dos negócios jurídicos é a declaração de uma ou mais pessoas.

claramente as intenções para que os negócios jurídicos sejam válidos e eficazes, o que não afasta o surgimento de problemas relativos à intenção e aos vícios.

Sobre o enfoque limitante da liberdade, Pereira (2001, p. 14) lembra que todo negócio jurídico possui requisitos que, caso não observados, resulta em sua ineficácia. Alguns são gerais, submetendo-se a todos os atos negociais, e outros específicos, regendo particularmente alguns contratos. Distribui os requisitos em três grupos: subjetivos, objetivos e formais. Quanto aos subjetivos, estes concernem à capacidade das partes em contratar, de modo que apenas aqueles com aptidão para emitir validamente sua vontade atendem este grupo. Porém, indica que não se trata de uma capacidade genérica, pois exige-se que nenhuma das partes seja "portadora de inaptidão específica para contratar". Em outras situações, a lei estabelece restrições à liberdade de contratar, segundo Pereira. Estas restrições legais alguns chamam de impedimento, para não serem confundidas com a incapacidade geral, esta inerente ao sujeito e não por força da norma.

Aos discorrer sobre o princípio da autonomia da vontade, Gomes (2009, p. 25-27) enfatiza sua importância e aplicabilidade. O princípio é caracterizado como o poder dos indivíduos de gerar efeitos jurídicos através de suas declarações de vontade, permitindo-lhes criar direitos ou obrigações. Essa autonomia se manifesta especialmente nos contratos, onde se observa grande extensão de sua aplicação.

O autor define a autonomia da vontade como um aspecto da liberdade de contratar, que inclui a auto regência de interesses, a livre discussão das condições contratuais e a escolha do tipo de contrato. Esta liberdade se manifesta em três aspectos: a liberdade de contratar propriamente dita, a liberdade de estipular o contrato e a liberdade de determinar o conteúdo do contrato. "A liberdade de contratar propriamente dita é o poder conferido às partes contratantes de suscitar os efeitos que pretendem, sem que a lei imponha seus preceitos indeclinavelmente".

Ressalta a prevalência das disposições legais de caráter supletivo ou subsidiário em matéria contratual, que se aplicam em caso de silêncio ou carência das vontades particulares. Isso permite que os contratantes regulem seus interesses de forma diversa ou até oposta à prevista em lei, dentro dos limites legais imperativos.

Diferencia entre leis coativas, que ordenam ou proíbem algum ato, e leis supletivas, que suplementam a vontade do indivíduo. No Direito Contratual, predominam as normas supletivas, oferecendo ampla liberdade para que as partes ajam em sua esfera. Contrapondo a ideia de que a autonomia das partes

é mais aparente do que real, o autor argumenta que a liberdade de contratar é um postulado prático e não apenas teórico, sendo utilizada conforme a conveniência das partes.

Sobre a questão das leis coativas no Direito Contratual, reconhece a necessidade de normas imperativas tanto por razões políticas quanto por injunções técnicas. Embora o amplo alcance do princípio da autonomia da vontade, são indispensáveis normas inderrogáveis pela vontade das partes em qualquer regime contratual.

O conceito de consentimento no contexto dos contratos, segundo Pereira (2001, p. 15), constitui requisito subjetivo e fundamental para a formação de um contrato válido. O autor destaca que o contrato nasce de um acordo de vontades ou consentimento das partes, e define o consentimento como a "aptidão para consentir". A expressão "consentimento" é compreendida como o acordo de vontades (*cum* + *sentire*), geralmente referindo-se à manifestação de vontade de cada um dos contratantes.

O consentimento é descrito como abrangendo três aspectos essenciais para a formação de um contrato válido: 1. acordo sobre a existência e natureza do contrato. Por exemplo, se uma parte deseja aceitar uma doação e a outra deseja vender, não há contrato; 2. acordo sobre o objeto do contrato. Se as partes divergem quanto ao objeto do contrato, este não pode ser considerado válido; 3. acordo sobre as cláusulas que compõem o contrato. Se houver divergência em um ponto substancial, o contrato não pode ter eficácia.

Pereira ressalta que para haver consentimento, é necessário a emissão da vontade de duas ou mais pessoas; a vontade de uma só pessoa é insuficiente. Ele aborda exceções a essa regra, como a autocontratação, que normalmente não é admitida como contrato, mas sim como uma declaração unilateral de vontade. No entanto, alguns modernos aceitam a autocontratação, decompondo as duas vontades presentes no ato, mas ressalvam seu caráter excepcional, principalmente na presença de representação e anuência expressa do representado.

Outra objeção discutida por Pereira é a questão do papel assinado em branco, que ele argumenta não valer como contrato, mas como prova de um contrato já anteriormente concluído. Ele enfatiza que se fosse uma modalidade de contratar, encontraria obstáculo na lei civil, que sujeita o ato ao arbítrio exclusivo de uma das partes. Esta problemática do papel assinado em branco enfrenta novos desafios diante dos contratos digitais que serão examinados posteriormente.

Esta liberdade para a contratação é expressa mediante o consentimento, que tem como pressupostos a própria liberdade e a compreensão daquilo que se deseja.

A conformação entre a compreensão do sujeito e a manifestação apresentada leva à necessidade de interpretação, inclusive com presunções legais, as próprias regras de interpretação, assim como o dever de comportamento com a invocação da probidade e boa-fé.

A problemática do consensualismo remete à questão probatória, sendo muitas vezes submetidas à decisão do poder judiciário que se debruça sobre a validade da manifestação de vontade através de elementos muitas vezes sutis ou que podem ser fonte de novos questionamentos. Neste contexto, a distribuição probatória pode ter relação direta ou ser influenciada pela natureza dos fatos, onde as condições gerais das relações, condições específicas e anormalidades sãos distinções que revelam a sua importância (DUARTE, 2020, p. 231).

Este ponto é relevante porque destaca a importância da intenção e do consentimento nas transações contratuais, tanto no meio físico quanto digital. A lei civil impõe restrições à validade de contratos baseados na arbitrariedade unilateral, o que se aplica tanto aos contratos tradicionais quanto aos digitais.

A liberdade contratual e o consentimento são pressupostos essenciais para a formação de contratos válidos. A adequação entre a compreensão das partes e a manifestação de vontade expressa é crucial, exigindo interpretação e, muitas vezes, a aplicação de presunções legais e regras de interpretação, bem como o princípio da probidade e boa-fé. Esses aspectos são fundamentais tanto em contratos assinados fisicamente quanto em documentos digitais.

Em contextos digitais, a questão probatória se torna ainda mais complexa devido à natureza intangível dos documentos e à facilidade de manipulação, tendo esta padronização influência na própria distribuição do ônus da prova.

Quando a validade do contrato digital é questionada judicialmente, a tendência é que o ônus da prova possa recair sobre quem fez uso do documento digital, inclusive sob o aspecto do consentimento informado e consciente. Isso se deve à necessidade de assegurar a autenticidade, a integridade e a não-repudiação dos documentos eletrônicos, elementos essenciais para a confiança nas transações digitais. Portanto, aqueles que se beneficiam da conveniência e eficiência dos documentos digitais também podem ter a responsabilidade de provar a legitimidade dessas transações quando questionadas.

A discussão levantada demonstra a complexidade da prova em contratos digitais e a importância de considerar tanto as nuances legais quanto tecnológicas no uso de assinaturas digitais. A evolução do direito contratual e das práticas probatórias no ambiente digital revela um campo desafiador e de vital importância para a segurança jurídica nas transações eletrônicas.

2.4.2 DESAFIOS NA EXPRESSÃO DA VONTADE EM AMBIENTES DIGITAIS

A expressão da vontade no meio digital apresenta desafios novos, complexos em razão da interdisciplinaridade com enfoque no Direito e na cidadania digital. É importante tratar sobre questões relacionadas, que vão desde a autenticidade e identificação do declarante até a compreensão e consentimento em relação a termos contratuais digitais.

É fundamental garantir que a declaração de vontade provenha efetivamente da pessoa que alega tê-la emitido. Conquanto tradicionalmente o papel tenha sido utilizado como instrumento do negócio jurídico, facilitando a comprovação de sua existência, inclusive com a assinatura dos contraentes demonstrando o consentimento com as disposições pactuadas, a contratação pelo meio digital remete à uma nova forma de identificação das pessoas, visto que os dígitos trabalhados pelos sistemas de informação não são personalizáveis em si, de modo a constituírem uma marca pessoal do sujeito que subscreve.

Em seu estudo sobre os contratos consumeristas eletrônicos, Tang (2015, p. 123-127) aborda o desafio que o comércio eletrônico (e-commerce) representa para o conceito tradicional de "escrita" em contratos. Tradicionalmente, um documento escrito é caracterizado por sua acessibilidade repetida, legibilidade, durabilidade, precisão e imutabilidade, servindo como uma forma confiável de demonstrar o consentimento genuíno das partes em um contrato e garantir que nenhum termo seja uma surpresa injusta. No entanto, no e-commerce, os contratos e seus termos são dados eletrônicos armazenados em *hard drives, sticks* de memória, cartões de memória, servidores, discos e outros hardwares, sendo intangíveis e ilegíveis sem o hardware e software apropriados.

Lembra a autora que alguns países adotaram a abordagem do "equivalente funcional" para reconhecer que a forma eletrônica satisfaz o requisito de "escrita" se tiver a função básica semelhante à da "escrita" baseada em papel. Esta abordagem fornece a flexibilidade necessária para aplicar o antigo termo legal na nova era da internet. Por exemplo, o Artigo 25(2) do Regulamento Bruxelas I Recast[24] especifica que "qualquer comunicação por meios eletrônicos que forneça um registro durável do acordo deve ser equivalente à 'escrita'".

24 Regulamento (UE) Nº 1215/2012 sobre jurisdição e o reconhecimento e execução de sentenças em matérias civis e comerciais (reformulação) [2012] JO L351/1, Artigos 17 – 19. Regulamento disponível em https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:en:PDF.

No entanto, a forma visual do contrato eletrônico requer a assistência de uma tela de computador e software de conversão apropriado, e erros de programa ou mecânicos podem fazer com que o contrato apareça como um código hash na tela[25].

Pimentel (2023b, p. 299-300) discute a importância e o funcionamento do método de hash criptográfico, destacando seu papel como uma "impressão digital virtual" dos dados cifrados. Esse método serve para verificar a integridade dos dados transmitidos em redes, permitindo identificar se houve alguma alteração nos conteúdos encriptados. Essencialmente, o hash criptográfico é uma ferramenta eficaz no controle da integridade comunicacional, especialmente em modelos de criptografia assimétrica, onde é crucial atestar se os dados transportados permaneceram intactos ou se houve violação na chave pública utilizada.

Para ilustrar o conceito, Pimentel fornece um exemplo prático: ao encriptar a expressão "devido processo legal", um sistema de criptografia gera uma sequência de caracteres alfanuméricos ininteligíveis (por exemplo, "aPf527 cmQ=*") que só pode ser decodificada pelo destinatário utilizando a chave criptográfica apropriada. Dessa forma, a mensagem original ("devido processo legal") é recuperada no dispositivo do receptor. Paralelamente, a função hash codifica a mesma mensagem não com o objetivo de esconder seu conteúdo, mas para assegurar sua autenticação e integridade, gerando um hash único (exemplo, "6f4doc3b7Kc%887jd5$") que representa a integridade dos dados originais.

Assim, o registro durável por si só não garante a legibilidade de um contrato eletrônico e não protege adequadamente as partes de serem vinculadas por um termo de contrato imprevisto. Alguns países, como a China, definem "escrita" de forma mais ampla, incluindo mensagens eletrônicas que são capazes de expressar seu conteúdo de forma tangível.

Afirma a autora que a definição mais apropriada de contrato eletrônico deve combinar durabilidade e legibilidade. Mesmo que a forma original de um contrato eletrônico seja duvidosa, ele ainda pode ser válido se for "evidenciado por escrito". Isso significa que, embora o contrato eletrônico esteja em uma forma intangível sem papel, seu conteúdo pode ser facilmente impresso em um documento de papel, servindo como um registro preciso dos termos acordados.

25 Um código hash é geralmente visualizado como uma sequência de caracteres alfanuméricos. Esta sequência é o resultado de uma função hash que converte dados de entrada (que podem variar em tamanho e tipo) em um conjunto de caracteres de tamanho fixo.

O Regulamento Bruxelas I Recast citado pela autora exige mais do que apenas gravar algo permanentemente em papel para permitir acesso repetido; também requer que os termos do contrato sejam registrados de maneira que forneçam aviso suficiente às partes sobre sua existência e conteúdo, visando garantir que o consentimento genuíno seja realmente alcançado entre as partes.

Segundo Tang, o e-commerce traz questões inovadoras sobre a qualidade da escrita. Por exemplo, um contrato eletrônico pode ser originalmente em letra pequena ou difícil de ler, mas a maioria dos navegadores da web permite que o usuário ajuste o tamanho do texto. Muitas cláusulas de jurisdição não são mostradas diretamente quando o contrato é concluído, mas podem aparecer em uma tela atualizada ou em uma janela pop-up após clicar em um hiperlink.

Finalmente, destaca a autora ser importante notar que a assinatura não é obrigatória para a validade formal do Regulamento Bruxelas I Recast. Uma cláusula de escolha de foro concluída online não será invalidada simplesmente porque as partes não assinaram. A maioria dos contratos eletrônicos com consumidores é concluída combinando um PIN[26] e clicando no ícone "Eu aceito". Assinaturas eletrônicas serão reconhecidas e válidas se tiverem a mesma funcionalidade das assinaturas tradicionais. O Regulamento da UE sobre Identificação Eletrônica, adotado em 2014, fornece uma base comum para o reconhecimento legal de assinaturas eletrônicas nos Estados-Membros.

Constitui um desafio atual assegurar que os usuários compreendam os termos aos quais estão consentindo, especialmente em ambientes digitais onde os contratos podem ser extensos ou complexos. Estudos sobre a clareza e transparência dos termos contratuais em plataformas digitais e a efetividade das políticas de "clique para concordar" são realizados, sendo destacado que um problema comum na era digital: a aceitação passiva de contratos e termos de uso sem uma leitura ou compreensão adequada.

Este fenômeno é ilustrado pelo modelo predominante de "clique para concordar", que limita as opções do usuário a aceitar os termos integralmente para acessar um serviço ou rejeitá-los e ficar sem o serviço. Esse modelo não oferece espaço para discussão ou negociação dos termos. Uma pesquisa citada no texto revela que uma grande maioria de pessoas (97 %) na faixa etária de 18 a 34 anos concorda com esses termos sem lê-los. Isso sugere uma falta significativa de consciência ou interesse em entender o conteúdo desses contratos digitais, o que pode ter implicações importantes em termos de consentimento

26 Personal Identification Number - PIN

informado e proteção dos direitos do usuário. Este é o desafio crescente na era digital: garantir que o consentimento para termos de uso e contratos digitais seja informado e genuíno (Lepan, 2020; Dresch e Freitas, 2021).

Considera-se o design de interfaces e sistemas influencia para a manifestação da vontade, podendo levar a consentimentos inadvertidos ou desinformados. Sobre o impacto que o design pode ter na manifestação de vontade, Marzullo, Oliveira e Monat (2021) discutem a importância e o potencial de uma abordagem mais visual e interativa na apresentação de termos de contratos eletrônicos, especialmente no contexto do e-commerce. A argumentação se baseia na necessidade de testes com usuários para avaliar a compreensão de informações visuais e esquemáticas, em comparação aos contratos eletrônicos tradicionais.

Os resultados iniciais sugerem que tanto consumidores quanto empresas poderiam se beneficiar dessa abordagem mais dinâmica. Os autores mencionam que "os primeiros resultados sugerem que o e-commerce poderia se beneficiar de uma abordagem mais visual e interativa para a apresentação de seus termos". A pesquisa destaca a *Design Science Research* como uma metodologia eficaz para estruturar e organizar conceitos de diversas áreas, visando criar artefatos que resolvam problemas específicos. Essa abordagem é particularmente relevante para o design de contratos eletrônicos, uma questão que ganhou importância com a expansão do e-commerce durante a pandemia da COVID-19.

Os autores ressaltam a importância de ampliar as discussões sobre a fundamentação teórica do design de informação e de interação, para que pesquisas futuras possam desenvolver uma base sólida no campo da Visualização de Contratos.

Destacam que o debate sobre essas práticas de design não se limita apenas à área de design em si, mas também pode influenciar a jurisprudência nas Cortes Judiciárias. Isso inclui a aplicação de fundamentos teóricos que podem alterar a natureza de contratos de adesão, como a utilização de formulários interativos para escolha e interação direta com o usuário.

Os autores expressam a expectativa de que a pesquisa em visualizações de contratos possa fornecer a usuários e empresas uma ferramenta de comunicação mais eficiente. Esta ferramenta deveria conscientizar e orientar sobre direitos e deveres, potencialmente reduzindo a quantidade de litígios virtuais. O objetivo é que as visualizações de contratos não apenas melhorem a compreensão dos termos, mas também promovam uma comunicação mais clara e efetiva entre as partes envolvidas.

Esta abordagem dialoga com o "*Visual Law*" ou "*Legal Desing*", uma iniciativa piloto divulgada pelo Professor e Desembargador do Trabalho Sérgio Torres

Teixeira que usa a linguagem gráfica para facilitar a compreensão do julgamento, buscando tornar a comunicação jurídica mais acessível e transparente para os cidadãos. Em Pernambuco, o Tribunal Regional do Trabalho da Sexta Região (TRT6) implementou essa abordagem, utilizando recursos visuais como infográficos, fluxogramas, vídeos e ícones em um dos seus processos.

Neste contexto, o desembargador Sergio Torres Teixeira, do TRT6, em parceria com a professora e pesquisadora Paloma Mendes Saldanha, realizou um projeto piloto. Durante o julgamento de um recurso, foi incluído um resumo gráfico junto ao acórdão publicado. Esse resumo tinha o objetivo de facilitar a compreensão do resultado do julgamento, embora o acórdão mantivesse sua formatação e elementos legais tradicionais. O desembargador Sergio Torres enfatizou a importância dessa iniciativa para a comunicação entre a justiça e o cidadão, expressando sua expectativa de que ela contribua para o acesso mais amplo e efetivo à justiça e democratize o diálogo na Justiça do Trabalho. Ele destacou: "esperamos com isso seguir no trilho da permanente busca pela concretização do amplo e efetivo acesso à justiça, democratizando ainda mais o diálogo na Justiça do Trabalho".

Para a compreensão da interface do usuário, Rodrigues (2023) também destaca sua crescente importância no sucesso de produtos e serviços digitais. À medida que a tecnologia avança, as expectativas dos usuários quanto à facilidade de uso e qualidade do design também aumentam, enfatizando o papel crucial dos profissionais de UI (User Interface) e UX (User Experience) Design. Explica que o UI Design foca na criação da aparência visual e da interação de um produto digital, como aplicativos ou sites. Ele envolve todos os elementos visíveis e interativos que permitem a interação dos usuários com o produto. O objetivo é criar uma interface visual atrativa e fácil de usar, melhorando a eficiência e eficácia da interação do usuário com o produto. UI Designers são responsáveis por desenvolver layouts, ícones, botões, menus, tipografia e outros elementos visuais, assegurando uma interface coesa e intuitiva.

Já o UX Design se concentra em criar experiências de usuário satisfatórias e significativas em produtos digitais. Ele abrange todos os aspectos da experiência do usuário, incluindo a interação com o produto, a eficácia das tarefas executadas, a qualidade da interação e as emoções do usuário durante o uso. O UX Designer deve considerar o público-alvo do produto, objetivos do usuário, acessibilidade, contexto de uso e restrições técnicas. Suas responsabilidades incluem realizar pesquisas com usuários, criar protótipos, realizar testes de usabilidade e colaborar com outros profissionais para garantir uma experiência consistente em todo o produto digital.

Assim, de acordo com Rodrigues, enquanto o UI Design é responsável pela estética e interação visual de um produto, o UX Design foca na experiência geral do usuário. Ambos são considerados pelo Autor como fundamentais para o sucesso de um produto digital, visando aumentar a satisfação e a fidelidade do cliente.

Estes ambientes digirais devem ser integrados aos princípios do direito de forma que a manifestação de vontade seja justa e equitativa. Cria-se um desafio para o legislador a adequação das normas jurídicas no contexto digital e o desenvolvimento, para a academia, das discussões a respeito da cidadania digital. Pimentel (2023) aborda profundamente o conceito de cidadania digital e o estado algorítmico de direito. A cidadania digital, no contexto da era tecnológica, é entendida como uma situação jurídica que busca assegurar acesso irrestrito à internet, livre de barreiras ou discriminação. Este acesso é visto como fundamental para a construção do estado algorítmico de direito, um termo cunhado por Moisés Barrio Andrés, que enfatiza a importância de tecnologias automatizadas que reforçam a legitimidade dos estados democráticos. Pimentel salienta que a algoritmização afeta não apenas o direito, mas também o próprio estado e a digitalização da vida social. O estado algorítmico de direito, inserido no contexto do liberalismo e da social democracia, surge como contraponto ao estado tecno-feudal caracterizado pela governança opaca e desterritorializada das grandes corporações tecnológicas. Por isso, explica que a cidadania digital é sustentada por normas jurídicas como a Lei de Acesso à Informação, o Marco Civil da Internet, a Lei Geral de Proteção de Dados, e leis voltadas para grupos específicos, como idosos e pessoas com deficiência. Ressalta-se a proteção do direito à internet e a defesa contra a invasão da privacidade pelas aplicações de Internet. Cita Pimentel exemplos internacionais como a Constituição chilena, que protege os direitos cerebrais como fundamentais na era digital, e a *Online Safety Bill* do Reino Unido, focada na segurança online, especialmente de crianças, contra conteúdos nocivos.

O autor defende que a cidadania digital é um conceito em construção que requer atenção da academia e dos operadores do direito para garantir benefícios de algoritmização a todos, sem discriminação. Destaca-se a necessidade de atenção aos "vulneráveis cibernéticos", abordando tanto o direito material quanto o processual, ampliando o acesso e a acessibilidade no ambiente digital, especialmente para pessoas com deficiência, através de tecnologias assistivas.

Propõe Pimentel um modelo de cidadania digital baseado em pilares como acesso universal à internet, tratamento isonômico dos usuários, proteção de dados pessoais, incluindo dados neuronais, e alfabetização digital para todos.

Enfatiza a importância da garantia de acesso a sistemas judiciais tecnológicos para usuários com deficiência e a proteção cerebral, particularmente para crianças e pessoas com deficiência.

Ele menciona a falta de legislação específica no Brasil para a proteção de dados neurais, não obstante existirem leis como o ECA e o Estatuto da Pessoa com Deficiência que oferecem alguma proteção, indicando a necessidade de evolução legislativa para abranger plenamente a proteção cerebral e digital dos cidadãos.

No contexto do presente trabalho, é valioso o argumento da necessidade de educação digital mencionada por Pimentel. A alfabetização digital, reconhecida como um pilar essencial da cidadania digital, é crucial para a compreensão efetiva dos contratos digitais e para uma manifestação de vontade genuína e informada. Em um mundo cada vez mais interconectado e tecnologicamente avançado, a capacidade de entender e navegar pelo espaço digital se tornou uma habilidade fundamental, especialmente no contexto jurídico e contratual.

Contratos digitais, muitas vezes complexos e repletos de jargões técnicos e legais, além de estarem em idiomas muitas vezes desconhecidos para a maioria, requerem um nível de compreensão digital para que os indivíduos possam efetivamente avaliar os termos e condições a que estão concordando. A alfabetização digital capacita os indivíduos a entenderem não apenas o conteúdo textual de um contrato digital, mas também as implicações dos aspectos técnicos, como o uso de dados, consentimento para compartilhamento de informações, e os direitos e obrigações que surgem desses acordos.

A capacidade de expressar uma vontade genuína e informada em ambientes digitais é diretamente influenciada pelo nível de alfabetização digital de uma pessoa, de modo que sem o entendimento adequado de como as plataformas digitais funcionam e dos termos dos contratos que elas propõem, os indivíduos podem inadvertidamente concordar com condições que não compreendem ou que não refletem suas verdadeiras intenções. Isso é particularmente relevante em questões de privacidade e consentimento de dados, onde a falta de compreensão pode levar a violações involuntárias de privacidade pessoal.

Não se trata apenas de uma ferramenta para compreender e concordar com contratos, pois é também um meio de capacitar indivíduos a navegarem com autonomia no espaço digital, permitindo a avaliação dos riscos e responsabilidades inerentes. Isso inclui a habilidade de identificar potenciais fraudes, entender as implicações de segurança digital e utilizar os recursos digitais de maneira eficaz e segura. Deve-se concordar com Pimentel no sentido de que a promoção da alfabetização digital é uma forma de combater a desigualdade digital. Indivíduos

que não possuem habilidades digitais adequadas são desproporcionalmente desfavorecidos no acesso a serviços, informações e oportunidades disponíveis online. Isso é especialmente crítico em contextos jurídicos, onde a falta de habilidades digitais pode impedir o acesso a direitos legais ou a capacidade de entender e exercer esses direitos adequadamente.

Torna-se cada vez mais premente a necessidade regulatória, isso em razão da natureza do ambiente cibernético, que tem a rápida evolução da tecnologia como uma de suas mais importantes características, de modo que alfabetização digital não seja um objetivo estático, mas um processo contínuo de aprendizagem e adaptação.

Esta alfabetização digital ultrapassa as fronteiras nacionais, isso em razão da natureza global da internet, onde a manifestação de vontade pode estar sujeita a diferentes jurisdições e legislações. Qualquer avanço na cidadania digital depende da análise das implicações legais transnacionais e desenvolvimento de marcos regulatórios internacionais ou harmonizados.

2.4.3 MANIFESTAÇÃO DE VONTADE NO AMBIENTE DE TELEMARKETING

Os contratos digitais muitas vezes emergem de interações que se iniciam em ambientes presenciais ou através de canais de comunicação de áudio. Esta prática, embora eficiente para o estabelecimento inicial de entendimentos e acordos, carrega consigo particularidades que demandam atenção especial, sobretudo no que tange à formalização desses acordos em contratos de adesão digitais.

Esses contratos, caracterizados pela sua natureza de adesão, onde uma das partes define os termos e condições, deixam pouca ou nenhuma margem para negociação por parte do aderente. A peculiaridade desses contratos reside na forma como os termos discutidos e acordados previamente, muitas vezes em conversas presenciais ou através de canais de áudio, são transpostos para o documento final. Essas discussões preliminares, que podem envolver uma série de persuasões e negociações verbais, acabam por se cristalizar em registros de áudio que, por sua vez, formam a base para os termos e condições dos contratos digitais.

Um dos métodos mais disseminados de discussão e negociação que precede a formalização de contratos digitais é o telemarketing. Esta técnica, amplamente utilizada por empresas para alcançar potenciais clientes, merece

uma análise detalhada devido à sua grande difusão e impacto na formação de contratos digitais. O telemarketing, por natureza, opera através de canais de áudio, onde operadores treinados utilizam táticas de persuasão para convencer os clientes a aderirem a serviços ou produtos. Estas conversas, apesar de efêmeras, são cruciais, pois os termos acordados verbalmente são posteriormente transcritos para contratos de adesão digitais.

A transição das negociações conduzidas via telemarketing para contratos digitais formais apresenta desafios únicos, especialmente no que se refere à fidelidade com que os métodos persuasivos são representados nos documentos contratuais. Esta etapa é crítica, pois qualquer discrepância entre o que foi discutido e o que é formalizado no contrato pode levar a mal-entendidos e, potencialmente, a disputas judiciais. Além disso, a natureza unilateral dos contratos de adesão, onde os termos são estabelecidos por uma das partes, coloca uma responsabilidade adicional sobre os fornecedores de serviços ou produtos para garantir que os contratos reflitam com precisão os acordos alcançados durante as conversas de telemarketing.

O telemarketing, enquanto técnica de formação de contratos digitais, exige uma atenção meticulosa tanto na etapa de negociação quanto na transcrição desses acordos para o formato digital. É imperativo que as empresas empreguem práticas rigorosas de documentação e revisão para assegurar que os contratos digitais de adesão reflitam fielmente as discussões precedentes, resguardando assim a integridade do processo contratual e protegendo os interesses de todas as partes envolvidas.

Rosenzweig (2000, p. 11-19) delineia quatro pontos fundamentais que distinguem o sucesso do insucesso em campanhas de telemarketing, uma técnica de venda direta que envolve a realização de chamadas telefônicas não solicitadas, ou "*cold calls*", para potenciais clientes. Este método é frequentemente visto tanto por vendedores quanto por prospectos como desafiador e, às vezes, incômodo, mas é defendido pelo autor como uma estratégia essencial de vendas devido à sua eficácia em identificar e qualificar rapidamente potenciais clientes.

O primeiro ponto enfatizado é a importância de se comunicar com a pessoa certa. Rosenzweig argumenta que, tal como nas vendas presenciais, o sucesso no telemarketing depende crucialmente de alcançar o decisor chave. Ele sugere técnicas específicas para identificar e se conectar com esses indivíduos, destacando a necessidade de superar o medo da rejeição e evitar apresentações a quem não tem o poder de decisão de compra.

O segundo ponto aborda a transição das observações iniciais para uma abordagem baseada em perguntas. Após capturar o interesse do prospecto nos

primeiros segundos da chamada, o vendedor deve focar em fazer perguntas que permitam entender melhor as necessidades e potenciais de venda, movendo-se eficazmente para uma discussão sobre como seus produtos ou serviços podem se encaixar nas necessidades do cliente.

O terceiro ponto trata da dinâmica de falar, ouvir e fechar a venda. Rosenzweig destaca que vender, e por extensão o telemarketing, é uma habilidade que se aprimora com prática e estudo. Ele reforça a importância de adaptar o estilo de venda ao próprio perfil e às necessidades do cliente para maximizar as chances de sucesso.

O quarto ponto trata do perfeccionismo, promovendo a ideia de aprender com os erros e prosseguir sem se prender ao passado (feedback). Rosenzweig argumenta que uma fixação em ser perfeito pode levar à inação e à depressão, dois grandes inimigos da produtividade em vendas. Em vez disso, ele encoraja um foco na melhoria contínua e na aceitação de falhas como parte do processo de crescimento.

O aperfeiçoamento desta técnica pode levar a resultados indesejáveis, visto que o consumidor, após refletir ou se informar melhor sobre a chamada, poderá exercer o direito ao arrependimento.

O Instituto Brasileiro de Defesa do Consumidor (IDEC) aborda a problemática do telemarketing abusivo, uma prática recorrente com ligações indesejadas e frequentes, muitas vezes sem qualquer relação prévia entre empresa e consumidor. Revela-se que 92 % dos consumidores relatam não ter vínculo com as empresas que os contatam, e 99 % afirmam não ter dado consentimento para receber tais ofertas. O IDEC destaca o impacto negativo dessas ligações, incluindo a perda de oportunidades importantes, e aponta para a exploração de consumidores vulneráveis, como idosos.

Embora não exista uma legislação específica regulando o telemarketing, algumas regras da Senacon e da Anatel visam proteger os consumidores. Destacam-se iniciativas como a lista de bloqueios "Não Me Perturbe", o uso obrigatório do prefixo 0303 para chamadas de telemarketing e 0304 para cobranças, além de medidas contra os chamados "*robocalls*". Segundo o IDEC, a Anatel também propõe a criação de um portal público para consulta das empresas responsáveis por ligações indesejadas e a suspensão da atuação de empresas que praticam telemarketing abusivo.

Para se defender, sugere o IDEC que os consumidores se cadastrem no site "Não Me Perturbe", procurem o Procon para denúncias e utilizem o novo canal do Ministério da Justiça para denúncias de telemarketing. Além disso, é possível consultar o site "Qual Empresa Me Ligou" para identificar a origem das

chamadas e realizar reclamações diretas às empresas. Em casos não resolvidos, ações judiciais são uma opção.

O IDEC enfatiza a necessidade de uma regulamentação específica para o setor de telemarketing, defendendo que apenas ligações com consentimento expresso e específico dos consumidores deveriam ser permitidas. A organização atua para pressionar por legislações eficazes que protejam os direitos dos consumidores contra o telemarketing abusivo.

2.4.4 ASSINATURAS DIGITAIS COMO MANIFESTAÇÃO DE VONTADE

O reconhecimento legal das assinaturas digitais como manifestação de vontade de uma pessoa específica constitui não só um avanço, mas também se tornou uma necessidade. Normas como as citadas anteriormente do Parlamento Europeu, do Mercosul, dos Estados Unidos, do Brasil, dentre outros, constituem um importante passe na segurança jurídica necessária para a validade dos negócios jurídicos.

Juridicamente, adota-se a teoria da equivalência legal das assinaturas digitais em comparação com as assinaturas manuscritas tradicionais, como citado nas normas anteriores.

Segundo Gillies (2008, p. 26-27), o desenvolvimento global do comércio eletrônico e as respostas legais a este fenômeno, as mudanças nas leis e políticas para acomodar a crescente atividade comercial online, isso ao longo dos últimos quatorze anos, tornou-se evidente um mercado global de bens e serviços, com empresas e consumidores realizando contratos eletronicamente. Este desenvolvimento internacional do comércio e do aumento de disputas entre empresas e consumidores em diferentes jurisdições foi identificado como o "berço de conflitos internacionais". Em resposta ao aumento do comércio eletrônico, governos nacionais introduziram novas leis ou adaptaram leis e políticas existentes.

A União Europeia adotou a Diretiva de Comércio Eletrônico para regular a prestação de Serviços da Sociedade da Informação no campo coordenado. A introdução desta diretiva levou a mais diretivas que regulam aspectos específicos de atividades de comércio eletrônico, como assinaturas eletrônicas, venda à distância e marketing à distância de serviços financeiros ao consumidor. Nos Estados Unidos, foram introduzidos *o Uniform Electronic Transactions Act* (UETA) e o *Uniform Computer Information Transactions Act* (UCITA) para regular a atividade de comércio eletrônico. Os tribunais estadunidenses também buscaram adaptar

as regras de jurisdição pessoal para se aplicarem às atividades comerciais do réu conduzidas por comércio eletrônico em um estado específico.

Aponta a autora que organizações internacionais como a Conferência de Haia sobre Direito Internacional Privado, OECD, WIPO e UNCITRAL realizaram projetos, escreveram relatórios e diretrizes que direcionaram uma abordagem nacional e particularista à regulação legal de contratos realizados por comércio eletrônico. Este movimento global reflete uma resposta jurídica à evolução do comércio eletrônico, evidenciando a necessidade de adaptação das leis para abranger as complexidades e desafios trazidos por esta forma de comércio.

A formação de contratos, especialmente no contexto do comércio eletrônico, é um elemento importante para o estudo da validade da assinatura digital. Esta análise é imprescindível, pois a assinatura digital é um componente fundamental na concretização de contratos eletrônicos, servindo como mecanismo de autenticação e confirmação da intenção das partes envolvidas. A maneira como um contrato é formado, incluindo a incorporação e aceitação de uma assinatura digital, determina em grande medida a sua validade legal, sendo de destaque a compreensão dos princípios que regem a formação de contratos eletrônicos, tais como o consentimento, a oferta e aceitação, e a intenção de estabelecer relações jurídicas, é essencial para avaliar a eficácia legal das assinaturas digitais, isso para que a validade da assinatura digital, por sua vez, represente um indicador chave da autenticidade e da força vinculativa do contrato.

Ao tratar da formação dos contratos eletrônicos, Tang (2015, p. 16), enfoca especificamente nas questões de validade e nas abordagens legais para lidar com esses desafios no contexto do direito internacional privado. O autor destaca que um contrato eletrônico não é apenas concluído de forma diferente, mas também por um procedimento distinto, o que levanta questões específicas quanto à sua validade.

Esta questão é crucial no conflito de leis, pois determina a validade de uma cláusula de escolha de lei ou de foro. Do ponto de vista do direito internacional privado, a validade de um contrato ou de termos contratuais pode ser abordada de duas maneiras: através da abordagem de escolha de lei ou pela abordagem de lei uniforme. Se for adotada a primeira opção, a dificuldade potencial é que, caso o sistema de lei relevante designado pela regra de escolha de lei não tenha legislação atualizada para e-contracts, o contrato pode ser invalidado irrazoavelmente, independentemente da intenção de ambas as partes. Se for adotada a segunda opção, surge a questão de como as regras uniformes poderiam ser estabelecidas para regular e-contracts e se tal compromisso poderia ser alcançado por diferentes países.

Argumenta que a complexidade e os desafios na formação de contratos eletrônicos devem tratar das abordagens legais adequadas e atualizadas para lidar com a natureza única e as peculiaridades do comércio eletrônico no âmbito do direito internacional privado. A escolha entre a abordagem de lei escolhida e a lei uniforme representa um dilema central na busca por soluções eficazes para regular os contratos eletrônicos em um ambiente globalizado.

A garantia da segurança das assinaturas digitais depende da correta aplicação do método criptográfico, sendo importante a utilização de uma infraestrutura de chaves públicas, criptografia assimétrica. Outras formas de validar uma manifestação de vontade pode ser fonte de questionamentos diversos, colocando em risco a segurança jurídica do contrato.

A decisão do Superior Tribunal de Justiça (STJ) no REsp 1.495.920/DF reflete um importante marco na jurisprudência brasileira sobre a validade jurídica dos contratos assinados eletronicamente. Segundo o Superior Tribunal:

> "Esta Corte Superior possui jurisprudência no sentido de que, diante da nova realidade comercial, em que se verifica elevado grau de relações virtuais, é possível reconhecer a força executiva de contratos assinados eletronicamente, porquanto a assinatura eletrônica atesta a autenticidade do documento, certificando que o contrato foi efetivamente assinado pelo usuário daquela assinatura" (REsp 1.495.920/DF, Rel. Ministro Paulo de Tarso Sanseverino, Terceira Turma, julgado em 15/5/2018, DJe 7/6/2018).

Esta decisão representa um reconhecimento significativo do papel crescente das tecnologias digitais no ambiente comercial. O STJ, ao validar a força executiva de contratos firmados eletronicamente, demonstra uma adaptação do sistema jurídico às mudanças trazidas pela era digital. A assinatura eletrônica é considerada uma ferramenta confiável para atestar a autenticidade de documentos, garantindo que o contrato foi assinado pela parte a quem a assinatura pertence.

Este posicionamento do STJ é um reflexo da evolução do direito em resposta às novas dinâmicas comerciais e sociais, oferecendo segurança jurídica nas transações digitais, sendo particularmente relevante no contexto de crescentes transações comerciais online, onde a agilidade e a eficiência proporcionadas pela assinatura eletrônica são fundamentais. A aceitação da assinatura eletrônica como meio de prova de contratos evidencia um alinhamento com as práticas globais e atende às demandas da sociedade digital contemporânea, assegurando a validade e a eficácia dos contratos celebrados eletronicamente.

2.4.5 CONTRATOS INTELIGENTES

Os contratos inteligentes representam uma inovação significativa no campo jurídico e tecnológico, transformando a maneira como as partes manifestam sua vontade em acordos digitais. Esses contratos, que operam na tecnologia blockchain, permitem a execução automática e a verificação de termos contratuais sem a necessidade de intermediários, prometendo garantir maior segurança, eficiência e transparência. Ao codificar as cláusulas contratuais em um programa de computador, os contratos inteligentes oferecem uma nova dimensão à expressão da vontade contratual, onde as condições pré-determinadas e acordadas pelas partes são cumpridas de forma automatizada, refletindo uma evolução no modo como as transações e os acordos legais são concebidos e executados no mundo digital.

Segundo Lo, Wang e Lee (2021, pág. 189-193), o conceito de contratos inteligentes foi primeiramente discutido no artigo de Nick Szabo, em 1997, intitulado "The Idea of Smart Contracts" ("A Ideia de Contratos Inteligentes"). Szabo propôs a incorporação de cláusulas contratuais em ativos digitais através de contratos inteligentes. Para que sejam úteis em ativos digitais, é necessário haver transparência e confiança entre as partes contratantes. O surgimento do Bitcoin reacendeu a discussão sobre contratos inteligentes como uma aplicação para blockchains, atuando como um sistema que auxilia na execução confiável de contratos inteligentes. Segundo os autores, eles são executados exatamente conforme programados, sem possibilidade de inatividade, censura, fraude ou interferência de terceiros.

Afirmam que Szabo ilustra a utilidade dos contratos inteligentes em transações digitais com o exemplo de Billy, que deseja comprar uma música. Nesse processo, Billy envia US$1 de sua carteira blockchain para o contrato inteligente, a música fica disponível para download, o contrato atribui os direitos de download à carteira de Billy e US$1 é distribuído aos criadores da música, com parte podendo ser retida como taxa pelo contrato inteligente. Importante destacar que não há intermediários, como gravadoras ou plataformas de música, nesse processo. O contrato sempre age conforme programado.

Explicam que os contratos inteligentes em blockchains têm outras aplicações, incluindo:

1. Emissão de tokens, que podem representar moeda virtual ou ativos físicos. Estes tokens podem ser utilizados para captação de recursos; Ofertas Iniciais de Moedas (ICOs) são um bom exemplo. Ativos que podem ser tokenizados incluem propriedades, ouro ou até moedas fiduciárias como o USD.

2. Comércio eletrônico, reduzindo a necessidade de intermediários na venda de bens virtuais, como música. Outro caso de uso significativo no comércio eletrônico são os contratos de custódia (*escrow*), que mantêm a custódia do pagamento entre comprador e vendedor até a conclusão da transação. Ao invés de um intermediário confiável (como o *PayPal*) segurar o pagamento, um contrato inteligente mantém os fundos (na forma de token).

3. Loterias, onde um contrato inteligente pode atuar como uma loteria. Os usuários compram a loteria enviando fundos para o contrato. Após a determinação dos resultados, o contrato inteligente paga os vencedores. O processo é transparente e não pode ser alterado.

Essas aplicações demonstram como os contratos inteligentes em blockchains podem revolucionar diversas áreas, segundo os autores, oferecendo soluções mais transparentes, seguras e sem intermediários.

Segundo Ouyang; Zhang; Wang (2022), a convergência de duas tecnologias disruptivas, *blockchain* e inteligência artificial (IA), conhecida como "*blockchain intelligence",* tem ganhado atenção generalizada recentemente. Essa combinação tem o potencial de revolucionar a transformação digital iminente, onde o blockchain pode fornecer uma infraestrutura de dados confiável e descentralizada para a IA, enquanto a IA pode ajudar o blockchain a extrair informações valiosas e realizar tarefas que exigem inteligência, como aprendizado, raciocínio, planejamento e resolução de problemas. A integração da IA nas tarefas baseadas em blockchain é vista como uma fusão mais profunda entre blockchain e IA, essencial para facilitar a IA descentralizada e a inteligência blockchain impulsionada pela IA.

Atualmente, acrescentam, tarefas de IA baseadas em blockchain têm levado a avanços significativos. Por exemplo, mercados de IA baseados em blockchain ajudam a compartilhar dados e modelos, mantendo propriedade e privacidade, além de permitir a terceirização ou *crowdsourcing* de tarefas de aprendizado com incentivos justos. A computação de IA distribuída baseada em blockchain transforma a IA centralizada tradicional em uma arquitetura semi-descentralizada ou descentralizada, eliminando pontos únicos de falha, incentivando a colaboração distribuída sem confiança e inovando a inteligência de borda.

Aditam ainda que Contratos Inteligentes (*Smart Contracts* - SCs) são tecnologias-chave para tornar o blockchain programável. Desenvolver SCs é mais fácil do que construir um blockchain do zero, e um número crescente de propostas para tarefas de IA baseadas em blockchain são implementadas com a ajuda de SCs flexíveis e portáteis. Exemplos incluem a especificação de protocolos de

colaboração com SCs em mercados de IA baseados em blockchain e a agregação de pesos de modelo com SCs em computação de IA distribuída baseada em *blockchain*. SCs estão gradualmente se tornando intermediários preferidos para realizar tarefas de IA baseadas em blockchain.

No entanto, demonstram que estudos estatísticos indicam que os SCs amplamente estudados são projetados principalmente para lógica de negócios. HE et al. analisaram milhões de SCs no Ethereum, a plataforma de SCs mais proeminente, e descobriram que a maioria desses SCs do Ethereum são altamente homogêneos e implementam lógica de controle simples e semelhante para tokens, jogos, Oferta Inicial de Moeda (ICO) e assim por diante. Os SCs projetados para tarefas de IA baseadas em blockchain têm funcionalidades diferentes dos SCs convencionais, o que pode levar a outras características e requerem um estudo separado. Para fazer a distinção, o artigo dos autores nomeia este tipo especial de SCs projetados para tarefas de IA baseadas em blockchain como Contratos Inteligentes (*Intelligent Contracts* - ICs). Embora os ICs mostrem um futuro promissor, suas tentativas atuais são independentes e fragmentadas, faltando análise sistemática.

O design do Bitcoin e sua blockchain garantem que os dados armazenados no ledger[27] sejam muito difíceis de alterar e adulterar com o uso da criptografia em blockchain assegurando essa robustez, isso segundo Lo, Wang e Lee, (2021. Pág. 171 – 172). Afirmam que mecanismos de incentivo embutidos no protocolo de consenso ajudam a alinhar todos os validadores para agirem de forma correta, enquanto a rede distribuída verifica a validade das transações para assegurar que nenhuma transação fraudulenta seja processada.

A segurança da rede blockchain advém de sua descentralização e distribuição. À medida que essas características diminuem, alguém pode ganhar controle sobre a rede e comprometer sua segurança. Alguns ataques comuns à rede são difíceis de executar em uma rede blockchain. Por exemplo, um ataque Sybil, em que alguém tenta assumir o controle de uma rede criando múltiplas contas no sistema, significaria operar múltiplos nós em uma rede blockchain. Se o atacante conseguir acesso a nós suficientes, ele pode bloquear transações

27 Refere-se ao registro digital ou banco de dados utilizado em uma blockchain para armazenar todas as transações realizadas na rede. É uma espécie de livro-razão que mantém um histórico imutável e cronológico de todas as transações, assegurando transparência e rastreabilidade. Em blockchains como o Bitcoin, o ledger é descentralizado, o que significa que é distribuído e mantido por diversos participantes na rede, em vez de ser controlado por uma única entidade central. Este aspecto é fundamental para a segurança e a integridade da blockchain.

(de outros usuários) e desconectá-los da rede pública. Isso permitiria que ele gastasse duas vezes ou bloqueasse suas transações.

Lo, Wang e Lee acrescentam que os algoritmos de consenso dificultam a realização de um ataque Sybil; geralmente, é necessário expandir recursos (como poder computacional ou tokens) para se tornar um nó na rede blockchain. Isso torna o ataque caro e difícil. Os mineradores têm um forte incentivo para continuar minerando honestamente, pois é necessário um grande número de recursos para minerar moedas. No entanto, esse tipo de ataque é conhecido por ocorrer na vida real em redes blockchain menores ou mais fracas. Em ataques Sybil de grande escala, onde os atacantes conseguem controlar a maioria do poder computacional da rede ou hashrate, eles podem realizar um ataque de 51 %.

Concluem Lo, Wang e Lee que a segurança da blockchain está intrinsecamente ligada à sua estrutura descentralizada e ao uso de mecanismos de consenso robustos, que dificultam ataques como o Sybil e o de 51 %. Esses ataques, embora possíveis, exigem recursos substanciais e são mais viáveis em redes menores, menos seguras.

Esta linha de pesquisa é crucial para entender como as tecnologias emergentes estão remodelando o conceito de vontade e consentimento no direito contratual. Ela abre caminho para a revisão de princípios jurídicos tradicionais e para a formulação de novas abordagens que se adequem à realidade das transações digitais e automatizadas.

2.5 A DETECÇÃO DE VÍCIOS DA VONTADE EM CONTRATOS DIGITAIS

Percebe-se que a natureza dos contratos digitais revela novos desafios à teoria dos vícios de vontade tradicional, sendo sua compreensão e percepção um tema de crescente importância na era da tecnologia avançada e da automação. À medida que as transações e acordos migram para o ambiente digital, questões relacionadas à validade e integridade desses contratos tornam-se cruciais. Vícios de vontade, como erro, dolo, coação e fraude, já são bem conhecidos no direito contratual tradicional.

A crescente incidência de demandas judiciais, especialmente em relação a contratos bancários digitais, fundamentadas na negativa de contratação, ressalta a importância crucial do estudo dos vícios de vontade no contexto digital. Essas ações frequentemente se baseiam na alegação de que o contrato foi firmado sem o consentimento genuíno de uma das partes, indicando a presença

de vícios como erro, dolo, fraude ou coação. No ambiente digital, a velocidade e a facilidade das transações, combinadas com interfaces de usuário muitas vezes complexas ou enganosas, podem levar a mal-entendidos ou manipulações, resultando em acordos que não refletem a verdadeira vontade de todas as partes envolvidas.

No caso de contratos bancários digitais, por exemplo, os desafios são ampliados pela natureza técnica dos serviços e produtos financeiros oferecidos, assim como pela assimetria de informações entre as instituições financeiras e os consumidores. A automação dos processos contratuais por meio de plataformas digitais pode ocasionalmente mascarar práticas predatórias ou termos desfavoráveis, levando os consumidores a concordar com condições que eles podem não compreender totalmente ou não ter a intenção de aceitar.

Este cenário sublinha a necessidade de uma análise aprofundada dos vícios de vontade em contratos digitais, bem como a implementação de salvaguardas legais e tecnológicas para proteger os consumidores. Isso inclui a criação de regulamentações mais rigorosas para as práticas de contratação digital, a promoção da transparência e da clareza na apresentação dos termos contratuais, e o desenvolvimento de tecnologias que garantam a autenticidade do consentimento e a prevenção de fraudes. A adoção dessas medidas é fundamental para garantir a confiança e a justiça nas transações digitais, especialmente em um setor tão sensível e impactante como o bancário.

Todavia, sua identificação e tratamento em contratos digitais, especialmente aqueles automatizados por meio de tecnologias como contratos inteligentes e blockchain, apresentam desafios únicos. Diversas operações são simples transferências de valores, como no caso do PIX, sendo outras respeitantes a empréstimos que terão efeitos por anos, com descontos mensais. Neste contexto, é essencial explorar como os vícios de vontade podem surgir em ambientes digitais e quais mecanismos jurídicos e tecnológicos podem ser utilizados para detectá-los e mitigá-los, garantindo assim a justiça e a equidade nas transações digitais.

2.5.1 TEORIA DA CONFIANÇA NOS VÍCIOS DA VONTADE EM CONTRATOS DIGITAIS

A invalidade dos negócios jurídicos tal com preconizado pelo art. 166 do Código Civil de 2002 aborda circunstâncias quanto ao sujeito, ao objeto, liceidade dos motivos, forma ou vedação legal expressa. Os vícios de vontade que

maculam a licitude do negócio jurídico são tratados no Código Civil como um defeito, passível de convalidação, conforme arts. 138 a 165.

Algumas hipóteses que representam defeito dizem respeito à compreensão do sujeito que contrata em relação às obrigações assumida. O Código Civil português de 1967, especificamente o artigo 247.º, estipula que são anuláveis os negócios jurídicos quando as declarações de vontade provêm de um erro substancial que uma pessoa de diligência normal poderia perceber, dadas as circunstâncias do negócio. É importante que o erro seja escusável, pelo que se adota um padrão abstrato conhecido como "*vir medius*" [28] para a aferição da escusabilidade do erro (Alves, 2003, p. 114).

Esta questão da escusabilidade aferida segundo um padrão abstrato remete à questão da capacidade pessoal que se amolde dentro de uma faixa de normalidade. Como bem lembrou Pimentel, a cidadania digital traz consigo, entre suas diversas nuances, a questão da educação digital. Diante das mudanças que a informatização acelerada apresenta na sociedade, o conhecimento do homem comum dificilmente lhe permitirá conhecer as peculiaridades dos contratos digitais, contratos inteligentes, interfaces, blockchain etc. Isso eleva a discussão da questão do erro escusável para novos desafios.

Caso uma pessoa comum, como por exemplo alguém com baixa escolaridade, mesmo com alguma experiência de vida, como um aposentado, pretenda obter um empréstimo bancário para resolver dívida, mas que não pretenda comprometer sua renda de forma substancial, necessariamente deverá procurar os canais digitais de atendimento, ou mesmo pessoas (em agências) que são meros operadores destes canais digitais à serviço das instituições de crédito. Com razão Venosa (2013, p. 206) quando aponta a necessidade de se observar a questão da escusabilidade do erro de acordo com o "conceito do homem médio para o caso concreto". Somente através da contextualização se poderá verificar se ocorrera defeito na "compreensão psíquica [....] da realidade, ou seja, a incorreta interpretação de um fato" (Venosa, 2013, p. 206).

Esta teoria é fecunda no direito civil, visto que o reconhecimento do defeito do negócio demanda elevada carga de interpretação. Teorias como a da vontade real (querer individual da pessoa), da declaração (privilegiando a

28 O conceito de homem médio, ou "vir bonus" ou "homem bom" é utilizado para se referir ao padrão de conduta de uma pessoa média, razoável, prudente e diligente na sociedade. É o que na Alemanha se refere "der kleine Mann auf der Straße", ou seja, ao homem comum da rua. Esse padrão é frequentemente empregado para avaliar ações e decisões nas esferas civil e comercial, servindo como critério para determinar a adequação e a razoabilidade das condutas das partes envolvidas em uma disputa legal.

segurança jurídica para dar primazia à declaração emitida), da responsabilidade (prevalência da declaração se o desacordo entre a declaração e a vontade for provocada por culpa do declarante), da confiança (além da responsabilidade, examina-se o comportamento de quem recebe a declaração, segundo a boa-fé) já povoaram diversos compêndios (Theodoro Júnior, 2003, p. 22-25).

Pondera Theodoro Júnior (2003, p. 26-28) que no embate entre a teoria da vontade e a teoria da declaração, mesmo que haja uma aparente preferência pelo resguardo da vontade real no novo Código Civil, ao permitir a anulação dos negócios em que o consentimento não foi livre e conscientemente manifestado, houve uma evolução significativa no tratamento do erro substancial. Nesse contexto, o autor menciona que a jurisprudência anterior estava impregnada pela "teoria da responsabilidade", na qual a culpa do autor da declaração era o foco. No entanto, o novo Código adotou a "teoria da confiança", inspirando-se em legislações modernas, como a italiana, a portuguesa e a peruana. Segundo essa teoria, a anulação do ato jurídico errôneo não depende apenas da ausência de culpa do declarante (erro escusável), mas também da culpa do destinatário da declaração, que poderia ter evitado o vício do negócio se o erro fosse perceptível por uma pessoa de diligência normal nas circunstâncias do negócio.

Menciona o autor a situação "*a contrario sensu*", em que, mesmo existindo um descompasso entre vontade e declaração, prevalecerá a declaração se o outro contratante, de boa-fé, não poderia perceber o erro. A teoria da confiança, mesmo nos vícios graves como dolo e coação, não exime a culpa do beneficiário para a configuração do vício de consentimento, exigindo conhecimento ou condições de conhecê-los por parte do beneficiário para que a anulação seja possível.

Theodoro Júnior avança argumentando que a teoria da confiança também é aplicável na fraude contra credores, onde a sanção só atinge o terceiro adquirente ou subadquirente que atua de má-fé. Assim, o sistema geral dos vícios de consentimento no novo Código está predominantemente submetido à teoria da confiança, que, segundo o Prof. Miguel Reale, corresponde ao princípio de socialidade do novo Código Civil, contrastando com o individualismo do Código de 1916 e ressaltando os valores coletivos sobre os individuais. A teoria da confiança que assegura a supremacia do interesse social sobre o individual no campo dos vícios de consentimento, valorizando a segurança do tráfico jurídico.

A teoria da confiança no direito civil adotada pelo Código Civil oferece importante balizamento para a validade dos negócios jurídicos, em especial no contexto dos contratos digitais, onde a assimetria de conhecimento tecnológico pode ser significativa. Presume-se que os contratantes agem com boa-fé e lealdade, confiando na manifestação de vontade alheia. No cenário digital, um

contratante com conhecimento técnico avançado tem o dever ético e jurídico de agir de maneira transparente, assegurando que a outra parte, especialmente o homem comum que não compreende as peculiaridades desta forma de contratação, compreenda plenamente as estipulações do contrato e as consequências de sua concordância. A omissão ou o aproveitamento indevido desse conhecimento superior para induzir a outra parte a um erro configura um vício na manifestação de vontade, o que pode levar à anulação do negócio jurídico.

2.5.2 DESAFIOS NA PROVA DE VÍCIOS DA VONTADE EM AMBIENTE VIRTUAL

A questão da prova dos vícios de vontade, especialmente como tratado no item anterior, faz emergir a questão da prova que deve ser interpretada para que o defeito possa ou não ser declarado. Esta questão probatória nos remete à duas teorias para a formação do negócio jurídico, o consensualismo e o formalismo.

Terré; Simler; Lequette; Chénedé (2019. pág. 226-253) analisam esta questão com profundidade, explorando seus fundamentos históricos e teóricos, principalmente no contexto do direito francês.

Segundo os autores, o consensualismo, que valoriza o acordo de vontades como suficiente para a formação de contratos, contrasta com o formalismo, que exige formas específicas para a eficácia do consentimento. No direito francês contemporâneo, o consensualismo é a norma, com o formalismo sendo a exceção, o que é evidenciado no artigo 1172 do Código Civil francês pós-reforma de 2016: "*les contrats sont par principe consensuels*" (os contratos são, por princípio, consensuais).

O consensualismo tem várias implicações práticas: a ausência de formalidades necessárias para a formação do contrato e a equivalência entre diferentes modos de expressar o consentimento, desde que sejam suficientemente expressivos. Esta abordagem é vista como uma extensão da liberdade contratual e respeita a vontade das partes, simplificando a conclusão de contratos e fomentando a atividade comercial.

As origens do consensualismo remontam ao direito romano primitivo, que era essencialmente formalista. Com o tempo, o direito romano admitiu certos contratos consensuais, influenciado pelas necessidades comerciais. Paralelamente, no direito francês antigo, houve um período de recuo do consensualismo, mas a partir dos séculos XI e XII, o formalismo começou a ceder, influenciado pelo direito canônico. O direito canônico enfatizou a força moral da

promessa, independentemente da sua forma, contribuindo significativamente para a valorização do consentimento sobre a forma.

Este processo histórico culminou na aceitação do princípio de que os contratos são obrigatórios pelo simples efeito da promessa, mesmo não solene. Destaca-se que, embora o formalismo do juramento religioso tenha inicialmente reforçado a formalidade, acabou por facilitar a transição para uma abordagem mais consensual, valorizando a intenção e o propósito moral por trás de um compromisso.

A evolução do consensualismo no direito contratual reflete uma mudança significativa nas práticas jurídicas, priorizando a vontade e o propósito moral sobre formalidades estritas, influenciando profundamente a formação e a execução dos contratos no direito moderno.

Terré; Simler; Lequette; Chénedé abordam o formalismo no contexto do direito contratual, destacando sua relevância e implicações na legislação moderna, embora seja frequentemente associado a noções negativas como lentidão, custo e complexidade. Os autores argumentam que, embora seja uma exceção no direito, o formalismo é amplamente presente na vida contratual contemporânea e não se limita apenas a desvantagens.

Os benefícios do formalismo incluem a promoção da reflexão e vigilância por parte das partes contratantes, ajudando a evitar consentimentos precipitados e fornecendo maior clareza e certeza sobre o conteúdo e a existência do contrato. Essa abordagem também auxilia na prevenção de fraudes contra terceiros e ajuda a manter o contrato transparente para o interesse público. O formalismo tem um papel crucial em assegurar a eficácia e a integridade dos contratos, bem como na proteção dos interesses das partes e de terceiros.

Os autores também destacam a evolução do formalismo. No passado, o formalismo era caracterizado pela rigidez e pela necessidade de cumprir formalidades estritas. Atualmente, porém, ele se adapta para atender a diferentes necessidades e contextos, sendo mais flexível e diversificado. Essa evolução reflete mudanças tecnológicas e sociais, como o avanço dos meios eletrônicos de comunicação, que influenciaram as formas de contratação e a prova dos contratos.

Os autores exploram a distinção entre formalismo direto e indireto. O formalismo direto se refere a contratos que exigem condições de forma específicas para sua validade, como os contratos solenes. Já o formalismo indireto aborda a eficácia do contrato, como nas formas probatórias e de publicidade, que não afetam a validade do contrato em si, mas são essenciais para sua oponibilidade a terceiros e para a segurança jurídica. Os autores reconhecem que, não obstante

suas vantagens, o formalismo pode ser usado de maneira abusiva, permitindo que uma parte evite suas obrigações contratuais com base em irregularidades formais. Contudo, destacam que tanto a legislação quanto a jurisprudência buscam equilibrar os aspectos positivos e negativos do formalismo, priorizando a justiça e a equidade nas relações contratuais.

Válido destacar a referência dos autores aos meios eletrônicos de comunicação em favor da teoria formalista. Além de a comunicação ser em grande parte eletrônica, estamos atualmente cada vez mais inseridos no ambiente digital, onde os negócios jurídicos, os contratos assumem a forma de dígitos, são registrados em sistemas informáticos, mesmo que a vontade da pessoa seja apresentada com um gesto. Nesta quadra atual, sistema algoritmos são capazes não só de registrar nossa vontade, mas também realizar prognósticos daquilo que desejamos, mas ainda não expressamos.

2.5.3 IMPACTO DAS TECNOLOGIAS NA MANIFESTAÇÃO DA VONTADE

O emprego de interfaces eletrônicas para atrair novos contratantes passou a ser uma realidade, ocorrendo o fenômeno da transição do modelo de negócios para negócios (B2B) para o modelo de negócios para consumidor (B2C), impulsionada pelo advento da Internet e da *World Wide Web*.

Gillies (2008, p. 26) destaca que as transações B2B eram as únicas a serem realizadas através de redes de computadores. Neste modelo, as empresas utilizavam o comércio eletrônico para contratar diretamente com outras empresas, muitas vezes sem a necessidade de intermediários ou agentes. Essa forma de comércio possibilitava uma comunicação direta entre empresas, simplificando e agilizando os processos de negociação e contratação. Com o desenvolvimento da Internet, houve uma expansão significativa nas possibilidades do comércio eletrônico, levando ao surgimento e popularização do modelo B2C. Neste modelo, as empresas passaram a usar a Internet como uma ferramenta de negócios e comunicação para atrair consumidores estrangeiros. Os contratos resultantes dessas atividades são denominados contratos B2C. Esses contratos caracterizam-se pela interação direta entre empresas e consumidores por meio de redes de computadores abertas.

Segundo Gillies, uma característica notável do modelo B2C é a possibilidade de as empresas contratarem diretamente com os consumidores sem a necessidade de operar por meio de um agente, filial ou representante na

jurisdição do consumidor. Isso representa uma mudança significativa em relação ao modelo tradicional, onde a presença física em uma localidade específica era muitas vezes necessária para facilitar as transações comerciais. Essa transformação nos modelos de comércio eletrônico reflete não apenas a evolução tecnológica, mas também uma mudança na maneira como as empresas e os consumidores interagem no mercado global. A capacidade de realizar transações diretamente, independentemente da localização geográfica, democratizou o acesso ao mercado global, permitindo que empresas de qualquer tamanho alcancem consumidores ao redor do mundo de maneira mais eficiente e com custos reduzidos.

As plataformas digitais emergem neste ambiente comercial para formar um novo mercado com características próprias. Grundmann; Hacker (2019) afirmam que as plataformas estão sob intenso escrutínio regulatório no direito antitruste. A literatura econômica sobre plataformas multilaterais e a dinâmica de mercado específica que elas geram foi aplicada às plataformas digitais para analisar em que medida plataformas dominantes podem potencialmente impedir a concorrência, abusar de concorrentes e clientes, e obstaculizar a inovação a longo prazo. Acrescentam que há um desenvolvimento significativo na literatura sobre barreiras à entrada na economia digital, e as plataformas, por serem os principais pontos de acesso a muitos serviços na economia digital, têm um papel proeminente nessa discussão. Apontam que Ezrachi e Stucke (2016) argumentam que plataformas baseadas em dados podem aplicar esquemas de precificação personalizados que não apenas se aproximam da discriminação de preços de primeiro grau, mas também potencialmente exploram viés do consumidor.

Argumentam Grundmann; Hacker (2019) que as plataformas desempenham um papel especial não apenas na manutenção de uma competição eficaz ou viável, mas também são um ingrediente crucial para o ambiente em que contratos facilitados digitalmente ocorrem frequentemente. Elas fornecem o quadro que molda a maneira como oferta e demanda são combinadas, como os produtos são percebidos e, consequentemente, como um grande número de contratos individuais são formados. Os efeitos de enquadramento, destacados pela economia comportamental, apontam para a importância específica dessa arquitetura de decisão.

Também apontam Grundmann; Hacker (2019) que as plataformas moldam concretamente as relações contratuais e os incentivos econômicos para seus usuários. A responsabilidade das plataformas pode decorrer da dependência dos usuários na influência predominante da plataforma sobre o fornecedor. A regulação pode ser necessária se a "predeterminação" contratual pela plataforma levar

a um desequilíbrio inaceitável na alocação de riscos entre os usuários da plataforma. Por exemplo, citam os autores, o Airbnb fornece apenas uma "garantia do anfitrião" que cobre, até certo ponto, danos à propriedade do anfitrião causados por hóspedes do Airbnb, mas não uma "garantia do hóspede" correspondente.

A regulação de tecnologias novas não deve ser vista como uma proibição da regulação, mas pode também ser utilizada para fomentar a inovação, por exemplo, fornecendo marcos legais para a introdução de características experimentais que não apresentam grandes riscos para os usuários, mas que introduzem um elemento de incerteza legal.

Principalmente em países com baixa escolaridade como o Brasil, a vulnerabilidade do consumidor com baixa instrução frente às práticas de coleta de dados pessoais nas plataformas digitais é uma questão preocupante. Esse grupo de consumidores, muitas vezes desconhecendo os meandros tecnológicos e as políticas de privacidade, pode inadvertidamente fornecer informações sensíveis ao buscar contratar um serviço ou comprar um produto. Esses dados, uma vez coletados, são utilizados para traçar perfis detalhados, permitindo que empresas direcionem publicidades e ofertas de forma mais eficaz, mas invasiva. Tal prática não apenas explora a falta de conhecimento desses consumidores sobre o uso de suas informações, mas também levanta sérias questões sobre a ética da manipulação de dados e a necessidade de proteção robusta dos direitos do consumidor no ambiente digital.

Percebe-se a necessidade de uma abordagem regulatória robusta e coordenada entre o poder legislativo e o executivo, especialmente através de órgãos de proteção e defesa do consumidor, sendo fundamental para salvaguardar os interesses dos consumidores na era digital. O poder legislativo tem o papel constitucional de estabelecer um marco legal abrangente e adaptável que enderece questões emergentes, como a privacidade de dados, a publicidade direcionada e o uso de inteligência artificial no comércio, inclusive como citado por Pimentel (2023) sobre a legislação chilena quanto à proteção cerebral. Simultaneamente, órgãos executivos de defesa do consumidor devem atuar na aplicação efetiva dessas leis, garantindo que as empresas cumpram as normativas e que os direitos dos consumidores sejam respeitados, assim como desenvolvam políticas de compliance. Isso inclui a implementação de medidas punitivas em caso de infrações, a promoção de campanhas educativas para aumentar a conscientização dos consumidores sobre seus direitos e riscos, e a oferta de canais acessíveis para reclamações e resolução de disputas.

3 A VALIDADE E EFICÁCIA DOS CONTRATOS DIGITAIS

3.1 BASE LEGAL COMO FUNDAMENTO DA VALIDADE

Discutimos neste trabalho que os contratos digitais são celebrados por meio de tecnologias digitais, como a internet, o e-mail e a assinatura eletrônica, utilizando a tecnologia da informação, tendo ganhado cada vez mais importância no mundo jurídico, à medida que as tecnologias digitais se tornam mais presentes em nossas vidas.

Para a compreensão do fenômeno jurídico é relevante o estudo dos elementos clássicos de validade contratual e sua adaptação às peculiaridades do contrato digital. Na forma clássica, tal como positivado nos arts. 166 e seguintes do Código Civil de 2002, são elementos de validade contratual:

1. Capacidade: as partes devem ser capazes de contratar.

2. Objeto: o objeto do contrato deve ser lícito, possível, determinado ou determinável e com valor econômico.

3. Causa: a causa do contrato deve ser lícita e moral.

4. Consenso: o consenso é a manifestação de vontade das partes em celebrar o contrato.

5. Forma: entre as doutrinas consensualistas e formalistas, a forma legalmente estabelecida é uma exceção.

No contrato digital, podem ser consideradas como hipóteses objeto de estudo diante da sua peculiaridade:

1. Capacidade: as partes devem ter capacidade para contratar nos termos da legislação brasileira. No caso de pessoas jurídicas, é necessário verificar se elas estão devidamente constituídas e em funcionamento.

2. Objeto: o objeto do contrato digital deve respeitar as mesmas regras do objeto do contrato tradicional. No entanto, é importante estar atento às peculiaridades das tecnologias digitais, como a possibilidade de intangibilidade e a dificuldade de controle da autenticidade do conteúdo.

3. Causa: a causa do contrato digital deve ser lícita e moral, assim como a causa do contrato tradicional.

4. Consenso: o consentimento no contrato digital pode ser manifestado por meios eletrônicos, como a assinatura eletrônica. A compreensão das peculiaridades e implicações do contrato digital e obrigações assumidas, especialmente com o uso de dados pessoais para fins outros relacionados à relação negociada deve ser objeto de consideração.

5. Forma: o meio digital deixa registros de diversas naturezas, além do que é campo aberto para a realização de fraudes e manipulações que devem ser consideradas na realização do negócio jurídico.

O princípio da equivalência funcional estabelece que os documentos digitais têm a mesma validade jurídica dos documentos tradicionais. Neste ponto, entra em discussão as normas positivadas nos arts. 212 do Código Civil brasileiro. No entanto, podem existir algumas barreiras tecnológicas, culturais e jurídicas que podem dificultar a aplicação do princípio da equivalência funcional.

As barreiras tecnológicas podem dificultar a prova da existência e da autenticidade do documento digital. Por exemplo, pode ser difícil provar que um documento digital não foi alterado após sua criação.

As barreiras culturais podem dificultar a aceitação do documento digital como meio de prova. Por exemplo, algumas pessoas ainda preferem documentos em papel, pois os consideram mais seguros e confiáveis.

As barreiras jurídicas podem dificultar a aplicação do princípio da equivalência funcional. Por exemplo, algumas leis ainda exigem que os contratos sejam celebrados por meio de documentos escritos.

Deverá o estudo voltar sua atenção para a jurisprudência brasileira e como esta tem reconhecido a validade dos contratos digitais, se, por exemplo, em alguns casos, os juízes têm exigido a adoção de medidas para garantir a segurança jurídica do contrato, como a utilização de assinatura eletrônica qualificada ou ata notarial. A confiança das partes é um elemento fundamental para a validade do contrato digital. As partes devem confiar na autenticidade do documento digital, na identidade das partes e na segurança da tecnologia utilizada, caso contrário demandas judiciais trarão o tema para a solução do controvérsias. A segurança tecnológica é um elemento essencial para a validade do contrato digital. As partes devem tomar medidas para proteger seus dados e evitar fraudes.

3.2 ELEMENTOS ESSENCIAIS PARA A VALIDADE CONTRATUAL

Segundo Diniz (2012, p. 485) a capacidade é indispensável à participação válida na seara jurídica, e que os absolutamente incapazes (como menores de 16 anos) não podem praticar nenhum negócio jurídico. Os relativamente incapazes (como maiores de 16 anos e menores de 18 anos), embora possam participar pessoalmente dos negócios jurídicos, deverão ser assistidos por pessoas a quem a lei determinar. Trata-se de uma exceção de caráter pessoal, que só pode ser invocada pelo próprio incapaz ou pelo seu representante legal. No caso de um

negócio jurídico celebrado por um relativamente incapaz sem a devida assistência, o negócio é anulável, a pedido do incapaz, do seu representante legal ou de terceiro prejudicado. Acrescenta que as pessoas jurídicas intervirão por seus órgãos, ativa e passivamente, judicial e extrajudicialmente. O órgão da pessoa jurídica é uma ou um conjunto de pessoas naturais que exprimem sua vontade.

Para um negócio jurídico ser considerado perfeito e válido, ele deve ter um objeto lícito, ou seja, conforme a lei, não sendo contrário aos bons costumes, à ordem pública e à moral. Se o objeto for ilícito, o negócio jurídico será nulo e não produzirá qualquer efeito jurídico. O objeto do ato negocial deve ser possível, física ou juridicamente, de modo que se o negócio implicar prestações impossíveis, como por exemplo voltar ao passado ou vender a herança de uma pessoa viva, ele será nulo, lembrando que a impossibilidade deve ser absoluta, ou seja, a prestação deve ser irrealizável por qualquer pessoa ou insuscetível de realização (Diniz, 2012, p. 489).

Segundo Delben; Manuela (2010), a causa, apesar de essencial, é um conceito sem consenso na doutrina jurídica, seja em termos do próprio conceito, da abrangência, da valoração ou da desvalia. Lembram que o negócio jurídico é um ato essencialmente volitivo, que nasce no interior do indivíduo e se materializa através de uma declaração ou consentimento. É nesse fator determinante da emissão de vontade, condição essencial para a existência do negócio jurídico, que repousa o estudo da causa. Apontam duas correntes antagônicas: a causalista, que vê a causa como a última razão que leva o sujeito a realizar um contrato, e a anticausalista, cujos partidários extremistas consideram o elemento causa inútil, confundindo-o com o objeto ou com o consentimento. Os mais moderados ignoram o aspecto subjetivo, relacionando-a à significação social e função desempenhada pelo negócio. Nesse sentido, o Estado apenas protege os negócios capazes de atender aos interesses sociais. Para harmonizar essas duas teorias, surge a teoria mista, com elementos das duas.

Argumentam Delben; Manuela que a teoria da causa suscita um confronto entre os postulados de apresentação estrita da força obrigatória dos contratos e a impossibilidade de se manter válido seus termos injustos. Assim, o fato da causa não ser considerada elemento do negócio jurídico não significa que é dispensada a sua invocação quando da análise da relação contratual. Entretanto, quando ela é contemplada como finalidade do ato e não como fonte deste, os problemas excedem em muito as relações creditícias, estendendo-se a todos atos jurídicos. “É na análise desse fator determinante da emissão de vontade, condição essencial para a existência do negócio jurídico, que repousa o estudo da causa.” As autoras concluem que todo negócio jurídico tem causa e toda causa

tem natureza imutável, traduzida na submissão de cada negócio a uma causa respectiva. Esse elemento legitima os juízes a analisar até onde o consentimento está viciado, flexibilizando a norma positiva. A causa proporciona ao juiz apreciar a licitude do negócio, inclusive sob seu aspecto social, independentemente de sua inclusão como requisito caracterizador do negócio jurídico, mas sim por ser parte integrante da relação negocial.

Nos negócios jurídicos, o consentimento e da declaração volitiva, seja ela expressa ou tácita, constitui elemento essencial para sua validade. Diniz (2012, p. 490) define o consentimento como "a anuência válida do sujeito a respeito do entabulamento de uma relação jurídica sobre determinado objeto". O consentimento pode ser expresso ou tácito, desde que o negócio, por sua natureza ou por disposição legal, não exija forma expressa. Será expresso se declarado, por escrito ou oralmente, de modo explícito. Será tácito se resultar de um comportamento do agente, que demonstre implicitamente sua anuência.

Quanto à forma, Silva (2015) entende ser está um dos elementos essenciais para a sua validade. A forma é o meio pelo qual se exterioriza a manifestação de vontade nos negócios jurídicos, para que possam produzir efeitos jurídicos. No sistema jurídico brasileiro, a forma é livre, ou seja, o ato pode ser celebrado do modo mais conveniente para as partes, desde que não haja uma forma prescrita em lei para a celebração do negócio jurídico. No entanto, há casos em que a lei exige uma forma especial para a validade do negócio jurídico, como no caso da compra e venda de imóveis de valor superior a trinta vezes o maior salário mínimo vigente no país. A forma do negócio jurídico pode ser verbal, escrita ou até mesmo silenciosa, tudo vai depender do ato a ser realizado. A forma pode ser prescrita pela lei ou pelas partes, que em alguns casos inserem cláusulas de validade do negócio jurídico.

Quanto à interpretação, Silva (2015) aponta que a declaração de vontade deve prevalecer sobre o sentido literal das palavras, pois os negócios jurídicos têm na vontade um elemento importantíssimo. O consentimento das partes, seja de forma expressa ou tácita, deve ser expressado livremente, sem sofrer a influência de fatores externos. Caso o negócio seja celebrado de forma diversa da prevista em lei, quando há essa previsão, o negócio jurídico será nulo, ineficaz, não produzindo qualquer efeito.

Sobre o uso de plataformas, vejamos as condições exigidas por aquelas que são utilizadas até para a confirmação da identidade dos usuários por terceiros, demonstrando sua relevância, como o FACEBOOK e o GOOGLE.

As restrições de idade para a gestão de Contas do Google e para o uso de certos serviços oferecidos pela empresa são apresentadas no sítio eletrônico

da empresa (GOOGLE, 2023). De forma geral, a idade mínima para gerenciar uma Conta do Google é de 13 anos nos países que não possuem uma legislação específica listada. Para crianças mais novas, um pai ou mãe pode criar e gerir uma conta por meio do Family Link, até que a criança atinja a idade mínima determinada no país de residência.

Essas restrições de idade podem não se aplicar a contas do *Google Workspace,* incluindo aquelas pertencentes ao domínio do *Google Workspace for Education*. São destacadas restrições específicas para alguns serviços do Google: vídeos do YouTube com restrição de idade são acessíveis apenas por usuários com 18 anos ou mais; e o mesmo limite de idade se aplica para o uso do *Google AdSense e Google Ads*.

Existe uma política do GOOGLE de desativação de contas: se for identificado que um usuário não cumpre a restrição de idade mínima para ter uma conta em serviços do Google, ele terá 14 dias para adequar a conta às normas. Caso contrário, a conta será desativada.

A META, detentora do FACEBOOK, apresenta compromissos que os usuários devem assumir para utilizar o Facebook, visando promover segurança e responsabilidade na comunidade. Os usuários devem usar o mesmo nome no Facebook que usam na vida cotidiana, fornecer informações precisas, criar apenas uma conta para uso pessoal, e não compartilhar a senha ou transferir a conta a terceiros sem permissão do Facebook.

Existem também restrições específicas para quem pode usar o Facebook. Indivíduos menores de 13 anos, condenados por crimes sexuais, ou aqueles que tiveram contas anteriormente desativadas por violar Termos do Facebook, Padrões da Comunidade ou outras políticas, não podem usar o Facebook. Se uma conta for desativada por esses motivos, o usuário não deve criar outra conta sem permissão do Facebook, que é concedida a critério exclusivo da empresa. Adicionalmente, o uso do Facebook é proibido para aqueles impedidos de receber produtos, serviços ou software da empresa conforme as leis aplicáveis.

O Mercado Livre, plataforma de comércio eletrônico, exige para o cadastramento dos usuários o fornecimento de e-mail, nome (a escolha do usuário), telefone e senha.

Um outro exemplo de cadastro em plataforma onde a identidade, e capacidade do usuário, não é verificada temos no IFOOD, empresa que presta serviços intermediando o restaurante do consumidor, em linhas gerais. A plataforma utiliza os dados de identificação do usuário já cadastrados em outras plataformas, que também já não apresentam segurança quanto à confiabilidade dos perfis criados.

Para se cadastrar no IFOOD, o processo inclui várias etapas: 1. Baixar o Aplicativo: é necessário baixar o aplicativo iFood na *App Store* para iOS ou na *Play Store* para Android. 2. Permitir Localização: O aplicativo solicita permissão para acessar a localização do usuário. Esta autorização é importante para que o app possa listar restaurantes e estabelecimentos próximos que oferecem delivery. 3. Permitir Notificações: o app pede permissão para enviar notificações, essenciais para informar sobre o status do pedido e possíveis contatos do restaurante ou entregador. 4. Escolher Método de Criação de Conta: O usuário pode criar a conta utilizando o Facebook, número de celular ou e-mail. 5. Código de Confirmação para Contas por E-mail: caso opte por criar a conta via e-mail, o iFood enviará um código de confirmação para o endereço de e-mail fornecido. 6. Confirmação de E-mail e Celular: depois de confirmar o e-mail, o usuário deve registrar o número de celular e escolher receber o código de confirmação por SMS ou WhatsApp. 7. Informar Dados Pessoais: o usuário deve fornecer seus dados pessoais, incluindo CPF e nome completo, para aumentar a segurança da conta e facilitar a identificação pelos estabelecimentos.

Ainda sobre as peculiaridades da validade do negócio jurídico em ambiente digital, válido destacar ser inerente à própria tecnologia o uso dos sistemas de informática. Snowden (2019, p. 353-365) descreve em detalhes o processo meticuloso e arriscado pelo qual, um administrador de sistemas, acessou e extraiu informações confidenciais de uma rede altamente segura. Ele começa explicando o conceito de "permissões" em computação, que define o que um usuário pode ou não fazer em um computador ou rede. Seu objetivo era "entrar no coração da rede mais segura do mundo para encontrar a verdade, fazer uma cópia dela e divulgá-la para todos", mantendo-se indetectável.

O autor destaca a extrema vigilância na NSA, onde cada ação deixa um rastro digital. Sabendo disso, ele utilizou sua posição como administrador de sistemas, que lhe dava uma compreensão única dos sistemas de segurança e monitoramento. Ele descreve como os próprios sistemas complexos da NSA, embora poderosos, tinham falhas devido à sua complexidade e ao fato de que nem mesmo os administradores entendiam completamente seu funcionamento.

As tarefas de leitura, escrita e execução, conforme descritas por Snowden, são fundamentais para entender como os sistemas de computador e redes funcionam, especialmente no contexto da segurança e do gerenciamento de informações.

1. Leitura: A permissão de leitura em um sistema de computador permite ao usuário acessar e visualizar o conteúdo de um arquivo.

2. Escrita: A permissão de escrita possibilita ao usuário modificar ou criar arquivos em um sistema.

3. Execução: A permissão de execução permite ao usuário rodar um arquivo ou programa.

A impossibilidade de apagar completamente os dados em computadores é outro ponto crítico. Quando o Snowden menciona a vigilância extrema na NSA, com cada ação deixando um rastro digital, isso sublinha um aspecto importante da computação moderna: é extremamente difícil, se não impossível, apagar completamente os vestígios de dados em sistemas de computador. Mesmo quando os dados são excluídos, eles podem ser recuperados por meio de técnicas forenses digitais, a menos que medidas extremamente rigorosas de destruição de dados sejam empregadas.

Como visto, enquanto algumas plataformas exigem apenas a prestação de informações sob a livre escolha do usuário, outras podem exigir dados adicionais para comprovação da identidade, como CPF, Identidade etc. Para se cadastrar no app do Nubank, por exemplo, após ser aprovado como cliente, é necessário seguir alguns passos. Primeiro, deve-se criar uma senha de no mínimo oito dígitos, combinando letras e números não sequenciais, e evitando senhas óbvias como datas de aniversário. Em seguida, o usuário será direcionado para outro painel onde deve registrar seus dados pessoais, sendo necessário enviar documentos e verificar o e-mail. Além de colher informações sobre pessoa politicamente exposta (conforme norma do Banco Central), o que se refere a alguém que nos últimos cinco anos exerceu cargo, emprego ou função pública relevante, seja no Brasil ou exterior, incluindo familiares e pessoas próximas, deve-se confirmar a identidade, tendo em mãos um documento de identificação válido, como RG, CNH ou RNM (para estrangeiros residentes no Brasil). Este documento deverá ser válido e a pessoa deverá tirar fotos do documento, isso sob o argumento de prevenção de fraudes. Deve-se colher dados biométricos, mediante uma foto de si mesmo como também segurando o documento próximo ao queixo, enquadrando o rosto na tela do celular e garantindo que as informações no documento estejam visíveis.

Aceitas as informações enviadas, o usuário poderá utilizar os serviços financeiros da plataforma, servindo, basicamente, a senha como instrumento de autenticação de acesso e validação das operações.

Algumas plataformas armazenam os dados de uma primeira operação realizada para as próximas operações, isso sem a repetição de passos, como é o caso da AMAZON. O recurso “Comprar agora” é uma modalidade de compra expressa que permite aos usuários da AMAZON revisar e modificar detalhes

como forma de pagamento e prazo de entrega antes de concluir a compra de forma rápida. Após realizar um primeiro pedido com pagamento via cartão, esses detalhes são automaticamente salvos como preferências padrão de pagamento do recurso "Comprar agora". Essas preferências também são aplicáveis a compras feitas com Alexa, Kindle e outras aquisições digitais, possibilitando compras imediatas com apenas um clique ou comando de voz, assim como por reconhecimento facial. Conforme a plataforma, ao escolher "Comprar agora" em qualquer página de produto, o pagamento será realizado usando a forma de pagamento padrão registrada na conta do usuário, e o produto será enviado para o endereço padrão. É possível verificar e confirmar as informações de pagamento e entrega em uma janela pop-up "Comprar agora" ou na tela de revisão antes de efetivar o pedido. Se o usuário desejar modificar as informações de pagamento ou entrega para um pedido específico na janela pop-up "Comprar agora", basta selecionar a opção desejada, atualizar as preferências e realizar o pedido. Alterações também podem ser feitas na tela de revisão ou finalização da compra, selecionando a opção "Alterar" na seção correspondente.

Existe um aspecto interessante no comércio eletrônico moderno, que é a vastidão do tráfego comercial no ambiente virtual. Parece crucial que as operações realizadas com assinatura digital com o uso de chaves públicas sejam aparentemente uma exceção.

A assinatura digital e o uso de chaves públicas são componentes essenciais da criptografia assimétrica, um método usado para garantir a segurança e a integridade dos dados nas transações online. A assinatura digital assegura que uma mensagem ou documento não foi alterado desde a sua criação, enquanto as chaves públicas permitem a segurança na troca de informações, garantindo que apenas as partes autorizadas possam acessar e interpretar os dados transmitidos.

O fato de essas operações deste tipo terem uma aparência de exceção sugere que, apesar da importância dessas tecnologias para a segurança das transações online, elas podem não ser tão amplamente utilizadas quanto seria ideal no comércio eletrônico. Isso pode indicar uma lacuna na implementação de práticas de segurança robustas em algumas plataformas de e-commerce ou uma falta de conscientização sobre a importância da criptografia na proteção contra fraudes e outras ameaças cibernéticas, isso em prol da dinâmica do consumo em que se busca soluções rápidas, acesso rápido a produtos e serviços, entregas rápidas.

Com o crescimento exponencial do comércio eletrônico, a segurança das transações online se torna cada vez mais crítica. A adoção generalizada de

assinaturas digitais e chaves públicas poderia significativamente melhorar a segurança do tráfego comercial na internet, protegendo tanto os consumidores quanto os comerciantes de atividades fraudulentas e vazamentos de dados, porém com o possível sacrifício da velocidade em que as negociações são realizadas.

3.3 A EQUIVALÊNCIA FUNCIONAL ENTRE DOCUMENTO TRADICIONAL E DIGITAL

O princípio da equivalência funcional entre os documentos digitais e tradicionais decorre da norma da não discriminação, tal como disposto no Modelo UNCITRAL. Ao abordar esta temática, Menke (2018) explica que a assinatura eletrônica visa identificar as partes no meio virtual, pois, citando Otto Ulrich: "sem identificação não se pode responsabilizar". A definição da UNCITRAL ilustra a amplitude do termo "assinatura eletrônica", incluindo diversas técnicas como autenticação biométrica, PINs e versões digitalizadas de assinaturas manuscritas.

Segundo Singh (2001, p. 183), a forma como os computadores processam e criptografam mensagens denota uma diferença mais significativa, e talvez a mais fundamental, em relação aos métodos tradicionais de criptografia, visto que os computadores trabalham com números binários, não com letras do alfabeto. Os computadores operam exclusivamente com números binários, que são sequências de uns (1) e zeros (0), conhecidos como dígitos binários ou bits[29].

A distinção entre assinaturas eletrônicas e digitais é reconhecida pela literatura especializada, onde se enfatiza que enquanto a assinatura eletrônica é um termo abrangente para qualquer forma eletrônica de assinatura, a assinatura digital é um tipo específico que utiliza criptografia de chave pública e funções

29 No contexto da assinatura digital, antes da criptografia, qualquer mensagem precisa ser convertida em dígitos binários. Essa conversão é realizada seguindo vários protocolos, sendo um dos mais comuns o Código Padrão Americano para o Intercâmbio de Informações (ASCII, na sigla em inglês). O ASCII atribui um número binário de sete dígitos a cada letra do alfabeto. Neste contexto, deve-se pensar em um número binário como um padrão de uns e zeros que identifica exclusivamente cada letra, de forma semelhante a como o Código Morse identifica cada letra com uma série única de pontos e traços. Como existem 128 maneiras de arranjar uma combinação de sete dígitos binários, o ASCII pode identificar até 128 caracteres distintos. Isso proporciona espaço suficiente para definir todas as letras minúsculas (por exemplo, a = 1100001), toda a pontuação necessária (por exemplo, ! = 0100001) e outros símbolos (por exemplo, & = 0100110). Após a mensagem ser convertida em binário, o processo de criptografia pode começar. Embora o processo envolva computadores e números, e não máquinas e letras, a criptografia ainda ocorre de maneira tradicional. A transição da criptografia de um método baseado em letras para um processo que utiliza a codificação binária é uma adaptação à tecnologia da computação moderna. A ênfase está na importância do sistema binário e do ASCII como meios fundamentais para a conversão de mensagens em um formato que possa ser criptografado por computadores (SINGH, 2001, p. 183).

hash[30]. A seleção da forma apropriada de assinatura eletrônica deve levar em conta o contexto específico e a análise de risco associada (Adams e Lloyd, 1999).

A assinatura digital é uma forma específica de assinatura eletrônica, baseada na criptografia assimétrica (Menke). A assinatura digital no Brasil ganhou destaque com a Medida Provisória 2.200-2/2001, que consagrou o uso da criptografia assimétrica.

Prossegue Menke com uma comparação entre a criptografia simétrica e a assimétrica. Na simétrica, ambos os interlocutores compartilham a mesma chave, enquanto na assimétrica, são utilizadas duas chaves distintas: uma privada e uma pública. Essa estrutura resolve as limitações da criptografia simétrica, como a necessidade de compartilhar previamente a chave e a dificuldade de escala. Na assinatura digital, o texto assinado não é criptografado, mas sim seu resumo, através de uma função hash.

O certificado digital, adita o autor, surge como uma solução para agregar segurança às comunicações eletrônicas, associando um par de chaves criptográficas ao nome e atributos do titular, validados por uma Autoridade Certificadora. Este elemento ajuda a contornar vulnerabilidades presentes em outras formas de assinaturas eletrônicas. Por conta disso, a equivalência funcional e o valor probatório das assinaturas digitais existem uma presunção relativa de autoria conferida às assinaturas digitais. Esta presunção, contudo, é refutável, permitindo a contestação em casos de coação ou outros vícios.

Menke aborda a relação entre a Medida Provisória 2.200-2 e as formas de atribuição de autoria no meio eletrônico, enfatizando que a MP não cria um modelo exclusivo ou obrigatório para autenticar documentos eletrônicos. Em vez disso, ela se insere no contexto mais amplo das normas civis e processuais, que permitem a utilização de diversas formas de prova. A assinatura digital da ICP-Brasil, não é a única forma válida, mas oferece uma segurança jurídica robusta, dificultando alegações de ausência de autoria.

Foi apresentado acima o estudo de Tang (2015, p. 123-127) a respeito do valor probatório e da equivalência funcional, especialmente diante da intangibilidade dos dados eletrônicos. Em seu estudo, baseado no Regulamento de Bruxelas I Recast, existe uma diferenciação entre assinatura eletrônica avançada

30 As funções hash são algoritmos que recebem dados de qualquer tamanho e os condensam em saídas de tamanho fixo e curto. Tradicionalmente, essas funções são utilizadas em estruturas de dados para criar tabelas hash, que permitem buscar elementos em tempo constante. (KATZ; LINDELL, 2015, p. 153-154). No contexto da assinatura eletrônica, o termo "hash" se refere a uma função hash criptográfica, que é um algoritmo fundamental no processo de criação de assinaturas digitais. A função hash tem a capacidade de receber uma entrada de dados de qualquer tamanho (como um documento ou uma mensagem) e produzir uma saída de tamanho fixo, conhecida como valor de hash ou resumo hash.

e qualificada. Por exclusão, as assinaturas simples possuem baixo nível de segurança, não garantindo a identidade, como um botão "concordo", "aceito".

As Assinaturas Eletrônicas Avançadas (AEA) devem, quanto à identificação e ligação, estarem claramente ligada ao signatário, de forma que a identidade do signatário possa ser confirmada de forma confiável. A criação da assinatura deve estar sob seu controle exclusivo, de modo que apenas o signatário tenha acesso e controle sobre esta. A integridade permite que qualquer alteração posterior seja detectável.

Por sua vez, as Assinaturas Eletrônicas Qualificadas (AEQ) inclui todas as características de uma AEA, requerendo um certificado qualificado para assinaturas eletrônicas, o que eleva o nível de segurança. Este certificado é emitido por uma Autoridade de Certificação (AC) confiável. A AEQ deve ser criada em um Dispositivo Seguro de Criação de Assinatura (DSCA) que garante a segurança dos dados de criação de assinatura. A AEQ tem um status legal equivalente a uma assinatura manuscrita em muitos contextos jurídicos, como são exemplos a União Europeia e o Brasil, oferecendo um alto grau de confiança na identidade do signatário e na integridade do documento assinado (Benincasa, 2023).

O reconhecimento da equivalência funcional depende da autenticidade e integridade[31] do documento digital. Burnett e Paine (2001, p. 304-305) apontam

31 Segundo LANGENBACH e ULRICH, dois conceitos fundamentais na comunicação digital são a autenticidade e integridade, ambos cruciais para a autodeterminação informativa, ou seja, o direito de controlar as próprias informações pessoais. Para a autenticidade é enfatizado o exercício do direito à autodeterminação comunicativa que depende da capacidade de, se necessário, confirmar a identidade do parceiro de comunicação. Essa capacidade é essencial para evitar que um indivíduo se torne um objeto passivo de informação. Ele deve ter o poder de decidir com quem e sobre quais assuntos deseja comunicar. A necessidade de confirmar a identidade dos parceiros de comunicação é especialmente evidente em comunicações que envolvem dados sensíveis, como no setor médico. "Die Wahrnehmung des kommunikativen Selbstbestimmungsrechts setzt zwingend die Möglichkeit voraus, sich bei Bedarf - gegebenenfalls mit dessen Zustimmung - über die Identität des Kommunikationspartners zu vergewissern" (A percepção do direito à autodeterminação comunicativa requer necessariamente a possibilidade de, se necessário, com o consentimento do outro, assegurar-se sobre a identidade do parceiro de comunicação). A integralidade está intimamente relacionada à autenticidade. Por razões semelhantes às que tornam essencial a verificação da autenticidade, também deve ser possível verificar se a informação foi alterada durante a comunicação. Assinaturas eletrônicas são destacadas como uma ferramenta importante para provar a integridade de um conjunto de dados eletrônicos, pois elas podem demonstrar que os dados não foram corrompidos ou alterados. Isso é crucial para a proteção do direito à autodeterminação informativa. „Eng mit der Authentizität hängt die Integrität zusammen... Da mit der elektronischen Signatur die Unversehrtheit eines elektronischen Datensatzes nachgewiesen werden kann, ist sie auch insoweit eine wichtige technische Voraussetzung zur Wahrung des Rechts auf informationelle Selbstbestimmung" (A integridade está intimamente ligada à autenticidade... Como a assinatura eletrônica pode demonstrar a integridade de um conjunto de dados eletrônicos, ela também é uma importante condição técnica para a preservação do direito à autodeterminação informativa). Os autores, portanto, defendem que a autenticidade e a integridade são fundamentais para a autodeterminação informativa no ambiente digital. Assinaturas eletrônicas são apresentadas como ferramentas vitais para garantir esses dois aspectos, possibilitando aos indivíduos a confirmação da identidade dos parceiros de comunicação e a integridade dos dados transmitidos. LANGENBACH; ULRICH (org.) (2002, p. 111-112)

aspectos importantes distintivos entre assinaturas eletrônicas e digitais, destacando suas características, usos e implicações legais.

Para os autores, a assinatura eletrônica é definida como qualquer símbolo ou método realizado por meios eletrônicos, que é executado ou adotado por uma parte com a intenção atual de se vincular ou autenticar um registro. Esta definição é abrangente e inclui uma variedade de métodos, desde a saída de um dispositivo biométrico sofisticado, como um sistema de reconhecimento de impressões digitais, até a simples entrada de um nome digitado no final de uma mensagem de e-mail. O foco está na intenção do signatário de assinar o registro, independentemente do meio ou da maneira escolhidos para efetuar a assinatura.

Aditam os autores, a assinatura digital é uma implementação específica da criptografia de chave pública. Formalmente, pode ser definida como a transformação de um registro usando um sistema criptográfico assimétrico e uma função hash, de tal forma que uma pessoa com o registro inicial e a chave pública do signatário possa determinar com precisão (a) se a transformação foi criada usando a chave privada correspondente à chave pública do signatário e (b) se o registro inicial foi alterado desde que a transformação foi feita.

Burnett e Paine afirmam que as assinaturas digitais são específicas da tecnologia, criadas por meio de sistemas de chave pública, enquanto as assinaturas eletrônicas são produzidas por qualquer método de computador, incluindo sistemas de chave pública. Isso torna as assinaturas digitais tecnologicamente específicas e as eletrônicas, tecnologicamente neutras. O uso de assinaturas eletrônicas de baixa segurança, como simplesmente digitar o nome em um e-mail, levanta questões sérias de autenticidade. No entanto, em situações informais ou de baixo valor, onde é improvável que surjam disputas, esse nível de segurança pode ser suficiente. Por exemplo, é comum terminar e-mails puramente sociais com a digitação do nome do remetente. Nesses casos, o nome serve para autenticar o documento, mas não necessariamente indica a intenção de ser vinculado ao seu conteúdo.

No entanto, segundo Burnett e Paine, para transações eletrônicas formais, mas de baixo risco, um sistema de assinatura mais robusto pode ser desejável. Isso não significa necessariamente a necessidade de uma solução completa de chave pública. Por exemplo, alguns serviços online profissionais e empresariais exigem um nome de usuário e senha para acesso, usando uma tecnologia de controle de acesso menos cara e mais simples do que os sistemas de criptografia de chave pública. Neste contexto, a assinatura eletrônica é criada pelo uso de um nome de usuário e senha, que podem autenticar o usuário e expressar a

intenção de ser vinculado a tarifas de cobrança ou outros termos, dependendo do entendimento entre as partes.

Para o contexto jurídico, os documentos digitais contestados judicialmente merecem uma atenção especial quanto ao seu valor probatório. Roßnagel e Pfitzmann (2003) destacam que, quando uma declaração de vontade é contestada, cabe à parte que se apoia nessa declaração provar sua autenticidade. No caso de declarações contidas em e-mails, o desafio é ainda maior, pois elas podem ser facilmente alteradas sem deixar rastros visíveis. Os auores apontam que *„elektronisch übertragene oder gespeicherte Daten ... verändert werden, ohne dass dies Spuren hinterlässt und nachgewiesen werden kann*"[32]. Isso significa que a integridade da declaração original não pode ser provada apenas pela apresentação do arquivo eletrônico.

Segundo os autores, além da autenticidade do remetente, a integridade da informação durante a transmissão é outra preocupação. E-mails podem ser alterados durante o trânsito em redes abertas sem que o destinatário perceba. A falta de rastreabilidade de alterações nos e-mails torna difícil provar a integridade da informação original. Os registros de log dos servidores de e-mail poderiam fornecer informações sobre o envio ou o caminho da mensagem pela Internet. No entanto, os autores argumentam que nem todos os servidores registram as informações necessárias para a prova, e mesmo quando o fazem, esses dados podem não estar mais disponíveis ou acessíveis devido às práticas de exclusão de dados e restrições de privacidade.

Para Roßnagel e Pfitzmann, a autenticidade também é desafiada pelo fato de que muitos sistemas de e-mail permitem o envio de mensagens sem a necessidade de uma senha, e até mesmo quando as senhas são usadas, elas podem ser vulneráveis a ataques. Os autores observam que *„selbst wenn aussagekräftige Protokolldaten vorgelegt werden könnten ... könnte dennoch ein Missbrauch dieses Accounts durch Dritte erfolgt sein*"[33].

A realidade consubstanciada nas assinaturas eletrônicas (realizadas pela pessoa em um dispositivo eletrônico como se estivesse assinando um papel) representam um novo desafio para a análise jurídica da prova em casos de litígios. Conforme Harralson (2013, p. 111), a informação biométrica das assinaturas é utilizada em sistemas de segurança baseados em biometria. Uma das

32 Tradução livre: dados transmitidos ou armazenados eletronicamente ... podem ser alterados sem deixar rastros e sem que isso possa ser comprovado.

33 Tradução livre: mesmo que registros de log detalhados possam ser apresentados ... ainda assim, o abuso dessa conta por terceiros pode ter ocorrido.

novas considerações na avaliação forense não envolve apenas dados eletrônicos computadorizados, mas também o hardware usado para realizar assinaturas eletrônicas, como o tablet. A avaliação dos sistemas de assinatura eletrônica revela uma grande variedade de sistemas no mercado, tanto na captura de assinaturas eletrônicas quanto na análise forense automatizada dessas assinaturas. A falta de padronização, tanto do ponto de vista de captura quanto de verificação, complica a análise forense desses tipos de assinaturas.

Hoje em dia, diversos prestadores de serviços pedem aos consumidores que assinem um contrato utilizando o dedo ou uma caneta em um tablet para validar o negócio jurídico. Harralson lembra um caso legal em que se verificou que os examinadores de documentos forenses precisam estar cientes de que examinar assinaturas eletrônicas apenas com base em imagens de rastreamento estático não é considerado a melhor evidência disponível em casos de assinaturas eletrônicas quando dados biométricos estão disponíveis. Recomenda-se que os examinadores de documentos colaborem com especialistas em evidências de computador e trabalhem dentro de um quadro metodológico.

3.4 FATORES DE EFICÁCIA DO NEGÓCIO JURÍDICO.

Além da questão da validade das assinaturas digitais, que é um aspecto determinante na era dos bits, é imprescindível considerar também a eficácia do negócio jurídico, um elemento fundamental que transcende a mera conformidade com os requisitos legais. A eficácia de um negócio jurídico, especialmente em um contexto digital, não se limita apenas à sua validade legal, mas engloba a efetiva realização dos efeitos jurídicos desejados pelas partes envolvidas. Isso implica em uma análise detalhada de como as assinaturas digitais e as tecnologias associadas influenciam a capacidade do negócio jurídico de produzir os resultados pretendidos, considerando as particularidades do ambiente digital, como a segurança dos dados, a autenticidade das partes, a informação e a integridade dos documentos. Além de assegurar a validade legal das assinaturas digitais, é crucial garantir que elas contribuam para a eficácia do negócio, assegurando que os objetivos jurídicos e práticos sejam efetivamente alcançados no ambiente digital.

De acordo com Azevedo (2002, p. 51-51), a validade é uma característica intrínseca ao negócio jurídico, justificando sua existência teórica. A validade é influenciada por diversos fatores, como o papel da vontade, a causa, e os limites da autonomia privada em relação à forma e ao objeto do negócio. Esse conjunto de características confere ao negócio jurídico um tratamento especial dentro do

ordenamento jurídico. O autor ressalta que «o ordenamento jurídico, uma vez que autoriza a parte, ou as partes, a emitir declaração de vontade, à qual serão atribuídos efeitos jurídicos de acordo com o que foi manifestado como querido, procure cercar a formação desse especialíssimo fato jurídico de certas garantias, tanto no interesse das próprias partes, quanto no de terceiros e no de toda a ordem jurídica".

A validade é definida por Azevedo como a conformidade do negócio jurídico com as regras jurídicas, sendo um pré-requisito para sua existência dentro do mundo jurídico. O autor clarifica: "Validade é, como o sufixo da palavra indica, qualidade de um negócio existente".

No que concerne à eficácia, Azevedo estabelece que este é um aspecto distinto, embora relacionado à validade. A eficácia diz respeito aos efeitos jurídicos do negócio, especialmente aos efeitos típicos ou desejados. É crucial distinguir entre um ato válido e eficaz e um ato nulo e ineficaz, pois existem situações em que um negócio jurídico nulo pode produzir efeitos jurídicos (os "efeitos do nulo") e um negócio válido pode ser ineficaz.

Propõe Azevedo uma classificação dos fatores que influenciam a eficácia do negócio jurídico em três categorias: a) fatores de atribuição da eficácia em geral (como uma condição suspensiva); b) fatores de atribuição da eficácia diretamente visada; e c) fatores de atribuição de eficácia mais extensa. Cada uma dessas categorias abrange diferentes aspectos e circunstâncias que afetam como e quando o negócio jurídico produzirá os efeitos desejados, tanto entre as partes envolvidas quanto em relação a terceiros.

O aspecto volitivo influi sobre a validade e sobre a eficácia do negócio, conforme reconhece Azevedo (2002, p. 85), de modo que a compreensão do consumidor sobre o ambiente digital e o alcance que este tem sobre não só o negócio jurídico em si, mas também sobre questões relacionadas à sua personalidade devem ser consideradas pelo aplicador do direito. Neste contexto, o fornecedor tem papel fundamental na colaboração do consumidor a respeito das peculiaridades inerentes ao ambiente digital, de modo que o ordenamento jurídico deve ter em consideração o comportamento daquele na relação negocial para que se reconheça a eficácia do negócio jurídico tabulado.

Em um mundo cada vez mais digitalizado, as transações online se tornaram parte integrante da vida cotidiana. No entanto, a rapidez e a desmaterialização inerentes ao ambiente digital podem gerar desafios para a efetiva proteção do consumidor. Nesse contexto, a compreensão do consumidor assume um papel fundamental na validade e eficácia do contrato digital. As reflexões de Azevedo sobre a influência do aspecto volitivo na validade e eficácia do negócio jurídico

nos alertam para a importância da autonomia e da compreensão do consumidor no ambiente digital. A evolução tecnológica, embora tenha trazido inúmeras facilidades e expandido o acesso a bens e serviços, também suscitou preocupações quanto à capacidade dos consumidores de entenderem plenamente as transações realizadas nesse meio.

A complexidade e a rapidez com que as informações são apresentadas nas plataformas digitais podem dificultar o discernimento do consumidor, levando-o a decisões precipitadas e sem a devida ponderação dos riscos e responsabilidades envolvidos. A pressão de tempo, a apresentação condensada de informações e o uso de técnicas de persuasão são alguns dos elementos que podem influenciar negativamente a capacidade de escolha do consumidor no ambiente digital. Diante desse cenário, o fornecedor assume um papel fundamental e de relevância jurídica ao assegurar que o consumidor esteja plenamente informado sobre todos os aspectos relevantes da transação. Isso inclui, mas não se limitando aos(às):

a. características do produto ou serviço: o fornecedor deve formular uma descrição clara, precisa e completa do produto ou serviço oferecido, incluindo suas funcionalidades, especificações, riscos e potenciais problemas.

b. termos do contrato: o contrato digital deve ser redigido em linguagem clara, concisa e de fácil compreensão, evitando termos técnicos e jurídicos obscuros. As informações sobre preço, prazos de entrega, forma de pagamento, política de troca e devolução, garantias e responsabilidades devem ser facilmente acessíveis e destacadas.

c. outras informações relevantes: o fornecedor deve prover qualquer outra informação que possa influenciar a decisão do consumidor, como custos adicionais, política de privacidade e uso de dados pessoais, termos de rescisão do contrato, etc.

A apresentação de informações de maneira clara, acessível e sem ambiguidades é fundamental para garantir a liberdade de escolha do consumidor. O uso de linguagem simples, recursos visuais e ferramentas interativas pode contribuir para tornar o processo de compra mais transparente e consciente.

É essencial que o ordenamento jurídico reconheça e se adapte às peculiaridades das transações digitais, protegendo os consumidores contra práticas abusivas e garantindo que sua vontade seja tão respeitada quanto seria em transações presenciais. Isso implica não apenas na aplicação dos princípios de direito do consumidor já existentes, mas também na elaboração de novas diretrizes específicas para o ambiente digital.

Algumas medidas que podem ser tomadas para fortalecer a proteção do consumidor no ambiente digital, tais como:

a. exigência de informações pré-contratuais claras e completas: o fornecedor deve fornecer ao consumidor todas as informações necessárias para que ele possa tomar uma decisão informada sobre a compra, assim como disponibilizar os registros detalhados da própria fase negocial.

b. direito de arrependimento ampliado: o consumidor deve ter um prazo razoável para cancelar a compra sem custos adicionais, mesmo após a entrega do produto ou serviço.

c. mecanismos de resolução de conflitos online: plataformas online de resolução de conflitos podem facilitar a resolução de problemas entre consumidores e fornecedores de forma rápida e eficiente, com ao menos as mesmas facilidades de interação e comunicação que existiram para a formação do contrato.

d. educação e conscientização do consumidor: campanhas educativas sobre os direitos e deveres dos consumidores no ambiente digital (assim como os riscos associados) são essenciais para que eles possam exercer seus direitos de forma consciente.

Ao garantir a compreensão do consumidor e fortalecer sua proteção, pode-se promover um ambiente digital mais justo e seguro para todos, favorecendo a validade e eficácia dos contratos.

3.5 JURISPRUDÊNCIA RELEVANTE E ANÁLISE DE CASOS

A pesquisa sobre a validade da assinatura eletrônica em contratos digitais deve enfrentar as discussões que são tratadas nos tribunais, visto que neles os litígios são apresentados em caso de disputas. Obviamente, não se esquece da possibilidade de utilização do juízo arbitral ou outros meios de solução de controvérsias. Todavia, diante da cultura brasileira de busca pela solução judicial dos litígios, este exame se faz necessário em nossa realidade.

No contexto jurídico contemporâneo, principalmente diante da massificação dos canais digitais e plataformas, a validade dos contratos digitais, especialmente no que tange às assinaturas digitais, representa um tema de relevante discussão. Neste ponto da pesquisa trataremos da jurisprudência relevante sobre o tema, buscando explorar e delinear o panorama atual da jurisprudência pertinente a este tema, concentrando-se especificamente nas

questões judiciais que emergem das disputas relacionadas às assinaturas digitais. Esta seleção jurisprudencial é essencial para compreender a aplicação prática e a interpretação dos princípios legais em casos concretos, permitindo uma análise detalhada da forma como os tribunais têm abordado a validade dessas assinaturas digitais.

Primeiramente, abordaremos como a jurisprudência tem reconhecido, ou não, a validade das assinaturas digitais em casos específicos. Esta análise é fundamental, pois reflete não apenas a conformidade com as normativas vigentes, mas também a adaptação do direito às inovações tecnológicas que permeiam as relações contratuais na era digital. Através desta perspectiva, será possível identificar padrões decisórios, bem como as variadas interpretações jurídicas que fundamentam a aceitação ou rejeição dessas assinaturas em diferentes contextos.

A análise da jurisprudência específica sobre as relações de consumo, em relação aos contratos digitais, será abordada com detalhes no capítulo próprio. Este delineamento tem o propósito de fornecer uma compreensão mais clara e segmentada, considerando as peculiaridades e desafios que as relações de consumo impõem ao direito digital e à jurisprudência correlata.

Este subtítulo não apenas estabelece o cenário atual da jurisprudência sobre a validade das assinaturas digitais, mas também prepara o terreno para uma discussão mais aprofundada sobre a aplicação desses preceitos nas relações de consumo, que será devidamente explorada no próximo capítulo. Com esta abordagem, busca-se oferecer uma visão holística e detalhada, que é indispensável para a compreensão integral dos desafios jurídicos apresentados pelos contratos digitais na sociedade moderna.

Cabe anotar que a interpretação judicial da validade das assinaturas digitais, conquanto haja um certo grau de objetividade por meio do uso de chaves públicas, podem existir situações limítrofes, especialmente quando tratamos de assinaturas eletrônicas (gênero), onde o grau de subjetividade é elevado em razão da diminuição do elemento assecuratório da identidade da pessoa. Neste

caso, cabe ao juiz[34], com sua atividade criativa, inerente à atividade decisória, reconhecer ou não a validade, porém assegurando um certo grau de coerência com a ordem jurídica, visto que a previsibilidade decorre da necessidade de "o homem ter segurança para conduzir, planificar e conformar autônoma e responsavelmente a sua vida" (Gouveia; Breitenbach, 2015, p. 508)[35].

No STF e STJ não há discussão em sede de precedentes qualificados sobre assinatura digital ou a infraestrutura de chaves públicas. Todavia, a revogada Resolução nº 01/2010 do STJ, em seu art. 21, atribuía a responsabilidade aos usuários pelo sigilo da chave privada de sua identidade digital, login e senha. Esta norma foi utilizada pela Segunda Turma do STJ para não conhecimento de petição eletrônica. No AgRg no AREsp 217.075-PE, julgado em 09 de outubro de 2012, o STJ abordou uma questão fundamental no contexto da era digital, especialmente no que se refere à prática jurídica: a validade e a autenticidade das petições eletrônicas assinadas digitalmente. A Decisão se concentra na necessidade de haver congruência entre o titular do certificado digital e o advogado autor da petição.

34 O papel do juiz na aplicação do direito, conforme apontado por Lúcio Grassi de Gouveia em referência ao pensamento de Castanheira Neves, transcende a mera aplicação de normas jurídicas preexistentes. O juiz, nesta perspectiva, atua como um agente criativo e construtor do direito. Essa atividade criadora não se restringe à execução passiva de normas, mas envolve uma participação ativa na formação normativa do direito, especialmente por meio de suas decisões judiciais concretas e históricas. Neste contexto, o pensamento jurídico é concebido como normativamente constitutivo, indicando que a jurisprudência não apenas interpreta ou aplica o direito, mas também contribui significativamente para a sua construção e evolução. Em outras palavras, a prática judiciária é um espaço de criação jurídica, onde o juiz, ao lidar com casos específicos e suas peculiaridades, tem a oportunidade de moldar e desenvolver o direito. Esta abordagem reconhece que muitas situações apresentadas ao judiciário não encontram respostas diretas ou claras na legislação existente. Nestes casos, o juiz é chamado a exercer sua criatividade jurídica para preencher lacunas, interpretar normas de maneira inovadora ou aplicar princípios gerais do direito de forma que resolva o conflito de forma justa e equitativa. A magnitude dessa criatividade varia conforme as peculiaridades do caso concreto, indicando que o direito é um organismo vivo e em constante evolução, moldado não apenas pelo legislador, mas também pela judicatura. Assim, a função do juiz é essencial para a dinâmica do direito, pois suas decisões não apenas solucionam disputas individuais, mas também guiam e influenciam o desenvolvimento do ordenamento jurídico como um todo (GOUVEIA, 2000, p. 24).

35 A pertinência da atividade criadora do juiz se torna ainda mais evidente diante dos novos desafios impostos pela assinatura eletrônica e outras inovações tecnológicas no âmbito jurídico. A assinatura eletrônica, sendo um fenômeno relativamente recente, traz consigo uma série de questionamentos legais e práticos que não estão completamente abordados pela legislação atual. Lacunas irão emergir. Isso demanda do juiz uma habilidade interpretativa inovadora e criativa para aplicar princípios jurídicos existentes a situações novas e muitas vezes sem precedentes. A capacidade do juiz de adaptar e aplicar o direito a essas novas realidades tecnológicas é fundamental para garantir a segurança jurídica, a validade dos atos processuais eletrônicos e a proteção de direitos em um contexto digital em constante mudança. Essa atividade criativa do juiz, portanto, é crucial para enfrentar os desafios e incertezas trazidos pela evolução tecnológica, garantindo uma interpretação e aplicação do direito que estejam em consonância com os avanços da sociedade e as necessidades emergentes da era digital.

É essencial entender o contexto legal e normativo então discutido. A Lei n. 11.419/2006, que regula a informatização do processo judicial, estabelece a possibilidade de uso de documentos eletrônicos e sua assinatura por meio de certificado digital. Conforme essa lei e a Resolução n. 1/2010-STJ, a assinatura eletrônica tem o objetivo de identificar de maneira inequívoca o signatário do documento, garantindo a autenticidade e a integridade do mesmo.

Neste caso específico, a jurisprudência destaca a importância da identidade entre o titular do certificado digital e o autor da petição. A razão para isso é dupla: (1) assegurar que o documento foi realmente elaborado e enviado pelo advogado que ele afirma ser, e (2) garantir a segurança jurídica e a confiabilidade do processo eletrônico. A falta de correspondência entre o titular do certificado e o advogado indicado como autor da petição gera uma desconformidade com as disposições legais e regulamentares, o que leva à inexistência da petição eletrônica para efeitos processuais.

Esta interpretação da Segunda Turma está alinhada com a responsabilidade atribuída aos usuários de manter o sigilo da chave privada de sua identidade digital, conforme estabelecido pela revogada Resolução n. 1/2010-STJ. Isso implica que os advogados devem não apenas zelar pela segurança de suas credenciais digitais, mas também assegurar que as petições enviadas eletronicamente sejam devidamente assinadas com seu próprio certificado digital.

A decisão citada reforça a necessidade de conformidade estrita com os requisitos legais e regulamentares para a validade das petições eletrônicas, enfatizando a importância da assinatura eletrônica como mecanismo de autenticação e segurança no processo judicial eletrônico. Este posicionamento visa salvaguardar a integridade do processo jurídico e manter a confiança nas transações e comunicações eletrônicas dentro do sistema de justiça.

Deve-se, contudo, chamar a atenção pelo fato de se invocar a Resolução nº 01/2010, art. 21, que trata do sigilo da chave privada no contexto do caso julgado que abordou a utilização da chave pública. Conforme citado pelo Ministro Herman Benjamin, Relator, em seu Voto:

> "Não conheço do Agravo Regimental de fls. 97-101, e-STJ, tendo em vista que, conforme Certidão da Seção de Protocolo de Petições do STJ (fl. 102, e-STJ), o nome do advogado indicado como autor da presente petição não confere com o do **titular do certificado digital utilizado para assinar a transmissão eletrônica do documento**.
>
> De acordo com a redação do art. 21, I, da Resolução STJ n. 1, de 10 de fevereiro de 2010, é de exclusiva responsabilidade dos usuários, entre outras coisas, o sigilo da chave privada de sua identidade digital, login e senha.

> Com efeito, a assinatura eletrônica destina-se à identificação inequívoca do signatário do documento, de forma que, não havendo identidade entre o **titular do certificado digital usado para assinar o documento e os advogados indicados como autores da petição**, deve esta ser tida como inexistente, haja vista o descumprimento do disposto nos arts. 1º, § 2º, III, e 18, ambos da Lei 11.419/2006, e nos arts. 18, § 1º, e 21, I, da Resolução STJ n. 1, de 10 de fevereiro de 2010" (destaquei)

Outro ponto de destaque que foi julgado pelo STJ diz respeito à diferenciação entre assinatura digitalizada em assinatura digital. No julgamento do AgInt no AREsp 1691485 / PE pela Terceira Turma do STJ, foi abordada a representação processual e especificidades das assinaturas no contexto digital, especialmente em procedimentos judiciais. A decisão destaca a distinção entre assinatura digitalizada (ou escaneada) e assinatura digital baseada em certificado digital, no contexto de uma ação cominatória cumulada com compensação por danos morais.

Essencialmente, o caso em questão gira em torno da validade de um recurso submetido por um advogado que não apresentou procuração nos autos. A Súmula 115 do STJ estabelece que, na instância especial, é inexistente recurso interposto por advogado sem procuração nos autos. Isso significa que, para um recurso ser considerado válido, é necessário que o advogado que o subscreve tenha sua representação processual devidamente regularizada.

O ponto central da decisão é a diferenciação entre dois tipos de assinatura eletrônica:

1. Assinatura Digitalizada ou Escaneada: Esta forma de assinatura envolve a inserção de uma imagem de uma assinatura manuscrita em um documento eletrônico. Essa prática, embora comum, não oferece os mesmos níveis de segurança e autenticidade que uma assinatura digital baseada em certificado digital. Ela é considerada insuficiente para fins de comprovação de representação processual em instâncias superiores, como o STJ.

2. Assinatura Digital Baseada em Certificado Digital: Este tipo de assinatura utiliza um certificado digital emitido por uma Autoridade Certificadora credenciada. Ela oferece maior segurança e é juridicamente reconhecida, pois assegura a autenticidade e a integridade do documento, além de vincular de forma inequívoca o documento ao seu signatário.

No julgamento em questão, o STJ reiterou que a assinatura digitalizada não é equiparada à assinatura digital baseada em certificado digital para fins processuais. Isso implica que, mesmo que um documento seja subscrito por um advogado com uma assinatura digitalizada, essa assinatura não satisfaz os

requisitos de autenticação exigidos para a representação processual em instâncias superiores.

A decisão reforça a necessidade de cumprimento rigoroso das normas processuais relacionadas à representação processual e à autenticação de documentos no ambiente digital, evidenciando a distinção entre diferentes formas de assinatura eletrônica e a importância da assinatura digital baseada em certificado digital no processo judicial.

Quanto à equivalência funcional entre documento tradicional e digital, o Tribunal de Justiça do Paraná, ao julgar o Processo nº 0006574-55.2022.8.16.0193, assinalou aspectos importantes sobre a validade e execução de títulos executivos extrajudiciais no contexto da assinatura eletrônica. A decisão aborda a equivalência entre contratos eletrônicos e tradicionais, e as exigências para que um contrato eletrônico seja considerado um título executivo extrajudicial válido.

A decisão reforça o princípio da equivalência funcional entre contratos tradicionais e eletrônicos, estabelecendo que a pactuação eletrônica possui a mesma validade e força jurídica que um contrato em papel, estando em consonância com a tendência moderna de reconhecer as transações digitais como equivalentes às suas contrapartes físicas, desde que cumpram certos requisitos de autenticidade e integridade.

A decisão a Corte Paranaense faz uma distinção importante entre um contrato eletrônico assinado digitalmente e um que não possui essa característica. O Superior Tribunal de Justiça (STJ), conforme citado no julgado, já reconheceu a executividade de contratos eletrônicos que contêm uma assinatura digital certificada por uma autoridade certificadora. No caso em análise, a cédula de crédito bancário não possuía indicação de que foi assinada eletronicamente, e o documento juntado para provar a suposta assinatura digital indicava um número de contrato diferente, levantando dúvidas sobre sua autenticidade e integridade.

Também aponta a decisão para a necessidade de clareza quanto à assinatura digital do contrato para que este seja considerado um título executivo extrajudicial. No caso, a ausência de um certificado digital emitido por uma autoridade certificadora credenciada prejudicou a verificação da autenticidade e da integridade do contrato, o que, por sua vez, afastou a sua executividade.

Esta decisão do Tribunal de Justiça do Paraná serve como referência na presente pesquisa por enfatizar a importância da clareza e da certificação adequada das assinaturas digitais em contratos eletrônicos, especialmente quando se tratam de títulos executivos extrajudiciais, destacando o equilíbrio entre a validade jurídica das formas digitais e a necessidade de cumprir requisitos essenciais para garantir a segurança jurídica e a confiabilidade do processo.

4 PROTEÇÃO AO CONSUMIDOR NA ASSINATURA DOS CONTRATOS DIGITAIS

4.1 CONTEXTO DA PROTEÇÃO DO CONSUMIDOR NO AMBIENTE DIGITAL

A proteção ao consumidor nos contratos digitais é uma área de crescente importância e complexidade no cenário jurídico atual, especialmente à luz da expansão do comércio eletrônico e da digitalização das transações comerciais. Este tema abrange uma gama de questões que vão desde a segurança das transações eletrônicas até a garantia de direitos fundamentais dos consumidores em um ambiente digital. Sobre o presente capítulo, nossa pesquisa irá explorar os riscos e proteções ao consumidor, o papel das agências reguladoras e órgãos de proteção, e as políticas de compliance e melhorias das práticas de mercado pelas empresas.

Quanto aos riscos, temos em primeira linha a vulnerabilidade dos dados em transações eletrônicas pode levar a fraudes, roubo de identidade e violações de privacidade. Frequentemente, há falta de clareza nas informações sobre produtos e serviços oferecidos digitalmente, o que pode induzir o consumidor ao erro. Diferentes jurisdições possuem leis variadas relativas ao comércio eletrônico, o que pode criar confusão e riscos legais para consumidores transnacionais, inclusive com a popularização do comércio com empresas sediadas em outros países, como a Alibabá, Shopee, Shein etc.

Muitos países implementaram leis específicas para proteger os consumidores no ambiente digital, como regulamentos sobre privacidade de dados e direitos de cancelamento de compras online. Quanto aos direitos do consumidor, a informação assume papel relevante, pelo que se enfatiza a necessidade de consentimento informado, direito a informações claras e precisas, e a proteção contra práticas comerciais injustas.

Neste contexto, também merece destaque o papel das Agências Reguladoras e Órgãos de Proteção. Agências como a ANATEL no Brasil, por exemplo, regulam aspectos das transações eletrônicas, garantindo que as empresas cumpram as normas de proteção ao consumidor. O BANCO CENTRAL possui papel de destaque com a regulação do mercado financeiro. Os PROCONS também possuem atribuições relevantes no contexto da proteção do consumidor, papel este que também vem sendo desempenhado por associações e empresas privadas como o RECLAME AQUI. Alguns destes órgãos exercem poderes regulatórios,

outros fiscalizatórios, outros educacionais para consumidores sobre seus direitos e riscos no comércio eletrônico.

Também as empresas merecem atenção da pesquisa, visto que suas políticas de *compliance* e melhorias das práticas de mercado são importantes para a efetivação dos direitos dos consumidores. As empresas devem estabelecer políticas internas que garantam a adesão às leis e regulamentos de proteção ao consumidor. Isso inclui a transparência nas informações sobre produtos e serviços, e a responsabilidade no tratamento de dados pessoais dos consumidores. Algumas empresas adotam padrões mais elevados de proteção ao consumidor como parte de uma estratégia de autorregulação e diferenciação no mercado, inclusive investindo em tecnologias avançadas para garantir a segurança das transações e proteger os dados dos consumidores.

A proteção ao consumidor nos contratos digitais é um campo dinâmico e complexo, exigindo uma abordagem multifacetada que inclui legislação robusta, regulamentação efetiva, educação do consumidor e práticas de mercado responsáveis. À medida que o comércio eletrônico continua a se expandir, esses aspectos se tornam cada vez mais cruciais para a proteção dos direitos do consumidor e a manutenção da confiança no ambiente digital.

4.2 RISCOS E PROTEÇÕES AO CONSUMIDOR EM TRANSAÇÕES ELETRÔNICAS

Os principais riscos para os consumidores envolvendo negócios jurídicos em ambiente virtual indicam a vulnerabilidade dos dados pessoais e o acesso não autorizado por terceiros, de modo que uma contratação, por exemplo, pode ser realizada em nome de uma pessoa, sem seu consentimento, favorecendo outrem. Este ambiente virtual se desenvolve em razão da facilidade que os consumidores encontram de atender suas necessidades, mas nele subjaz a questão da confiança. Esta confiança muitas vezes está associada à escala de reputação dos fornecedores que algumas plataformas fornecem, como por exemplo o MERCADO LIVRE, MAGALU, AMAZON etc (Dutenkefer,; Leal, 2018).

Segundo Feitosa e Garcia (2015), a crescente importância dos sistemas de reputação no comércio eletrônico tem sido relevante quanto à preocupação com segurança e privacidade nesse setor. O aumento de crimes e fraudes na internet elevou a percepção de riscos nas compras online, levando os consumidores a serem mais cautelosos e a buscarem informações sobre os vendedores. Essa necessidade de conhecer melhor o vendedor antes de uma decisão de compra

incentivou a criação de sistemas de reputação, que reduzem a assimetria de informações entre consumidores e vendedores e estabelecem escores e selos de confiança. A relevância desses sistemas é enfatizada em mercados como o brasileiro, onde a confiança nas práticas sociais não é amplamente difundida e o volume de negócios online está em expansão. Os consumidores tendem a considerar avaliações e experiências passadas na escolha de lojas ou produtos.

Contudo, acrescentam os autores, diferentes entidades estão envolvidas nos sistemas de reputação, incluindo consumidores, vendedores e empresas que administram os sistemas. Isso pode levar a vieses nos resultados e escores publicados. A literatura nacional sobre sistemas de reputação é escassa, o que gera uma lacuna sobre o papel desses sistemas no comércio eletrônico brasileiro. Uma pesquisa da PROCON em São Paulo revelou que varejistas com altos escores de confiança figuram entre as empresas com mais reclamações fundamentadas. Isto coaduna com a tese de que o Código de Defesa do Consumidor seja considerado um microssistema jurídico, inter e multidisplinar (Filomeno, 2012), onde informações associadas à relação de consumo, que não se limitam apenas aos produtos e serviços, são levadas em consideração pelo consumidor.

O trabalho desenvolvido por Feitosa e Garcia foca na relação teórica entre confiança e reputação, utilizando dados de dois dos principais sistemas de reputação brasileiros, eBIT e Reclame Aqui, para responder se há coerência entre os escores apresentados por eles. Foram coletados dados de lojas virtuais avaliadas por esses sistemas e comparados os índices de reputação de empresas com diferentes selos de confiança, isso com o objetivo de analisar a coerência de selos e escores aferidos por diferentes empresas no comércio eletrônico de uma mesma região.

Exploram Feitosa e Garcia a relação teórica entre confiança e reputação nos sistemas de reputação, apresentando uma nova abordagem para analisar a coerência dos escores de reputação, utilizando o teste ANOVA para comparação de médias. Sua pesquisa revelou uma incoerência entre os escores de reputação estudados, sugerindo que eles não refletem adequadamente as relações teóricas estabelecidas na literatura. Este resultado implica que há variáveis adicionais influenciando a relação entre confiança e reputação que não foram consideradas. Assim, o estudo sugere a necessidade de investigações futuras sobre as fontes de vieses e características específicas dos escores de reputação no contexto brasileiro. O estudo também propõe o desenvolvimento de novas métricas e técnicas para avaliar escores e selos concedidos pelos sistemas de reputação nacionais. Há um interesse em identificar discrepâncias entre os índices de empresas de diferentes segmentos de mercado. O estudo oferece insights

empíricos, sugerindo que os consumidores busquem informações de diversas fontes para reduzir riscos no processo de compra. Para empresas e desenvolvedores de sistemas de reputação, recomendam os autores a revisão dos escores utilizados, de modo que reflitam fielmente os conceitos de confiança e reputação que se propõem a medir. Uma alternativa seria integrar diferentes mecanismos de reputação para gerar um escore composto que mantenha a coerência entre os mecanismos. Por fim, apresentam como sugestão que os órgãos de defesa do consumidor invistam em sistemas ou empresas de certificação para assegurar a integridade dos índices publicados sobre empresas de comércio eletrônico. Esta abordagem visa garantir que os consumidores tenham acesso a informações confiáveis sobre a reputação das empresas, contribuindo para um ambiente de comércio eletrônico mais transparente e confiável.

4.2.1 PROTEÇÃO DE DADOS

Uma das principais vulnerabilidades dos consumidores diz respeito ao fato de que o registro de sua identidade não depende apenas de um ato volitivo seu consubstanciado em uma declaração pessoal, escrita ou oral, como tradicionalmente é tratado pelo direito civil. Os registros públicos que individualizam a pessoal, como a certidão de nascimento, documentos de identificação, geral e profissional, cadastro de contribuinte, cadastro em entidades e empresas, são dados que não ficam confinados em um ambiente controlado.

Estes dados trafegam nos sistemas informáticos interconectados, onde perfis são criados para formar a identificação de uma pessoa, novos dados que vão além destes registros são coletados, voluntária ou involuntariamente.

Além dos dados relativos às pessoas, os sistemas informáticos trabalham com metadados. Segundo Luciano (2004), o conceito de metadados é frequentemente descrito como “dados sobre dados”, uma definição que, embora comum, é considerada superficial por não capturar a importância dos dados em contexto. Metadados são mais do que simples dados; eles descrevem e dão significado a outros dados, estabelecem como esses dados podem ser utilizados e auxiliam na transformação de dados brutos em conhecimento. Eles podem ser vistos como uma abstração de alto nível que fornece informações sobre dados de menor nível, e são fundamentais para a definição de objetos em ambientes de armazenamento de dados. A complexidade do termo “metadados” reside no seu amplo leque de significados e aplicações, o que torna sua definição exata desafiadora e, por isso, requer uma análise mais abrangente para uma compreensão completa. Em essência, as diversas interpretações de metadados convergem para a noção

de que seu propósito central é descrever dados, conferindo-lhes contexto e regras para sua correta aplicação e contribuindo para a criação de conhecimento.

Cabe lembrar que a necessidade de proteção de dados não emergiu em decorrência da informatização, mas com esta se intensificou. Em 1970, o estado alemão de Hesse, foi editada a "*hessisches Datenschutzgesetz*", tido como o primeiro diploma legal a tratar do assunto (Doneda, 2021, p. 3). Relata, ainda, Doneda (2021, p. 7) que desde a década de 1960, houve nos Estados Unidos uma crescente preocupação com a expansão do processamento automatizado de dados pessoais e a criação de bancos de dados informatizados. O projeto de um National Data Center, uma base de dados centralizada no país, gerou debates acalorados devido aos riscos à privacidade e liberdade percebidos pela sociedade. Essa discussão chegou ao Congresso estadunidense, onde se reconheceu que o avanço da tecnologia de processamento de dados pessoais carecia de regulamentações apropriadas para garantir a proteção necessária. Durante as audiências no Congresso, especialistas, incluindo o sociólogo Vance Packard, alertaram sobre os perigos do uso de informações pessoais para controle social. Packard expressou a preocupação de que o "Big Brother" estadunidense poderia não emergir como uma figura tirânica, mas sim como um burocrata estatal obcecado por eficiência. Ao concluir as audiências, o Deputado Cornelius Gallagher admitiu que, não obstante os benefícios potenciais para a eficiência governamental, o projeto do *National Data Center* também apresentava significativas ameaças à privacidade individual.

Na nossa Constituição de 1988, no capítulo 5º não há especificamente referência à proteção dos dados pessoais quanto ao seu uso por sistemas informatizados, todavia, depreende-se do princípio da dignidade da pessoa que esta proteção pode ser inferida, inclusive quanto à necessidade do consentimento livre para o seu uso. Conforme Sarlet (2021, p. 32), o direito à autodeterminação informativa é intrinsecamente ligado à dignidade da pessoa humana e ao direito ao livre desenvolvimento da personalidade. Esta conexão fundamenta-se na autonomia individual, enfatizando a importância crucial do consentimento no que tange à proteção de dados pessoais. O consentimento, que deve ser livre e informado, é uma exigência constitucional para a realização da autodeterminação informacional, formando um aspecto essencial do direito fundamental à privacidade.

A Lei nº 13.709, do dia 14 de agosto de 2018, introduziu no ordenamento jurídico brasileiro a Lei Geral de Proteção de Dados Pessoais (LGPD), destacando-se no seu art. 5º, inciso I, que para fins da lei, considera-se dado pessoal a informação relacionada a pessoa natural identificada ou identificável.

Os dados tratados, inclusive por meios digitais, são protegidos com o objetivo de proteção da liberdade, o que é importante para o tema proposto na presente pesquisa, que envolve a livre manifestação de vontade representada na assinatura digital para a formação de um vínculo obrigacional. O tratamento inadequado dos dados pessoais representa risco para as pessoas que podem passar à condição de obrigado em uma relação jurídica da qual não quis fazer parte. Diversas são as possibilidades de uso destes dados para a formação de contratos. Explica Brancher (2019) que a validade dos contratos eletrônicos, historicamente questionada devido à ausência de assinatura física, é hoje reconhecida pela possibilidade de classificar a manifestação de vontade em três categorias: interpessoal, intersistêmica e interativa. Na comunicação interpessoal, como e-mails e mensagens instantâneas, as partes se comunicam diretamente e cada uma expressa sua vontade em sua vez. Essa forma se assemelha ao contrato por correspondência, diferenciando-se pelo meio eletrônico em vez do papel, e ao contrato verbal à distância, como o telefone.

Na comunicação interpessoal, adita, a presença não é definida pela simultaneidade, mas pela natureza da comunicação, sendo necessário avaliar caso a caso para determinar a vinculação das partes. A comunicação intersistêmica ocorre quando sistemas de informação interagem automaticamente, sem intervenção humana direta, como no caso do Electronic Data Interchange (EDI) ou na Internet das Coisas (IoT), onde as máquinas executam comandos pré-programados para realizar operações como pedidos de estoque. Entretanto, lembra Brancher, os termos contratuais não são estabelecidos pelos sistemas automatizados, mas por contratos pré-existentes que definem as regras das transações. Esses contratos determinam como a vontade das partes é manifestada e as consequências jurídicas de cada solicitação. Já na comunicação interativa, arremata, uma pessoa envia uma manifestação de vontade por meio eletrônico e um sistema responde automaticamente, comum em plataformas online onde os usuários selecionam produtos, preenchem formulários e autorizam pagamentos, sendo essa a forma predominante de contratação eletrônica atualmente.

4.2.2 ACESSO E COLETA NÃO AUTORIZADOS

Diversas demandas judiciais buscam solucionar disputas relacionadas ao acesso não autorizado e uso de dados pessoais para a formação de um vínculo obrigacional. Conquanto o uso de chave pública não represente, pela sua maior segurança, uma quantidade significativa de reclamações dos consumidores e

demandas judiciais[36], os casos envolvendo acesso não autorizado com o uso de senha pessoal, token, assinatura com chaves privadas representam quantidade importante de demandas a serem resolvidas pela justiça[37].

Os dados obtidos sem o consentimento do consumidor, seja por meio de vazamento voluntário ou por falha de segurança, seja através de técnicas como o *phishing* podem causar dados em razão de tais dados serem utilizados para realizar operações que aparentemente seriam legítimas se praticadas pelos seus titulares (Pimentel, 2023b, p. 363).

Segundo Nascimento (2014), o *phishing* é uma forma de fraude online que visa roubar dados pessoais como senhas, informações financeiras e bancárias ou outros dados pessoais. O termo surgiu em 1996, associado a cibercriminosos que roubavam contas da *America Online* (AOL), e as contas hackeadas eram utilizadas como moeda de troca no submundo hacker. Com o tempo, o *phishing* evoluiu e se tornou mais sofisticado. Os ataques de *phishing* são realizados através de e-mails, aplicativos e sites falsos criados para parecerem confiáveis, com o objetivo de enganar as vítimas para que revelem suas informações. Os criminosos esperam que as vítimas abram as mensagens e cliquem em links maliciosos que permitem o acesso aos dados desejados. Esses golpes têm uma taxa de sucesso preocupante e são realizados em massa por meio de spam. Os ataques seguem um processo que inclui planejamento, no qual os alvos e objetivos são escolhidos; preparação, onde a "isca" é criada; o ataque, que é o envio das mensagens; coleta dos dados obtidos; a fraude, que é o uso desses dados; e, por fim, a etapa pós-ataque, que envolve a eliminação de evidências e, em casos de roubo monetário, a lavagem do dinheiro. Para evitar cair em golpes de *phishing*, segundo Nascimento, deve-se ter cautela ao abrir e-mails de remetentes desconhecidos, evitar downloads automáticos ou desnecessários, não executar arquivos não solicitados e manter o sistema operacional e softwares de segurança atualizados, preferencialmente configurados para atualizações automáticas.

Recente artigo publicado na Folha de São Paulo revela um novo método de coleta de dados para operações bancárias fraudulentas em que o consumidor, involuntariamente, acaba por autorizar a transferência do dinheiro para os

36 Não se encontram muitos julgados discutindo a validade de contratos em decorrência de violação das chaves públicas.

37 Existe farta jurisprudência sobre o tema, uso de senhas pessoais, cartões, assinaturas eletrônicas por meio de senha pessoal, uso de dados biométricos para a validade de contratos, especialmente bancários. Estas demandas são comumente encontradas nos juizados especiais, visto terem sido desenvolvidos para proporcionar uma solução mais célere às demandas de menor complexidade, especialmente relacionadas às relações de consumo (FINKELSTEIN, SOCCO NETO, 2010, p. 162)

golpistas. Segundo Teixeira (2023), um novo golpe, originário do Brasil, está direcionando seus esforços a lojas de shoppings e postos de gasolina para desviar pagamentos por aproximação. Divulgado pela Kaspersky, o esquema envolve o bloqueio da comunicação da máquina de cartão, induzindo o cliente a inserir o cartão fisicamente e digitar a senha. O malware Prilex, responsável pelo ataque, cria uma conexão falsa, redirecionando as informações do pagamento para os criminosos e permitindo compras fraudulentas. Este golpe afeta principalmente maquininhas com fio, pois a invasão se dá pelo computador do estabelecimento, onde há mais vulnerabilidades. O cibercriminoso, fingindo ser um representante técnico, visita o local para verificar a segurança do sistema e, se possível, instalar o *malware* (Pimentel, 2023b, p. 354). A escolha por shoppings e postos deve-se ao maior fluxo de dinheiro e à menor capacidade destes estabelecimentos em investir em segurança de TI. Desde a sua primeira detecção, o número de casos aumentou, e várias versões do malware foram identificadas. O Prilex, ativo desde 2014, já era conhecido por realizar "compras fantasmas" e agora parece estar se preparando para expandir suas operações para além do Brasil. Ainda segundo Teixeira, para se proteger, os consumidores devem contestar gastos indevidos e ficar atentos a mensagens de erro nas máquinas de cartão, preferindo insistir no pagamento por aproximação ou buscar formas alternativas de pagamento. Os lojistas devem verificar a identidade dos técnicos que entram em contato para evitar a instalação de softwares maliciosos.

Como se verificam nos exemplos acima, a criatividade dos criminosos na esfera digital para acessar e coletar dados pessoais para fins ilícitos é verdadeiramente ilimitada e constantemente evolutiva. A natureza do cibercrime é tal que se adapta rapidamente às mudanças tecnológicas e às contramedidas de segurança, explorando novas vulnerabilidades e enganando os usuários de maneiras cada vez mais sofisticadas.

Em razão de os dados pessoais possuírem valor econômico, existe um impulsionamento da criatividade para a prática de atos ilícitos, fazendo com que as empresas que utilizam estas tecnologias desenvolvam novas técnicas de segurança para proteção dos seus consumidores. A proliferação de big data e algoritmos avançados permitiu aos criminosos personalizar e automatizar ataques em larga escala, tornando-os mais eficazes, isso mediante técnicas de aprendizado de máquina para refinar suas táticas e mirar em vítimas específicas, aumentando as chances de sucesso.

Como se isso não fosse suficiente, diversas plataformas compartilham voluntariamente os dados pessoais dos seus usuários com terceiros, seja sem o

consentimento dos consumidores, seja mediante a inclusão de cláusulas específicas nos termos gerais de uso.

Bioni e Luciano (2021) fazem uma análise de diversos casos envolvendo o compartilhamento de dados por diversas plataformas com terceiros, fazendo considerações a respeito do "consentimento informado", que surgiu em 1950 e se estendeu para a medicina, direito e filosofia. Segundo os autores, o seu estudo parece fornecer alguns ganhos analíticos à discussão do consentimento no campo da proteção de dados pessoais. O referencial analítico consentimento como ato e consentimento como processo parece valioso para distinguirmos o uso do consentimento como salvaguarda daquele como base legal autorizativa do processamento de dados pessoais – e dos requisitos e obrigações que este último coloca. Foca-se, assim, a autodeterminação informacional do indivíduo para pensar, então, nas informações e mecanismos necessários para garanti-la. Essas complexificações, contudo, não são sinônimo de paralisia. Em termos operacionais, o cenário para a inovação é fértil. Aditam que a jurisprudência já tem se posicionado sobre algumas práticas estabelecidas – avaliando, por exemplo, as limitações e as possibilidades do uso de políticas de privacidade e boxes opt-in[38] à luz do Código de Defesa do Consumidor e da GDPR (Regulamento Geral de Proteção de Dados da União Europeia). Concluem que estudos empíricos comportamentais dos usuários também fornecem pistas, além do que painéis de controle de privacidade e a criação de jornadas com o usuário seriam algumas das possibilidades para endereçar a "fadiga do consentimento". No âmbito teórico, concluem, permanece uma agenda de pesquisa para se pensar como endereçar o consentimento, no contexto de uma economia de dados, diante das dinâmicas de assimetria de poder (e até de conhecimento) e vulnerabilidade de determinados grupos.

38 As abordagens opt-in e opt-out representam métodos distintos de gerenciamento do consentimento na coleta de dados pessoais, com implicações importantes para a privacidade do usuário. O opt-in exige que os usuários concedam explicitamente permissão antes que seus dados sejam coletados, colocando a privacidade como configuração padrão e alinhando-se com legislações rigorosas de proteção de dados que exigem consentimento ativo. Por outro lado, o opt-out permite a coleta de dados por padrão, cabendo ao usuário recusar ou retirar seu consentimento, o que pode comprometer a proteção da privacidade ao colocar o ônus da ação sobre o indivíduo. A escolha entre essas duas abordagens afeta diretamente o controle do usuário sobre suas informações pessoais e a transparência das práticas de coleta de dados das empresas.

4.2.3 USO DE CHAVES PRIVADAS

A identificação digital é um processo de verificação e autenticação que confirma a identidade de um usuário ao realizar transações bancárias e negócios pela internet, tendo como objetivo principal garantir que as informações e os dados financeiros estejam protegidos e sejam acessados apenas por pessoas autorizadas. Visando garantir a segurança jurídica da autorização, são utilizadas diversas tecnologias e métodos de comprovação de identidade, sendo os mais comuns:

1. Senhas e nomes de usuário: são as formas mais básicas de identificação digital. O usuário cria um nome de usuário e uma senha únicos, que serão solicitados sempre que precisar acessar sua conta bancária ou realizar transações online.

As senhas são qualificadas como fortes envolve questões como o comprimento (acima de 08 caracteres), complexidade (inclusão de caracteres especiais, como #, &, %), aleatoriedade (evitando sequência de números ou letras que sejam facilmente memorizáveis), utilização exclusiva.

Todavia, este sistema não garante a autenticidade do consumidor em razão de esta poder ficar armazenada na plataforma, estando sob riscos de vazamento.

2. Autenticação de dois fatores (2FA): é um método de segurança adicional que requer que o usuário forneça duas formas diferentes de identificação. Geralmente, envolve a combinação de algo que o usuário sabe (como uma senha) e algo que o usuário possui (como um token ou dispositivo móvel). Um exemplo comum é o envio de um código por SMS ou aplicativo de autenticação para o celular do usuário, que deve ser inserido juntamente com a senha para acessar a conta.

Segundo Freire (2021), a autenticação de dois fatores (2FA) é uma medida de segurança essencial no mundo digital, oferecendo uma camada adicional de proteção para contas online. Freire destaca que o 2FA, ou "*two-factor authentication*", adiciona uma segunda verificação de identidade durante o processo de login, o que é crucial especialmente em casos de vazamento de senhas. Esta funcionalidade está disponível em muitos serviços online populares, como Google, Facebook, Instagram, Amazon, entre outros, oferecendo diferentes métodos de verificação. Estes podem incluir códigos via SMS, dispositivos de token, biometria e outros. A autenticação de dois fatores serve para confirmar a identidade do usuário, exigindo uma segunda forma de verificação após o login e senha, aumentando significativamente a segurança da conta. O processo de

2FA pode variar, mas a forma mais comum envolve o envio de um código de verificação para o telefone do usuário. Mesmo que a senha seja comprometida, a presença do segundo fator dificulta o acesso não autorizado. A biometria, como impressões digitais ou leitura da íris, representa uma forma sofisticada de 2FA, enquanto tokens USB, como a Titan Key do Google, geram códigos únicos para o login. Aplicativos como Authy e Google Authenticator também fornecem códigos de autenticação, e alguns serviços enviam notificações push para o celular ao invés de códigos numéricos. Ressalta Freire que senhas são fatores de segurança fracos por si só. Muitos usuários optam por senhas simples para facilitar a memorização, ou reutilizam a mesma senha em diversas contas, práticas que aumentam a vulnerabilidade a ataques. Com o aumento de atividades online, especialmente devido à pandemia de Covid-19, os riscos de golpes como *phishing* cresceram exponencialmente, tornando a segurança online ainda mais crítica.

Afirma Freire que para usar a autenticação de dois fatores, é necessário que a plataforma suporte esse recurso. Geralmente, a ativação ocorre nas configurações de segurança da conta. O Google, por exemplo, oferece métodos de 2FA via notificação push, token físico, ou mensagem de texto/voz. O Facebook e o Instagram também oferecem várias opções, incluindo dispositivos físicos, SMS, apps de autenticação e geradores de códigos. Alguns aplicativos fornecem códigos de reserva para situações em que o método padrão de 2FA não está disponível, como em áreas sem cobertura de celular. Estes códigos são de uso único e devem ser armazenados em local seguro. Assim, a autenticação de dois fatores não é apenas uma recomendação, mas uma necessidade para proteger a segurança online em um mundo cada vez mais conectado e vulnerável a ataques cibernéticos.

Para comprovar a identificação digital, os usuários devem passar pelos processos de verificação e autenticação exigidos pelas instituições financeiras ou plataformas de negócios online. Isso pode envolver a combinação de várias tecnologias e métodos mencionados acima para garantir a máxima segurança e proteção das informações e dados financeiros do usuário.

Algumas operações bancárias, por exemplo, sequer exigem o uso de senha pessoal, bastando aproximar o cartão (*Magnetic Secure Transmission* - MST) ou celular (que tenha a tecnologia NFC - Near Field Communication) para validar uma operação financeira. Em que pese o ganho no tempo para a realização da autorização de pagamento, este sistema requer apenas a utilização de um instrumento por aproximação de outro instrumento. Esta aproximação pode ser feita por qualquer pessoa que esteja de posse do dispositivo, não sendo uma garantia de autenticidade.

O Tribunal de Justiça de Minas Gerais (TJ-MG), ao julgar a AC: 10000211464193001, pela 18ª Câmara Cível, reflete um entendimento importante sobre a responsabilidade em transações bancárias eletrônicas. No caso em questão, tratou-se de um apelo relacionado a danos morais e materiais derivados de um empréstimo bancário realizado por meio de um caixa eletrônico, utilizando-se do cartão e senha pessoal do correntista.

A decisão, proferida pelo relator Desembargador Habib Felippe Jabour, concluiu que não havia responsabilidade da instituição financeira na questão. Isso se deve ao fato de que a contratação do empréstimo foi realizada através de meios eletrônicos, validando a transação com a comprovação da utilização do cartão e senha pessoais do cliente. A corte entendeu que a ausência de fraude de terceiros ou vício de consentimento implica na validade da operação.

Essencialmente, o Tribunal reiterou que a utilização do cartão bancário magnético e da respectiva senha é de responsabilidade exclusiva do correntista, que deve assegurar a segurança de seus documentos e dados pessoais. Em conformidade com a jurisprudência do Superior Tribunal de Justiça (STJ), conforme a Decisão, apontou-se que, em situações onde a transação é efetuada com o uso de cartão bancário e senha pessoal, a culpa pelos danos recai exclusivamente sobre o titular da conta, eximindo a instituição financeira de qualquer responsabilidade. Deste modo, segundo a corte mineira, fica evidenciada a importância da segurança pessoal em operações bancárias eletrônicas e a responsabilidade individual em proteger dados de acesso, como cartão e senha, reforçando a ideia de que os usuários devem ser diligentes no manejo de suas informações bancárias para evitar fraudes e prejuízos.

Mesmo sem o uso de assinatura digital com chave pública e privada, a contratação pode ser comprovada com o uso associado de senha pessoal, biometria, digitalização dos documentos pessoais, informações a respeito do IP – Internet Protocol, o número ou código hash, visto que consiste em um conjunto de dados transmitidos segundo regras e formatos definidos que permitem individualizar o tempo e o local do uso da rede. Embora um endereço IP não forneça uma localização geográfica precisa de um dispositivo, ele pode fornecer dados aproximados de onde o dispositivo esteja localizado, isso em razão dos blocos de endereços IP serem distribuídos geograficamente.

Caso seja questionada a autenticidade da assinatura digital judicialmente, poderão ser utilizados outros meios de provas que envolvam as circunstâncias da operação, como por exemplo a transferência bancária do valor emprestado em favor do mutuário, imagem registrada, gravação do áudio, localização do dispositivo eletrônico utilizado, padrão de uso.

Resta o problema do dever de informação que o consumidor tem a respeito dos produtos e serviços contratados, o que poderia invalidar a assinatura digital. Esta questão será objeto de consideração a respeito do papel das agências reguladoras e políticas internas das empresas.

4.3 O PAPEL DAS AGÊNCIAS REGULADORAS E ÓRGÃOS DE PROTEÇÃO

4.3.1 LEI Nº 14.063 DE 2020

Antes de avaliar a questão regulatória das agências, é imperioso observar o disposto na Lei Federal nº 14.063, do dia 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de software desenvolvidos por entes públicos. Primeiramente, trata-se de uma norma editada no contexto da Pandemia Covid-19 (Pinheiro; Weber; Neto, 2022), onde o isolamento social impunha medidas excepcionais de distanciamento com a manutenção das relações interpessoais através dos canais digitais e telemáticos.

Esta norma tem como objetivo principal proteger informações pessoais e sensíveis dos cidadãos, em consonância com a Constituição Federal e a Lei Geral de Proteção de Dados Pessoais. Ela busca também atribuir eficiência e segurança aos serviços públicos, especialmente em ambiente eletrônico. Suas disposições se aplicam principalmente à interação entre órgãos e entidades públicas, entre pessoas naturais ou jurídicas de direito privado e entes públicos, e entre os próprios entes públicos. No entanto, ela exclui situações como processos judiciais, interações que permitam anonimato, sistemas de ouvidoria pública, e programas de assistência a vítimas e testemunhas ameaçadas.

A Lei classifica as assinaturas eletrônicas em:

1. Assinatura Eletrônica Simples: Identifica o signatário e associa dados eletrônicos.

2. Assinatura Eletrônica Avançada: Utiliza certificados não emitidos pela ICP-Brasil ou outros meios de comprovação de autoria/integridade dos documentos eletrônicos.

3. Assinatura Eletrônica Qualificada: Utiliza certificado digital nos termos da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

Define a Lei a autenticação como o processo eletrônico que permite a identificação eletrônica de pessoas naturais ou jurídicas, sendo estabelecido

que deve haver meios de revogação ou cancelamento das assinaturas em caso de comprometimento da segurança ou vazamento de dados.

Os entes públicos definirão o nível mínimo exigido para a assinatura eletrônica em seus documentos e interações, variando conforme o impacto e a necessidade de proteção de informações (Aith; Dallari, 2022). A assinatura eletrônica qualificada é aceita em qualquer interação eletrônica com entes públicos, e seu uso é obrigatório em determinadas situações, como atos assinados por chefes de Poder ou Ministros de Estado, emissões de notas fiscais eletrônicas em certos casos, e atos de transferência e registro de bens imóveis.

Em caso de conflitos entre normas ou entre normas de entes diferentes, prevalece o uso de assinaturas eletrônicas qualificadas. A lei também menciona que certidões eletrônicas da Justiça Eleitoral possuem fé pública para constituição de órgãos partidários, dispensando registros em cartórios.

Serão apresentados os regulamentos das agências regulatórias mais importantes, que possuem impacto significativo no cotidiano dos consumidores, como é o caso dos serviços de energia elétrica, telecomunicações e financeiro.

4.3.2 ANEEL

A Resolução Normativa ANEEL nº 1.000, de 7 de dezembro de 2021, define as novas regras para a prestação do serviço público de distribuição de energia elétrica no Brasil. Esta resolução revoga as anteriores normativas ANEEL nº 414 de 2010, nº 470 de 2011 e nº 901 de 2020, consolidando e atualizando as diretrizes nesse setor. O objetivo principal é regular de maneira abrangente as operações das distribuidoras de energia elétrica, garantindo a qualidade e a confiabilidade do serviço prestado aos consumidores, além de estabelecer medidas e procedimentos administrativos pertinentes à regulação desse serviço essencial.

Os contratos para aquisição de energia elétrica são por adesão, conforme art. 123 da Resolução, não existindo forma específica. Identificado o usuário solicitante, feito seu cadastro e da unidade de instalação, estando observados os padrões exigidos pela Resolução para o fornecimento de energia, a ligação é efetuada.

O art. 131 da Resolução permite a assinatura eletrônica dos contratos, nos termos da Lei nº 14.063/2020, sem especificar qual das modalidades. Contudo, não há obrigatoriedade, segundo a Resolução, de assinatura digital qualificada para que a contratação do fornecimento de energia seja efetivada. Isso representa um risco à segurança jurídica em face da possibilidade de terceiros realizarem

uma ligação em nome de um consumidor que não manifestou sua vontade legítima de contratação.

Em algumas situações, a Resolução exige a assinatura do consumidor no papel, como no caso de emissão do TOI – Termo de Ocorrência e Inspeção (art. 591), sem, contudo, afastar a possibilidade de emissão do documento eletrônico com a coleta da assinatura eletrônica. Neste caso, poderá haver a recusa do consumidor de assinar o Termo, ato que deve ser registrado, preferencialmente na presença de testemunhas, visto que o documento não possui a presunção de legitimidade.

Os tribunais têm se deparado com questões envolvendo a legitimidade do TOI como instrumento para a recuperação do crédito da distribuidora de energia elétrica. Conforme decidiu o Tribunal de Justiça de São Paulo, pela 30ª Câmara de Direito Privado (AC: 10436015120208260224), de 2021, foi julgado um caso em que o Termo de Ocorrência de Inspeção foi elaborado sem a presença do consumidor. Isso sugere uma possível falta de transparência ou de participação do consumidor no processo de inspeção ou verificação, o que pode levantar questões sobre a legitimidade ou a justiça do procedimento. A ausência de assinatura no TOI e a não entrega de uma cópia ao consumidor podem indicar uma falha nos procedimentos padrão e na documentação formal. Normalmente, a assinatura é um elemento essencial para validar a autenticidade e o reconhecimento formal de um documento. A não entrega de uma cópia ao consumidor compromete a transparência e impede que o indivíduo tenha um registro ou prova do que foi inspecionado ou relatado. No julgado citado, a referência a "telas sistêmicas e fotografias genéricas" sugere a utilização de provas ou evidências que não são específicas ao caso em questão. Isso pode ser problemático, pois evidências genéricas ou não específicas não oferecem uma representação precisa ou confiável dos fatos relacionados ao consumidor ou ao imóvel em questão. Conclui o Tribunal de Justiça paulista que essas práticas violam a norma regulatória e o direito fundamental à ampla defesa e ao contraditório.

4.3.3 ANATEL

A Resolução da ANATEL nº 632, de 7 de março de 2014, apresenta o "Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações". Este regulamento define os direitos dos consumidores nos serviços de telecomunicações no Brasil, nele estando abrangidas regras e normativas relacionadas ao atendimento, cobrança, e oferta de diversos serviços de telecomunicações.

Especificamente, o regulamento trata de serviços como o Serviço Telefônico Fixo Comutado (STFC), Serviço Móvel Pessoal (SMP), Serviço de Comunicação Multimídia (SCM), e os Serviços de Televisão por Assinatura. Seu principal objetivo é assegurar que os direitos dos consumidores sejam respeitados e protegidos no âmbito dos serviços de telecomunicações, garantindo práticas justas de atendimento e cobrança, além de uma oferta adequada de serviços. Em razão de sua abrangência, torna-se fundamental o exame mais acurado a respeito da formação dos contratos que ele regulamenta, especialmente norteados pela vulnerabilidade do consumidor e o direito à informação.

Cabe destacar que por diversas vezes a Resolução trata da assinatura, mas não no contexto de manifestação de vontade do consumidor para a contratação, mas como uma modalidade de prestação de serviços televisivos, para os diferenciar da televisão aberta.

O contrato de permanência é definido como "documento firmado entre Consumidor e Prestadora, regido pelas regras previstas no Código de Defesa do Consumidor, que trata do benefício concedido ao Consumidor em troca da sua vinculação, durante um prazo de permanência pré-determinado, a um Contrato de Prestação do Serviço" (RESOLUÇÃO nº 632/2014 – ANATEL).

Aqui também temos o contrato de adesão, não havendo forma definida para a contratação, salvo aquelas relativas ao dever de informar e fornecer cópia do contrato. Conforme seus artigos 50 a 52, dentre as obrigações das prestadoras de serviços de telecomunicações está o dever de informar o consumidor sobre as condições de contratação de serviços e a entrega de cópias de contratos.

As prestadoras de serviços devem prover informações claras e detalhadas ao consumidor antes da contratação. Isso inclui, mas não se limita a, preços e tarifas (com e sem promoção), período promocional, regras de reajuste, custos de aquisição, instalação e manutenção, limitações do serviço, limites de franquia e políticas após sua utilização, velocidades mínima e média de conexão, viabilidade de instalação e ativação imediata, e informações sobre prazo de permanência e multas por rescisão antecipada. Essas informações devem ser consolidadas em um sumário entregue ao consumidor antes da contratação, destacando-se claramente as cláusulas restritivas ou limitadoras de direitos.

No momento da contratação, é mandatório que a prestadora entregue ao consumidor uma cópia do contrato de prestação do serviço, incluindo o Plano de Serviço contratado e outros documentos pertinentes à oferta. Isso deve ser acompanhado por informações de acesso, como login e senha, caso o consumidor necessite acessar informações sobre o serviço na internet. Em situações

onde a contratação ocorra remotamente, a prestadora deve enviar esses documentos por meio eletrônico ou outra forma acordada com o consumidor.

As prestadoras devem comunicar aos consumidores com pelo menos 30 dias de antecedência sobre quaisquer alterações ou extinção de Planos de Serviço, Ofertas Conjuntas e promoções, preferencialmente via mensagem de texto ou eletrônica. Isso deve ser feito respeitando as regras específicas aplicáveis, assegurando que o consumidor esteja ciente de quaisquer mudanças que possam afetar o serviço contratado.

De acordo com o regulamento citado, embora as empresas de telecomunicações empreguem diversas técnicas de identificação do consumidor – como coleta de fotografias, assinaturas em tablets, e gravação de chamadas – estas medidas por si só não garantem a legitimidade do processo de contratação caso as informações obrigatórias não sejam fornecidas de maneira satisfatória ao consumidor. A transparência e a clareza na comunicação das condições do serviço, incluindo preços, tarifas, limitações e prazos, são fundamentais. É essencial que o consumidor tenha acesso não apenas às informações fornecidas por escrito, mas também àquelas transmitidas oralmente pelos representantes das prestadoras de serviços. Isso significa que as informações prestadas verbalmente durante o processo de vendas ou atendimento devem estar alinhadas com o que é apresentado nos documentos contratuais. Qualquer discrepância entre as informações verbais e escritas pode levar a mal-entendidos e conflitos, prejudicando os direitos do consumidor. A integridade e a consistência das informações em todas as formas de comunicação são cruciais para assegurar um processo de contratação justo e transparente, em conformidade com os direitos do consumidor estabelecidos pela legislação vigente.

Benjamin, Marques e Bessa (2021, p. 124-132) destacam a importância do direito à informação e da transparência nas relações de consumo, bem como a necessidade de boa-fé e combate ao abuso de direito. Lembram da vulnerabilidade do consumidor, reconhecida pelo CDC, e a consequente necessidade da presença do Estado no mercado para proteger esse sujeito de direitos. Enfatizam que a liberdade considerada aqui é a do consumidor, o "alter", o "outro", em oposição ao fornecedor mais forte. Este ponto de vista busca uma igualdade material, não apenas formal, levando a um papel preponderante da lei sobre a vontade das partes, impondo maior boa-fé nas relações de mercado, como estipulado no artigo 4, inciso III do CDC. Uma das principais contribuições do CDC é o estabelecimento do direito à informação, considerado um direito básico. Mencionam os autores que "o inciso III assegura justamente este direito básico à informação", que se manifesta na exigência de informações claras e adequadas

sobre produtos e serviços. Essa transparência abrange todas as fases da relação contratual, desde o pré-contratual até o pós-contratual, e não é apenas um elemento formal, mas afeta a essência do negócio. As informações fornecidas ou requeridas são parte integrante do conteúdo do contrato, e a falha na informação é vista como um vício na qualidade do produto ou serviço oferecido. Lembram Benjamin, Marques e Bessa que no V Congresso Brasileiro de Direito do Consumidor/Brasilcon, foram aprovadas conclusões que reforçam o dever de informação nos contratos de longa duração ou contratos relacionais. Esses contratos exigem que o fornecedor mantenha o consumidor adequadamente informado sobre todos os aspectos relevantes da relação contratual ao longo de sua duração.

Aditam os autores, existe o dever de transparência e a boa-fé como elementos cruciais para combater o abuso de direito. O inciso IV do artigo 6 do CDC proíbe o abuso de direito e exige transparência e boa-fé nos métodos comerciais, na publicidade e nos contratos. O CDC visa restabelecer o equilíbrio nas relações de consumo, compensando a vulnerabilidade fática do consumidor e combatendo cláusulas e práticas abusivas.

A própria adesão do consumidor, mesmo com o uso de técnicas pelas prestadoras de serviço como a biometria, assinatura eletrônica, gravação de voz, só tem validade se houver correspondência entre o contrato e a informação prestada antes da contratação, além do que a própria manutenção do vínculo depende da continuidade do dever de informar, da transparência e boa-fé.

4.3.4 CONSELHO MONETÁRIO NACIONAL

O Sistema Financeiro Nacional (SFN) do Brasil, regulado pelo art. 192 da Constituição Federal, constitui a estrutura econômica e social do país, sendo formado por uma complexa rede de instituições financeiras e mercados, organizada de modo a promover o desenvolvimento equilibrado do Brasil, garantindo que as necessidades financeiras de todas as regiões sejam atendidas. Este arranjo inclui, mas não se limita a, bancos comerciais, bancos de investimento, cooperativas de crédito, e outras entidades que operam no campo do crédito e do financiamento.

A regulação do SFN é feita por meio de leis complementares, que detalham as regras de funcionamento, supervisão e controle das instituições financeiras, e também regulam a participação do capital estrangeiro no sistema. Um órgão crucial dentro do SFN é o Conselho Monetário Nacional (CMN), que representa o mais alto nível de decisão dentro do sistema. O CMN é responsável por formular

a política monetária, de crédito e cambial do país, cujas decisões têm um impacto direto na estabilidade monetária e na saúde econômica do Brasil, afetando a inflação, os juros, a oferta de crédito e a taxa de câmbio.

O CMN busca atingir objetivos macroeconômicos, como a estabilidade da moeda e o desenvolvimento econômico e social do país. Para isso, ele se utiliza de diversos instrumentos, como a definição das taxas de juros de referência, normas de reservas bancárias, e diretrizes para o crédito. O Conselho é também responsável por estabelecer diretrizes para a atuação do Banco Central do Brasil, a entidade executiva que opera sob a orientação do CMN para implementar as políticas definidas.

Como órgão responsável pela regulação do sistema, o Conselho Monetário Nacional (CMN) aprovou três resoluções para atualizar as operações bancárias com as tecnologias digitais. Tais resoluções permitem a abertura e o fechamento de contas de depósito exclusivamente online, definem situações para atendimento ao cliente somente por meios eletrônicos e estabelecem regras para a gestão de documentos digitalizados, isso com o objetivo de modernizar processos bancários, agilizar o atendimento e reduzir o uso de papel.

A Resolução nº 4.480, de 25 de abril de 2016, estabelece normas para a **abertura e o encerramento de contas de depósitos** por meios eletrônicos nas instituições financeiras e em outras instituições autorizadas a operar pelo Banco Central do Brasil. Seu principal objetivo é adaptar os processos bancários às tecnologias digitais, garantindo maior eficiência e segurança nas operações bancárias.

Define a Resolução os meios eletrônicos como canais e instrumentos utilizados para comunicação e troca de informações à distância, excluindo o uso exclusivo de telefonia por voz para este fim. As instituições financeiras podem agora realizar a abertura de contas de depósito por meios eletrônicos para pessoas físicas, com a utilização de assinatura eletrônica, conforme a legislação vigente. É permitida a coleta de assinaturas por meio de dispositivos eletrônicos, como tablets e smartphones.

Para assegurar a segurança e a autenticidade desses processos, a Resolução exige que as instituições adotem procedimentos e controles rigorosos. Estes devem confirmar a identidade do cliente, garantir a autenticidade das informações fornecidas e adequar-se às normas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo. É obrigatório que as instituições permitam o encerramento de contas abertas eletronicamente por meio eletrônico.

A Resolução também determina que os procedimentos e tecnologias utilizados na abertura e encerramento de contas eletrônicas devem assegurar a

integridade, autenticidade e confidencialidade das informações e documentos eletrônicos. Estes devem ser protegidos contra acessos e usos não autorizados, e deve haver produção de cópias de segurança e mecanismos de rastreamento e auditoria dos processos utilizados.

Por fim, a Resolução exige que os procedimentos e tecnologias empregados sejam detalhados em um manual específico da instituição e sejam submetidos a testes periódicos pela auditoria interna, mantendo registros e informações sobre esses processos disponíveis para o Banco Central do Brasil por um prazo mínimo de cinco anos.

Esta resolução tem impacto importante para os serviços que sejam prestados exclusivamente pelo meio eletrônico, o que não afasta a opção do consumidor pela utilização dos canais tradicionais de atendimento, como nas agências bancárias, isso quanto a instituição não opere exclusivamente pelos meios eletrônicos, conforme Resolução nº 4.479, do dia 25 de abril de 2016.

Cabe às instituições financeiras a responsabilidade de identificar a pessoa que está interessada em abrir uma conta, especialmente com o uso exclusive dos canis digitais. A falha na identificação representa falha no serviço, representando em responsabilização da instituição financeira pelos danos causados. A jurisprudência do Superior Tribunal de Justiça (STJ) no Recurso Especial 1197929 PR 2010/0111325-0, representativo da controvérsia, estabelece um precedente importante em relação à responsabilidade civil das instituições bancárias por danos causados por fraudes e delitos cometidos por terceiros, incluindo a utilização de documentos falsos ou fraudes na abertura de contas-correntes ou na obtenção de empréstimos. Este caso é particularmente relevante no contexto da assinatura eletrônica, um domínio em crescente expansão e adoção, especialmente no setor bancário. Na decisão, o STJ determinou que as instituições bancárias têm responsabilidade objetiva nesses casos. Isso significa que os bancos são responsáveis pelos danos causados aos clientes ou a terceiros, independentemente de terem cometido um erro ou negligência. A justificativa para essa posição reside no conceito de "risco do empreendimento". Nesse entendimento, os riscos de fraudes e delitos são considerados riscos inerentes à atividade bancária, e cabe ao banco prevenir e remediar tais ocorrências.

No contexto da assinatura eletrônica, essa jurisprudência assume uma importância ainda maior, visto que este novo instrumento de validação dos contratos digitais, com maior eficiência e conveniência, também apresenta riscos de segurança, como a possibilidade de falsificação ou uso indevido dos dados das vítimas. Cabe verificar que a jurisprudência citada do STJ foi julgada em 2011, antes da Resolução do CMN de 2016. Com a responsabilidade objetiva

estabelecida pelo STJ, as instituições bancárias precisam assegurar que seus sistemas de assinatura eletrônica sejam seguros e à prova de fraudes, pois em caso de qualquer falha ou fraude, serão elas as responsáveis pelos danos causados.

Esta jurisprudência também implica que os bancos devem investir continuamente em tecnologia de segurança e em procedimentos de verificação robustos para minimizar o risco de fraudes com assinaturas eletrônicas. Devem implementar medidas eficazes para a rápida detecção e resolução de fraudes, de modo a limitar o impacto sobre os clientes.

As instituições financeiras procuram garantias de recebimento dos empréstimos concedidos. Uma das modalidades de garantia mais difundidas é o consignado em folha de pagamento, permitindo que milhões de pessoas tenha acesso ao crédito. O Instituto Nacional de Seguro Social – INSS, editou norma regulando a consignação em folha de pagamento dos seus beneficiários.

A Instrução Normativa INSS/PRES Nº 28, de 16 de maio de 2008, com várias alterações posteriores, inclusive pela Instrução Normativa INSS nº 100, do dia 28 de dezembro de 2018, estabelece critérios e procedimentos operacionais relacionados à consignação de descontos em benefícios da Previdência Social para o pagamento de empréstimos e uso de cartões de crédito, isso com o objetivo de disciplinar o processo de consignação em benefícios previdenciários, simplificar a tomada de empréstimos pessoais e cartões de crédito, e incentivar a redução de juros por instituições financeiras conveniadas.

A normativa especifica que os descontos em aposentadorias e pensões por morte para pagamento de empréstimos pessoais e cartões de crédito devem seguir os procedimentos estabelecidos na instrução. Inicialmente, os benefícios permanecem bloqueados para operações de consignação até que haja uma autorização expressa do titular ou seu representante legal para o desbloqueio. Para autorizar o desconto nos benefícios, o titular deve contratar o empréstimo com uma instituição financeira que tenha convênio com o INSS/Dataprev. O contrato deve ser assinado com a apresentação de documentos de identidade e CPF. A autorização para consignação deve ser dada de forma expressa, escrita ou eletrônica, e é irrevogável e irretratável. Não são aceitas autorizações por telefone ou gravação de voz.

A autorização para consignação, seja por escrito ou eletrônica, é válida enquanto subscrita pelo titular do benefício e não se estende aos pensionistas e dependentes. Em relação aos procedimentos digitais, a normativa exige a pré-autorização como requisito para a disponibilização das informações do beneficiário, necessárias à elaboração do contrato eletrônico. Quando a autorização é produzida eletronicamente, dispensa-se a apresentação do termo

digitalizado, desde que sejam atendidos os requisitos de segurança que garantam a integridade e o não repúdio do documento.

A Instrução Normativa estabelece que as operações de crédito consignado só podem ocorrer se realizadas na própria instituição financeira ou através de seu correspondente bancário, respeitando o limite de contratos ativos. A instituição financeira só deve encaminhar o arquivo para averbação de crédito após a devida assinatura do contrato pelo beneficiário, inclusive se realizada eletronicamente.

A vulnerabilidade de pessoas idosas e/ou com baixo grau de instrução, especialmente no que trata de utilização dos meios não tradicionais do sistema financeiro, como os canais digitais de atendimento, tem levantado questionamentos a respeito da validade dos contratos de empréstimo consignado. Aquines (2018) discute o combate das práticas fraudulentas contra aposentados e pensionistas, inclusive quanto ao assédio crescente por parte de instituições financeiras, muitas vezes localizadas perto de agências da Previdência Social, usam estratégias para persuadir idosos a aderir a empréstimos consignados, que são descontados diretamente do benefício. Segundo Aquines, o Procon de Porto Alegre realizou uma operação de campo para entender melhor como essas instituições operam. A coordenadora jurídica do Procon, Priscila Telles dos Santos, menciona que os idosos são frequentemente abordados de maneira amigável e persuasiva, o que pode levá-los a aceitar empréstimos desnecessários. Segundo a coordenadora, "o idoso, muitas vezes, é carente e fica sensibilizado com uma acolhida assim". A Instrução Normativa do INSS, com as alterações promovidas pela nº 100/2018, em vigor desde março de 2019, determina que as instituições financeiras só podem contatar os segurados seis meses após a concessão do benefício. Os benefícios serão bloqueados para empréstimos por 90 dias após a aposentadoria, evitando o assédio imediato. Contudo, muitos idosos são enganados por termos como "crédito liberado", pensando que se trata de um direito, não de um empréstimo com juros. Aquines destaca a preocupação com o vazamento de dados pessoais, como relatado pela aposentada Leila de Castro, que recebe ligações de estranhos oferecendo créditos. Para evitar fraudes, o autor recomenda nunca fornecer dados pessoais como CPF por telefone, não contratar empréstimos consignados por telefone, e procurar agências bancárias ou financeiras credenciadas para realizar empréstimos. Também é sugerido que os beneficiários bloqueiem seus benefícios para empréstimos e, caso detectem problemas, registrem queixa na Ouvidoria do INSS.

O empréstimo consignado é descrito como uma modalidade de empréstimo facilitada e, em muitos casos, acessível mesmo para pessoas com restrições

de crédito. Contudo, diante da vulnerabilidade do mutuário, da deficiência de instrução para o uso de canais digitais, a contratação, mesmo com a assinatura eletrônica, deve atender a critérios mínimos de informação para ser eficaz. Conforme Coelho (2020), o princípio da transparência possui desdobramentos que importam na relação de consumo, especialmente "a não vinculação do consumidor à obrigação da qual não tenha tido prévio e claro conhecimento".

A questão aqui discutida poderia, hipoteticamente, ser contextualizada em uma alegação de uma assinatura eletrônica que o consumidor diz não ter realizado para a contratação de um empréstimo consignado. Neste caso hipotético, a instituição financeira poderia defender a validade do negócio jurídico, baseando-se na coleta de fotografia, uso do aparelho móvel do consumidor e depósito do valor na conta deste, porém sem apresentar o documento digital com a assinatura digital do consumidor, conforme regulamentado pela norma sobre chaves públicas brasileiras e certificados digitais.

Neste cenário hipotético, a decisão careceria de uma avaliação probatória mais robusta, que não dependeria de um documento assinado eletronicamente por meio de certificado digital.

Existe uma peculiaridade jurisprudencial quanto aos contratos bancários onde o consumidor contesta a autenticidade da assinatura, tendo sido a questão debatida pelo Superior Tribunal de Justiça.

Todavia, o Tema 1061 discutido no REsp 1.846.649-MA, decidido em 24 de novembro de 2021, pelo Superior Tribunal de Justiça (STJ), tratou da controvérsia acerca do ônus da prova em casos em que o consumidor impugna a autenticidade da assinatura constante do contrato juntado ao processo pela instituição financeira. A tese fixada foi: "Na hipótese em que o consumidor/autor impugnar a autenticidade da assinatura constante em contrato bancário juntado ao processo pela instituição financeira, caberá a esta o ônus de provar a autenticidade (CPC arts. 6º, 369 e 429 II)".

Este Tema 1061 específico, no contexto da presente pesquisa, pode revelar uma distinção relevante (*distinguishing*). Enquanto o Tema 1061 se concentra especificamente na impugnação da autenticidade da assinatura em documentos físicos juntados ao processo e atribui o ônus da prova à instituição financeira, a pesquisa ora representada na situação hipotética acima revela a ausência de apresentação de um documento digital assinado digitalmente conforme a legislação específica sobre certificados digitais. Isso implica que, embora ambos os cenários envolvam a questão da prova da autenticidade da manifestação de vontade do consumidor, o caso hipotético adiciona a complexidade da regulamentação específica sobre assinaturas digitais, não diretamente abordada no Tema 1061.

4.3.5 PROCON

Os contratos regulados merecem atenção das agências regulatórias, diferentemente do que ocorre no cotidiano das atividades comerciais ordinárias, não reguladas. Nestas, a liberdade das formas nos contratos particulares é um princípio fundamental no direito contratual que assegura às partes a possibilidade de estabelecer acordos sem a necessidade de seguir um formato ou modelo específico, sendo este um princípio intrinsecamente ligado à autonomia privada, tal como delineado nos arts. 170 e seguintes da Constituição Federal, que é a liberdade dos indivíduos de regular seus próprios interesses dentro dos limites da lei.

Infraconstitucionalmente, tem relevância a norma civil, em que se reconhece a liberdade das formas (art. 104 do Código Civil), que estabelece os requisitos de validade do contrato, e pelo art. 107, que preconiza que a validade do negócio jurídico não depende de forma especial, exceto quando a lei expressamente a exigir. Assim, os contratos podem ser celebrados oralmente, por escrito, ou até mesmo por meio de comportamentos concludentes, desde que respeitados os requisitos legais de validade e as exigências formais específicas para determinados tipos de contrato.

Entretanto, em que pese essa liberdade, os contratos particulares não estão isentos de fiscalização e devem respeitar as normas de ordem pública e os princípios gerais do direito, em especial quando se trata de relações de consumo, especialmente diante da disposição constitucional do art. 170, inciso V. Nesta seara, os Procons (Programas de Proteção e Defesa do Consumidor) desempenham papel relevante como órgãos de defesa do consumidor presentes em diversos municípios e estados do Brasil.

Os Procons atuam no âmbito do Sistema Nacional de Defesa do Consumidor (SNDC), e sua função é garantir que as relações de consumo se desenvolvam de forma justa e equilibrada, assegurando o respeito aos direitos dos consumidores (art. 105 do Código de Defesa do Consumidor).

Segundo Marques (2019), o art. 105 do Código estabelece que o SNDC é composto tanto por órgãos públicos (federais, estaduais, do Distrito Federal e municipais) quanto por entidades privadas dedicadas à defesa do consumidor. Este arranjo reflete o espírito do Código, que visa à integração e cooperação entre diferentes atores para promover efetivamente a proteção do consumidor. Esta perspectiva é reforçada pelos princípios da Política Nacional das Relações de Consumo, que incluem ações governamentais para proteger os consumidores, incentivar a criação de associações representativas, e a regulação e fiscalização do

mercado de consumo. Um ponto central é a previsão de medidas concretas para a proteção do consumidor, como a assistência jurídica gratuita para consumidores carentes, a criação de Promotorias e Delegacias especializadas, e estímulos para associações de defesa do consumidor. Além dos órgãos tradicionalmente associados à defesa do consumidor, como o Procon, o sistema inclui também outras entidades que desempenham atividades relacionadas à defesa do consumidor, como Promotorias de Defesa do Consumidor, Defensorias Públicas e Agências Reguladoras. Um exemplo citado é o Banco Central do Brasil, que se vincula ao SNDC através de suas funções de regulação e fiscalização do sistema financeiro.

Em caso de violações desses direitos, como práticas abusivas, cláusulas contratuais desleais ou publicidade enganosa, os Procons podem intervir de diversas maneiras:

1. Os Procons desempenham um papel fundamental na educação e orientação dos consumidores sobre seus direitos e deveres.

2. Frequentemente, atuam na mediação de conflitos entre consumidores e fornecedores, buscando uma solução amigável para as partes.

3. Realizam a fiscalização das práticas comerciais, verificando a conformidade dos contratos com as normas de proteção ao consumidor.

4. Em casos de infrações às normas de proteção ao consumidor, os Procons têm poder para aplicar sanções administrativas, que vão desde multas até a suspensão temporária de atividades ou interdição do estabelecimento.

5. Os Procons trabalham em conjunto com outros órgãos de defesa do consumidor, como o Ministério Público e a Justiça, para garantir a aplicação efetiva das normas de proteção ao consumidor.

Os Estados possuem autonomia legislativa para editar normas criando os Procons, como é o caso de Pernambuco com a Lei Estadual nº 8.117/1980 e São Paulo com a Lei Estadual nº 9.192, de 23.11.1995 (Junior, 2014).

Esta liberdade das formas nos contratos particulares coexiste com a necessidade de proteção dos direitos dos consumidores, sendo os Procons instrumentos essenciais, porém não exclusivos, para assegurar esse equilíbrio nas relações de consumo, observada a garantia da autonomia privada nas relações contratuais com a vulnerabilidade dos consumidores, o direito à informação, transparência e boa-fé.

A Fundação Procon-SP editou o Guia do Comércio Eletrônico (2021) destacando pontos relevantes para a validade e eficácia das assinaturas eletrônicas no ambiente digital, onde os registros dos dados representam peculiaridades na relação de consumo que devem ser observadas, mesmo diante do princípio da liberdade das formas.

Seguindo o Guia do Procon-SP, o comércio eletrônico é definido como a comercialização de produtos ou serviços por meios eletrônicos, sem a necessidade da presença física tanto do fornecedor quanto do consumidor. Isso inclui a compra via telefone, SMS, internet, aplicativos em smartphones e tablets, entre outros. A conveniência, a ampla gama de produtos e serviços, a facilidade em comparar preços e a comodidade de receber produtos em casa são destacadas como vantagens do e-commerce[39]. Para garantir uma experiência de compra segura, o consumidor deve estar atento a vários aspectos. É fundamental analisar com cautela a oferta e evitar compras por impulso. Identificar claramente o fornecedor é essencial, procurando por dados como razão social, CNPJ/CPF, endereço físico e eletrônico, e contato. A verificação do CNPJ e a situação cadastral do fornecedor no site da Receita Federal é recomendada, assim como buscar referências de fornecedores recomendados por conhecidos. Outro ponto importante é a verificação das características do produto, observando a descrição, comparando com outras marcas e visitando a página do fabricante. O fornecedor deve discriminar no preço todas as despesas adicionais, como frete. É crucial também estar ciente da política de troca e devolução dos produtos, e guardar todos os comprovantes relacionados à compra.

É essencial ler a política de privacidade do site para entender como os dados pessoais serão manuseados e garantir que o fornecedor use mecanismos de segurança para proteger esses dados. O Guia destaca considerações específicas sobre compras em lojas ou sites internacionais, como a regulamentação do Código de Defesa do Consumidor aplicável apenas a empresas com representação no Brasil, e dicas para importação direta, incluindo a verificação da legalidade dos produtos e o pagamento de tributos.

Um ponto crucial é a necessidade de fornecer informações adequadas sobre produtos e serviços, que devem ser corretas, claras, precisas e ostensivas, abrangendo características, preço, garantia, prazos de validade, dados do fabricante e eventuais riscos. O atendimento facilitado é essencial, com a exigência de que o fornecedor apresente um resumo claro das principais cláusulas do contrato antes da contratação, forneça meios para correção de erros, confirme a aceitação da oferta, disponibilize o contrato na íntegra após a contratação, e mantenha um atendimento eletrônico eficaz.

39 Decreto nº 7.962, de 15 de março de 2013, regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico.

A facilidade e conveniência para aquisição de produtos é um atrativo tecnológico que não elimina os riscos de acessos não autorizados às contas e perfis dos consumidores por terceiros. Neste ambiente, é comum que os negócios jurídicos sejam concluídos primeiros através do acesso à plataforma com o uso de senha pessoal, seguida da escolha dos produtos para inclusão em uma cesta e posterior pagamento, isso para entrega em endereço à escolha do usuário.

A validade depende da correta identificação do usuário e da inviolabilidade do acesso não autorizado, inclusive quanto aos dados de pagamento. Havendo comprometimento da segurança do sistema, não se pode validar o uso da assinatura eletrônica, seja ela uma simples senha, seja através da confirmação por dois fatores. A eficácia da assinatura eletrônica deve pressupor o cumprimento do dever de informação, transparência e boa-fé do fornecedor para como o consumidor, pois são estes elementos essenciais para a formação do contrato de consumo, especialmente sem a sua realização presencial.

Estes contratos massificados revelam ainda mais a importância do comportamento do fornecedor nas relações do consumo, trazendo ao palco em especial boa-fé. Conforme Marques (2021), a boa-fé é vista como um elemento fundamental nas relações de consumo, especialmente nos contratos massificados de serviços, que são aqueles padronizados e oferecidos em larga escala ao público. A boa-fé, conforme a autora, é entendida como uma atuação refletida, que considera e respeita o parceiro contratual, seus interesses legítimos e direitos. Implica em agir com lealdade, sem abusar da posição contratual, evitando causar lesão ou desvantagem excessiva, e cooperando para alcançar os objetivos do contrato. A autora enfatiza que:

> "boa-fé nos contratos, em especial nos contratos de serviços ou 'fazeres' 'massificados' significa uma atuação 'refletida', atuação refletindo, pensando no outro, no parceiro contratual, respeitando-o, respeitando seus interesses legítimos, seus direitos, respeitando os fins do contrato, agindo com lealdade, sem abuso da posição contratual, sem causar lesão ou desvantagem excessiva, com cuidado para com a pessoa e o patrimônio do parceiro contratual, cooperando para atingir o bom fim das obrigações" (Marques, 2021)

No contexto dos contratos privados, completa Marques, a boa-fé é entendida como objetiva, um padrão de conduta leal baseado na confiança, e não apenas como boa-fé subjetiva. A boa-fé objetiva serve como um padrão de comportamento leal, respeitando as expectativas legítimas da outra parte e contribuindo para a segurança nas relações contratuais. Este princípio é orientador em todas as relações de consumo, especialmente nos serviços, conforme

estabelece o CDC. O princípio da boa-fé no direito privado brasileiro possui uma função dupla. Primeiro, como uma função criadora de novos deveres, como o dever de informar, de cuidado e de cooperação, e como fonte de responsabilidade por atos lícitos. E segundo, como uma função limitadora, restringindo a liberdade dos parceiros contratuais ao definir condutas e cláusulas abusivas e controlando a transferência de riscos profissionais.

A relação do princípio da boa-fé com a assinatura eletrônica do consumidor no direito privado brasileiro é significativa e multifacetada, visto que a boa-fé, ao atuar como geradora de deveres, ressalta a importância de informar claramente o consumidor sobre os termos do contrato, inclusive quando estes são acordados e firmados eletronicamente. Por força desta obrigação legal, qualquer contrato assinado eletronicamente deve ser transparente, acessível e compreensível, assegurando que o consumidor esteja plenamente ciente do que está assinando. O cuidado e a cooperação são fundamentais para garantir que a assinatura eletrônica ocorra em um ambiente seguro e confiável, sem riscos indevidos para o consumidor, de modo a reforçar a necessidade de equidade e justiça nas transações eletrônicas, protegendo o consumidor de possíveis abusos e assegurando a integridade do processo de assinatura eletrônica.

4.4 POLÍTICAS DE COMPLIANCE E MELHORES PRÁTICAS DE MERCADO

A responsabilidade das empresas em desenvolver políticas de compliance é um aspecto crucial na governança corporativa moderna, especialmente quando estas atuam em relações de massa como as de consumo, onde diversas pessoas, interessadas e/ou necessitadas em adquirir seus produtos e serviços são postas em posição de vulnerabilidade. Essas políticas abrangem uma variedade de áreas, incluindo, mas não se limitando a, legislação antitruste, prevenção à lavagem de dinheiro, proteção de dados e privacidade, direitos trabalhistas e responsabilidade ambiental. O desenvolvimento e a implementação efetiva de políticas de compliance não apenas protegem as empresas contra riscos legais e financeiros, mas também reforçam sua reputação e sustentabilidade no longo prazo, contribuindo para um ambiente de negócios mais transparente e ético.

A evolução do controle social das corporações, decorrente das mudanças nas estruturas empresariais e às demandas da sociedade moderna, desde o fim do século XIX e início do século XX, é fruto do surgimento das fusões empresariais nos Estados Unidos e na Inglaterra, que levaram à formação de

grandes oligopólios. Este movimento visava regular o poder econômico para evitar abusos que pudessem prejudicar a livre iniciativa de mercado e o crescimento econômico. Essas ações representaram os primeiros passos para estruturar um Estado capaz de controlar a agressividade dos oligopólios, garantindo a sustentabilidade dos negócios e das corporações, ao mesmo tempo em que preservava condições econômicas favoráveis. Com o passar do tempo, as iniciativas de controle social se tornaram mais sofisticadas e modernizadas, adaptando-se ao ritmo acelerado de mudanças na vida das pessoas e nas formas de fazer negócios. A era digital intensificou esse movimento, uma vez que as organizações passaram a ser mais observadas e avaliadas em suas ações, tanto positivas quanto negativas. Essa transformação nas empresas e no controle social do negócio reflete uma adaptação contínua às demandas e mudanças da sociedade, evidenciando a importância de uma gestão eficaz e responsável no contexto corporativo moderno (Pereira; Carvalho; Giron, 2021).

O avanço do ordenamento jurídico brasileiro no reconhecimento de mecanismos extralegais para melhorar a eficácia da lei demanda uma a maturidade jurídica no sentido de se afastar de modelos estritamente estatais para atingir objetivos públicos, sendo relevante a evolução e importância do compliance e na implementação da Lei Geral de Proteção de Dados (LGPD) no contexto brasileiro. De acordo com o princípio da responsabilização e prestação de contas, introduzido pela LGPD, as entidades privadas devem adotar medidas eficazes para a observância e cumprimento das normas de proteção de dados, mitigando os riscos inerentes ao seu tratamento e estabelecer normas claras para o tratamento de dados, incentivando uma cultura de responsabilidade e conformidade pelas entidades privadas (Frazão; Cueva, 2022).

No contexto das relações de consumo através dos serviços financeiros, Frazão e Cueva (2021) discutem os desafios do compliance de dados. Segundo os autores, com a promulgação da LGPD e a criação da autoridade nacional de dados pessoais, as instituições financeiras, que já estavam sujeitas a outras normas de proteção de dados, enfrentam desafios específicos. A necessidade de conformidade com a LGPD exige que as instituições financeiras estejam preparadas para atender às solicitações dos titulares de dados, como é o caso do direito à portabilidade dos dados, que deve ser viabilizado mediante solicitação do cliente.

Enfatizam a importância da segurança da informação, particularmente em relação ao Pix e ao Open Banking. As instituições financeiras devem aprimorar técnicas para identificar indivíduos e prevenir fraudes, como os ataques de *phishing,* que são um ponto de vulnerabilidade do Pix. É sugerido que as

instituições financeiras invistam em educar seus clientes sobre como identificar e neutralizar tentativas de ataques.

No contexto do Open Banking, destacam o desafio de garantir a segurança cibernética devido ao amplo compartilhamento de dados pessoais, ponderando que os investimentos em segurança não devem aumentar os custos de transação a ponto de prejudicar a competição, especialmente para as fintechs. Conforme os autores, "o Open Banking é lastreado no prévio consentimento dos clientes das instituições financeiras e no direito à autodeterminação informativa." O sucesso do Open Banking depende da capacidade das instituições de garantir que os clientes estejam bem informados e possam gerenciar o uso de suas informações.

Para isso, aditam, as instituições financeiras são aconselhadas a evitar políticas de privacidade e termos de consentimento complexos, favorecendo a clareza e a simplicidade para que os clientes possam compreender e gerenciar seus dados. A sugestão é que se empreguem tecnologias que fortaleçam o controle dos indivíduos sobre seus dados, como as ***Privacy Enhancing Technologies***, por meio de plataformas simples e amigáveis.

Segundo a OCDE (2023), o desenvolvimento e a aplicação das tecnologias de proteção da privacidade (*Privacy-Enhancing Technologies* - PETs) têm o potencial de mudar fundamentalmente as práticas de coleta e processamento de dados pessoais. Essas tecnologias não são novidade, mas estão evoluindo de maneiras que poderiam permitir um uso de dados pessoais mais protetivo em relação à privacidade, alinhando-se com o conceito de privacidade desde a concepção (*privacy by design*). PETs oferecem técnicas criptográficas avançadas e mudanças estruturais no processamento de dados, proporcionando novas proteções de privacidade e segurança digital.

Conforme a OCDE, dovernos e reguladores, particularmente as autoridades de proteção de dados, têm enfatizado as PETs como soluções proeminentes para a proteção da privacidade e dos dados pessoais. Um exemplo citado pela OCDE é o Comunicado de 2022 do G7 que reconhece a importância das PETs: *"[T]he use of PETs can facilitate safe, lawful and economically valuable data sharing that may otherwise not be possible, unlocking significant benefits to innovators, governments and the wider public."*[40].

40 Tradução livre: O uso de PETs pode facilitar o compartilhamento de dados seguro, legal e economicamente valioso que de outra forma não seria possível, desbloqueando benefícios significativos para inovadores, governos e o público em geral.

As PETs, adita, alteram a maneira como as organizações coletam, acessam e processam dados, especialmente pessoais, apoiando análises colaborativas sobre dados que estariam muito sensíveis para serem divulgados ou combinados. Essa tecnologia representa um desafio para os formuladores de políticas e reguladores, dada a natureza altamente inovadora e técnica das PETs, que cria uma barreira de linguagem entre os engenheiros que desenvolvem esses sistemas e os responsáveis pelas políticas que determinarão seu uso. Essas tecnologias, em diferentes estágios de desenvolvimento, precisarão ser parte de estruturas de governança de dados mais amplas para garantir que sejam usadas em linha com os riscos associados, incluindo riscos à privacidade, e que os dados estejam seguros.

Segundo a OCDE, o sucesso da implementação das PETs no cenário regulatório dependerá da capacidade dos governos e das autoridades de proteção de dados de compreender como os dados pessoais são coletados e processados por essas tecnologias e como elas se encaixam nos frameworks de proteção de dados e privacidade existentes.

A integração das tecnologias de proteção da privacidade (PETs) no arcabouço regulatório e nas políticas de compliance das organizações surge como um ponto de inflexão na maneira como os dados pessoais são manuseados no contexto corporativo, especialmente no que tange à identificação digital dos consumidores. No cenário descrito pela OCDE, a assinatura digital emerge como um componente essencial dessas tecnologias, permitindo que os processos de verificação de identidade não apenas cumpram com os mais altos padrões de segurança e privacidade, mas também se alinhem com as expectativas regulatórias e com o compromisso ético das empresas com a proteção de dados. A adoção das PETs, incluindo as assinaturas digitais, exige que as empresas não só incorporem essas ferramentas em suas operações diárias, mas também revisem e aprimorem continuamente suas políticas de compliance, assegurando que a coleta e o processamento de dados estejam em conformidade com a legislação vigente e com as melhores práticas de mercado. Tal alinhamento ressalta a proatividade corporativa em promover a confiança dos consumidores e a integridade dos dados, elementos-chave para a sustentabilidade e a reputação no universo digital contemporâneo.

4.5 NOVAS TECNOLOGIAS E PERSPECTIVAS PARA O CONSUMIDOR

A evolução das tecnologias emergentes está remodelando profundamente a esfera dos contratos digitais, introduzindo tanto inovações revolucionárias quanto desafios significativos, sendo um destaque inicial a Internet das Coisas (IoT) e o uso crescente de sistemas de tomada de decisão baseados em Inteligência Artificial (IA), ampliando as fronteiras da automação contratual, permitindo a execução e gestão de contratos em tempo real e com complexidade crescente. Esta integração resulta em eficiências operacionais, mas também suscita questões sobre a autonomia e a transparência das decisões algorítmicas.

A cibersegurança, especialmente no contexto do blockchain e da criptografia quântica, oferece um novo paradigma para a segurança de contratos digitais. Enquanto o blockchain proporciona uma infraestrutura descentralizada e resistente a alterações, a criptografia quântica promete um nível de segurança quase inquebrável, essencial para a confiança e integridade dos contratos digitais.

Por sua vez, a coleta e utilização de dados em grande escala, juntamente com o uso de biometria em assinaturas digitais, apresentam novos desafios sobre a relação da privacidade e liberdade.

Hine (2020) aborda a evolução da percepção e do uso da Internet, destacando a transição de uma visão ciberpunk, onde o ciberespaço era visto como um domínio alternativo para a construção de identidades virtuais, para uma compreensão mais integrada e corporificada da Internet na vida cotidiana.

Argumenta que, ao contrário das expectativas iniciais de uma experiência transcendental online, a Internet tornou-se uma extensão das formas corporificadas de existência, onde as identidades virtuais e físicas estão interligadas.

As experiências online e offline não são separadas, mas contínuas e integradas, desafiando a noção de que a presença no ciberespaço é descorporificada. Hine destaca a importância de reconhecer a diversidade e a natureza pessoal da experiência online, bem como a relevância das interações físicas e emocionais no uso da Internet.

A antropologia ciborgue e digital denota a relação entre tecnologia e humano, e propõe uma abordagem etnográfica reflexiva para entender melhor a complexidade da experiência online. Este enfoque inclui a autoetnografia e a etnografia reflexiva, que ajudam a explorar a textura da vida cotidiana à medida que transita entre os domínios online e offline, reconhecendo a Internet como uma experiência corporificada e integrada à existência humana.

A proliferação de *fake news* na Internet ilustra vividamente como a experiência online está corporificada na vida e na sociedade, refletindo a fusão entre os ambientes online e offline. À medida que a Internet se torna cada vez mais uma extensão do nosso ser físico e social, as informações que consumimos online têm um impacto direto em nossas percepções, emoções e ações no mundo físico. As *fake news*, ao serem disseminadas através de plataformas digitais, não apenas circulam no ciberespaço mas também afetam decisões, opiniões e comportamentos no espaço físico, evidenciando a falta de um limite claro entre os dois ambientes.

Esse fenômeno destaca a importância da autenticidade e da responsabilidade nas interações online, pois o que acontece no ambiente virtual pode ter consequências reais e tangíveis. A dificuldade em distinguir entre verdade e falsidade na Internet reflete a complexidade da experiência corporificada online, onde as *fake news* se tornam parte da realidade vivida das pessoas, influenciando a política, a sociedade e as relações interpessoais.

A corporificação da Internet na vida e na sociedade ressalta a necessidade de uma abordagem crítica e reflexiva ao navegar no ambiente online, reconhecendo que as experiências virtuais são inseparáveis do contexto social e físico mais amplo. Isso também sublinha a importância de estratégias educacionais e regulatórias para fortalecer a literacia digital e promover uma cultura de verificação de fatos, fomentando um ambiente online mais autêntico e confiável.

Associado a estes desafios, é importante para a compreensão do fenômeno jurídico tratado nesta pesquisa a discussão das perspectivas relacionadas ao problema da inclusão digital, visto que a vulnerabilidade de certos segmentos da população, como jovens, pessoas com baixa escolaridade e idosos, pode ser exacerbada na era digital. Esta temática tem sua importância não só para a formação dos contratos, mas também para a defesa dos direitos a eles associados em juízo, pois, como aponta Teixeira, Costa e Orengo (2022) a "inclusão digital é indispensável a fim de que seja possível efetivar o direito ao acesso à justiça no cenário das novas tecnologias, sobretudo considerando-se o sistema de justiça como um todo". Estes grupos podem encontrar dificuldades em acessar, entender e utilizar plenamente os contratos digitais, o que coloca em risco sua autonomia contratual e exige atenção tanto em termos de políticas públicas quanto de design tecnológico.

4.5.1 A INTERNET DAS COISAS E AS DECISÕES BASEADAS EM INTELIGÊNCIA ARTIFICIAL

Os dados podem ser extraídos das mais variadas fontes, não apenas aqueles que as pessoas alimentam os sistemas informáticos voluntariamente, mas também quando o fazem involuntariamente. Além destes dados relacionados às pessoas, existem, como já mencionado, os dados sobre dados (metadados), que servem aos sistemas algoritmos baseados em aprendizado de máquina. O desenvolvimento do aprendizado de máquina[41] pode dispensar a ação humana na realização de várias tarefas, inclusive em situações banais, como a compra de produtos de primeira necessidade.

Neste contexto, a internet exerce um papel fundamental para a coleta de dados que serão tratados pelos sistemas de aprendizado de máquinas. Segundo explica Pimentel (2023a, p. 66-70), a complexidade e omnipresença da Internet na era digital a distância de uma simples ferramenta, transformando-a em uma nova realidade existencial do homem. Cita Pimentel Tiburi, para quem a "internet não é apenas uma ferramenta, ela é um mundo que atravessa nosso mundo, um mundo que é atravessado pelo mundo que a cerca e que, ao mesmo tempo, ela duplica constituindo um espaço em que tudo se concentra", para enfatizar a profundidade e a extensão da influência da Internet.

Para Pimentel, a "Internet Incorporada" relaciona a rede com os objetos diretamente, o que é compreendido como a Internet das Coisas (IoT), de modo que a tecnologia é integrada em objetos do cotidiano, melhorando a comunicação entre dispositivos e pessoas, além de aumentar a capacidade de vigilância.

41 Segundo PIMENTEL (2023a, p. 283-285), existem três tipos principais de aprendizado de máquina: aprendizado supervisionado, não supervisionado e por reforço. No aprendizado supervisionado, o foco está na classificação e identificação de padrões em dados previamente rotulados. Este método depende do entendimento de como os dados são classificados para aprimorar a análise. Já o aprendizado não supervisionado difere por não requerer intervenção humana direta e ser empregado em grandes volumes de dados não rotulados, como na identificação de perfis de usuários em redes sociais. Neste caso, os algoritmos trabalham autonomamente para classificar os dados com base nos padrões reconhecidos. O aprendizado por reforço, por sua vez, é descrito como uma modalidade comportamental em que o algoritmo recebe feedback da análise de dados e orienta o usuário sobre como proceder. Diferente dos outros tipos, este aprendizado não se baseia em um treinamento prévio com dados específicos, mas sim em um processo de tentativa e erro para a tomada de decisões. O conceito de deep learning é introduzido como uma evolução do machine learning e um subgrupo da inteligência artificial. O termo foi cunhado por Rina Dechter em 1986 e destaca-se por utilizar um conjunto de algoritmos que modelam soluções para problemas através de representações de dados que simulam o comportamento do cérebro humano. O trecho "o deep learning objetiva o treinamento de computadores para a realização de tarefas como se fossem seres humanos, incluindo a identificação de imagens, textos e vozes" destaca seu objetivo principal: treinar máquinas para realizar tarefas complexas de maneira similar aos humanos, incluindo o reconhecimento de imagens, textos e vozes.

Segundo Pimentel, o conceito de IoT é explorado como um ecossistema que conecta objetos físicos à Internet para troca, armazenamento e coleta de dados, que não só conecta as "coisas" pela Internet, mas também as torna inteligentes e capazes de coletar e processar informações. Este fenômeno é descrito como uma ferramenta poderosa para vigilância e governança algorítmica, especialmente no que se refere à coleta de dados e metadados usados para impulsionar o capitalismo digital. O autor aborda as preocupações com a privacidade e a intimidade, realçando o potencial invasivo da IoT, especialmente quando as redes de telefonia celular são usadas para coletar dados e metadados. As big techs são mencionadas como as principais interessadas nessas informações íntimas e sensíveis dos usuários[42], que são coletadas, armazenadas, mineradas e utilizadas para diversos fins, indo além do controle de aparelhos domésticos.

Estas "*commodities digitais*", conforme denomina Pimentel, podem ser objeto de comercialização. Quando associada à inteligência artificial mediante o aprendizado profundo existe a possibilidade de que decisões sejam tomadas por algoritmos baseados nesta coleta massiva de dados para a formação de contratos de consumo, onde a assinatura digital específica para cada negociação seria dispensável.

Diante das recentes novidades dispostas ao público sobre o uso da inteligência artificial, iniciou-se um amplo debate sobre sua importância crescente no contexto global, refletindo uma conjunção de avanços tecnológicos e desafios éticos, regulatórios e sociais. À medida que a IA se integra cada vez mais em diversos setores, desde segurança e militar até educação e inclusão digital, surge uma demanda premente por um marco regulatório robusto e adaptável que aborde tanto as potencialidades quanto os riscos associados a essa tecnologia.

Um dos principais desafios regulatórios reside na questão da perda de empregos, uma preocupação significativa dada a capacidade da IA de automatizar tarefas anteriormente realizadas por humanos. Isso exige políticas públicas voltadas para a requalificação e o redirecionamento da força de trabalho, assegurando que os avanços tecnológicos não resultem em desigualdades sociais

42 Segundo PIMENTEL (2023c), a "lex algorítmica" consiste em uma arquitetura funcional do ciberespaço, uma lei estrutural que rege a Internet e forma uma compilação de regras de condutas sociais a serem seguidas pelos usuários. A argumenta que, devido ao fracasso na tentativa de regulamentação jurídica do ciberespaço e a necessidade de proteger as liberdades individuais e a democracia, é urgente que cada Estado regulamente a atuação das big techs. Observa que a falta de regulamentação estatal resultou em um ambiente capitalista ultraliberal, gerido por suas próprias leis, onde as big techs predominam.

exacerbadas, mas sim em oportunidades de desenvolvimento humano e econômico (SCOTT, 2023, p. 229).

Além disso, a limitação da IA em áreas sensíveis, tais como segurança e uso militar, demanda uma abordagem cuidadosa para prevenir a adoção de sistemas autônomos em contextos que possam comprometer a segurança e a ética. Na regulação, é importante a compreensão dos limites claros para o desenvolvimento e uso da IA, assegurando que tais tecnologias sejam empregadas de maneira que respeitem os direitos humanos e os princípios de justiça e paz.

No âmbito da educação, a inclusão digital emerge como um campo vital para a implementação da IA, destacando a necessidade de políticas que promovam o acesso equitativo às tecnologias digitais. A IA pode desempenhar um papel significativo na personalização da aprendizagem e na ampliação das oportunidades educacionais, especialmente para populações historicamente marginalizadas. Contudo, é essencial que a implementação da IA na educação seja acompanhada de salvaguardas que protejam os dados sensíveis dos estudantes e assegurem que os sistemas de IA sejam transparentes, justos e responsáveis.

Estas novas oportunidades de trabalho e mudança na abordagem educacional tem relação direta com a regulamentação da IA no que diz respeito aos direitos e deveres subjetivos nas relações jurídicas mediadas por tecnologias como o blockchain. A utilização da IA em conjunto com o blockchain tem o potencial de revolucionar a maneira como as transações são realizadas e registradas, oferecendo maior segurança, transparência e eficiência. No entanto, isso também levanta questões sobre a proteção de dados sensíveis e a necessidade de políticas de compliance que assegurem a conformidade com as leis de proteção de dados e privacidade. As empresas que utilizam essas tecnologias devem ser obrigadas a implementar medidas rigorosas de proteção de dados e a aderir a padrões éticos estritos para prevenir abusos e garantir a confiança do público.

Para abordar esses desafios, é imperativo que os marcos regulatórios sejam desenvolvidos em um processo colaborativo que envolva stakeholders de diversos setores, incluindo governos, academia, indústria e sociedade civil. Tal abordagem multifacetada assegura que as políticas reflitam uma compreensão abrangente das complexidades associadas à IA e que promovam um equilíbrio entre a inovação tecnológica e a proteção dos direitos fundamentais.

4.5.2 CIBERSEGURANÇA: CRIPTOGRAFIA QUÂNTICA E BLOCKCHAIN

A cibersegurança também desperta a atenção para a nova realidade contratual e seus desafios apresentados à tradicional teoria da manifestação de vontade.

O impacto da computação quântica no contexto da criptografia é discutido atualmente, sendo uma preocupação em razão da necessidade de preservação de técnicas de segurança que são fundamentais para as assinaturas digitais.

A criptografia, conforme explica Dodt (2021), é fundamentalmente vulnerável a dois fatores: tempo e poder de processamento. Enquanto algoritmos antigos são facilmente quebráveis hoje em dia, os métodos matemáticos atuais como AES, RSA e ECDSA são seguros contra-ataques de força bruta, dada a massiva quantidade de tempo e capacidade computacional necessária para quebrá-los. No entanto, a computação quântica representa uma nova ameaça a essa segurança. A computação quântica, segundo Dodt, difere da convencional ao utilizar Quantum Bits (QuBits), que podem existir em múltiplos estados simultaneamente, permitindo operações computacionais mais rápidas e eficientes em termos energéticos. Grandes empresas como Intel, Google, IBM e Microsoft estão investindo no desenvolvimento de computadores quânticos.

O impacto da computação quântica na criptografia é significativo, especialmente para os algoritmos de criptografia de chave pública, que protegem a maioria das transações eletrônicas. Explica Dodt que algoritmos como o RSA, que se baseiam na dificuldade de fatoração de grandes números inteiros, podem ser vulneráveis a computadores quânticos. O Algoritmo de Shor, por exemplo, pode simplificar a fatoração de números em componentes primos, tornando a criptografia de chave pública praticamente inútil. Contudo, algoritmos simétricos como o AES, com chaves de tamanho razoável (por exemplo, AES 256), ainda poderiam ser considerados seguros. Dodt menciona que já existem estudos tratando da criptografia pós-quântica, com alternativas como a criptografia baseada em reticulados, multivariada ou baseada em hash, que poderiam assegurar proteção no mundo pós-quântico.

Pimentel (2023b, p. 290) também reconhece o caráter experimental da criptografia quântica, que utiliza qubits ao invés de bits para fins de codificação da informação, sendo o método revolucionário por ser capaz de detectar tentativas de ataques.

Esta computação tem uma perspectiva de alteração profunda de paradigma, repercutindo na questão criptográfica em geral, visto que esta depende

da limitação da capacidade computacional, onde a suposição de que o atacante não terá condições instrumentais de testar as diferentes combinações. Esta mudança fundacional tem recebido o nome "Q-Day", consistindo em um evento no qual a computação quântica supere os limites para o rompimento dos sistemas de segurança, afetando o sistema bancário e comunicações governamentais, revelando uma corrida quântica mundial (Suleyman; Bhaskar, 2023, p. 128 e 158).

A segurança cibernética em blockchains desperta discussões em razão da crescente dependência da sociedade das plataformas e sistemas eletrônicos. Revoredo (2021) enfatiza a importância de gestores e tomadores de decisão prestarem atenção à cibersegurança em blockchains, especialmente em um mundo cada vez mais hiperconectado. Um ponto chave abordado pela autora é a proteção da «tríade da CIA» (Confidencialidade, Integridade, Autenticidade) com Blockchain. A confidencialidade é vista como crucial para proteger dados contra acessos indevidos ou roubo, e blockchains oferecem suporte a isso por meio do gerenciamento de direitos de acesso. A integridade é mantida pela precisão e consistência dos dados, com a tecnologia blockchain apoiando isso através de carimbos de data/hora. A autenticidade, que garante a veracidade dos dados, também é reforçada por blockchains que fornecem credenciais digitais e garantem a escassez digital.

Os contratos inteligentes estão expostos aos ataques, sendo compostos, conforme Revoredo por códigos autoexecutáveis geridos por um blockchain e apresentam várias vulnerabilidades, como serem acessíveis ao público e imutáveis, o que impede a correção de bugs após o lançamento. A autora também aponta para problemas comuns de segurança fora da cadeia, como vulnerabilidades em bancos de dados, sites, gerenciamento de chaves e APIs, que compõem uma grande parte dos aplicativos blockchain e são frequentemente negligenciados[43]. Ela cita exemplos de incidentes de segurança comuns, incluindo autenticação insegura e uso incorreto de criptografia.

Dentre os fatores de risco, está a interação humana, isso decorrente de possíveis desleixos e do desleixo e comportamento irracional, sendo destacado por Revoredo que as ações humanas, como engenharia social e vazamento de informações, são comuns em termos de comprometimento da segurança cibernética. Em que pese a autora reconhecer que os protocolos de blockchain

43 "Pois bem, quando um sistema computacional utiliza um servido central que detém o poder sobre qual decisão tomar diante de determinada situação, os usuários tendem a confiar na decisão adotada pelo servidor central. Por outro lado, quando a informação e o poder de decidir são compartilhados entre vários servidores a desconfiança surge à medida que o risco de ataques cibernéticos aumenta" (PIMENTEL, 2023b, p. 307).

sejam seguros, mas não estão imunes a ataques. A segurança varia conforme os diferentes tipos de blockchain, com diferenças entre blockchains públicos e privados, assim como entre estruturas não permissionadas e permissionadas.

Assiste razão à autora quando defende a necessidade de ações defensivas contra ataques, além do constante escrutino dos sistemas contras as vulnerabilidades, sendo que, apenar dos riscos, a tecnologia blockchain é atraente para a mitigação do risco cibernético, especialmente em estruturas mais descentralizadas.

4.5.3 COLETA E USO DE DADOS: RECONHECIMENTO BIOMÉTRICO EM ASSINATURAS DIGITAIS

Devido à facilidade de coleta e utilização, os dados biométricos estão sendo cada vez mais utilizados, seja para ingresso em instalações, seja para o registro do consumidor no momento da contratação de um serviço de telefonia ou aquisição de crédito em instituição financeira. O uso indiscriminado da técnica alimenta os diversos sistemas de informação e comunicação com dados pessoais dos consumidores, especialmente aquelas envolvendo o reconhecimento facial (Alvoreda, 2019).

O big data tem como dentre uma de suas características o valor, intrínseco ao capitalismo digital, cuja informação tem sua utilidade na aplicação de vários sistemas, tendo interesse mercadológico (Pimentel, 2023d, p. 121). Sendo os dados biométricos úteis para a identificação do consumidor, deve-se reconhecer o seu valor para o mercado, abrindo uma nova frente no risco cibernético de violação de sua identidade com repercussão na validade e eficácia dos contratos digitais.

Alvoreda destaca que a LGPD classifica dados biométricos como dados pessoais sensíveis, exigindo consentimento específico e destacado para o seu tratamento, exceto em situações específicas que visam proteger a vida, a saúde do usuário ou cumprir determinações legais. Neste ponto, os controladores dos dados biométricos possuem responsabilidade na informação, coleta e tratamento dos dados biométricos, podendo o usuário exercer o direito de oposição.

Todavia, para que o consumidor possa exercer o direito de oposição, deve estar adequadamente informado dos riscos inerentes. Isso se torna um desafio ainda maior diante de parcela significativa da sociedade que não tem acesso à informação adequada sobre a coleta e tratamento de dados pessoais, sendo este um novo ponto a ser discutido a seguir

4.5.4 PROBLEMA DA VULNERABILIDADE E EXCLUSÃO DIGITAL

As transformações nas relações humanas e comerciais trazidas pela internet e pelas Tecnologias da Informação e Comunicação (TICs) são abordadas por Lehfeld; Contin; Siqueira; Barufi, 2020, destacando a transição do valor dos bens materiais para os imateriais, como dados pessoais e seguidores online. Enfatizam que, apesar da aparente insignificância, dados pessoais podem ser valiosos e perigosos, especialmente quando combinados com outras informações.

Segundo os autores, a Sociedade da Informação, caracterizada pela revolução tecnológica, gerou inúmeras possibilidades, mas também expôs lacunas na legislação e práticas de proteção de bens jurídicos fundamentais. O ciberespaço, descrito como uma extensão do espaço geográfico, é visto como carente de regras de convivência similares às do mundo físico.

A vulnerabilidade dos consumidores na web é exacerbada pela armazenagem, análise e compartilhamento de dados por empresas visando lucro, negligência e falta de segurança, tornando-os alvos de práticas publicitárias, financeiras abusivas e criminosos virtuais. Apontam os autores a respeito da precariedade no combate aos crimes cibernéticos e a crescente vulnerabilidade dos consumidores devido à importância atribuída às suas informações, que podem ser exploradas tanto por empresas quanto por cibercriminosos. O crime online é diferenciado do crime físico por sua natureza menos tangível e visível, tornando-se um desafio em termos de detecção e solução. A informatização em rede proporcionou melhorias na vida das pessoas, mas também relaxou a postura de segurança dos usuários, atraindo indivíduos com elevado conhecimento tecnológico que cometem crimes cibernéticos.

Lehfeld, Contin, Siqueira e Barufi concluem que dados pessoais devem ser considerados não apenas como fonte de riqueza, mas principalmente como fonte de poder, particularmente para fins de controle social. A ausência de proteção adequada para os consumidores online representa uma ameaça aos direitos fundamentais, tornando a internet um meio potencial para a violação desses direitos.

Segundo Pimentel (2023b, p. 83), enquanto os excluídos digitais não estão na rede, os vulneráveis "são aqueles que, por alguma deficiência sensorial, cognitiva ou financeira, estão na rede, mas apresentam essa condição de deficiência ou limitação no acesso ou na compreensão do funcionamento do sistema social-digital".

O Estatuto dos Jovens (Lei Federal nº 12.852/2013), o Estatuto do Idoso (Lei Federal nº 10.741/2003) e a Lei do Marco Civil da Internet (Lei Federal nº

12.965/2014) trazem disposições para a inclusão das pessoas à rede, pois, como enfatizado por Hartmann (2017), a Internet não deve ser considerada apenas como uma tecnologia, mas como um meio de comunicação essencial que estabeleceu uma nova esfera pública. Esta nova dimensão impactou significativamente a realização de diversos Direitos Fundamentais, de modo que o acesso deve ser reconhecido como um direito fundamental. Hartmann enfatiza que para os indivíduos, diversos aspectos da vida social estão intrinsecamente ligados ao acesso à rede, exigindo o livre acesso à rede mundial de computadores para todos. Reconhece a responsabilidade do Estado em manter terminais de acesso em condições operacionais, derivado dos princípios fundamentais da cidadania, relacionando-se com a fiscalização da atuação estatal e a participação popular no governo, e da dignidade humana, sendo essencial para a noção de autonomia, identidade pessoal e acesso à informação.

Para Hartmann, o direito de acesso à Internet é hoje um "direito sindicável", sublinhando a importância de manter políticas públicas estatais que visem alcançar a inclusão digital de milhões de brasileiros. Isso ressalta o papel vital do Estado na facilitação do acesso à Internet como um meio para garantir a inclusão social e digital, e como um direito fundamental para o exercício pleno da cidadania e dignidade humana.

Além desta preocupação com a exclusão, Pimentel (2023b, p. 77) ressalta a questão da vulnerabilidade cibernética, onde pessoas suscetíveis ao engodo, manipulação, ofensas, armadilhas e golpes estão expostas no ambiente virtual.

Chama a atenção o rápido avanço das relações sociais digitais tem feito na sociedade, de modo que não só o aspecto exclusivo, mas também a vulnerabilidade daqueles que acessam a rede, seja por curiosidade, seja por diversão, seja por necessidade, estão expostos diariamente. A norma não pode se limitar apenas a garantir o acesso, mas desenvolver o acesso consciente e responsável, frente aos desafios das novas tecnologias, especialmente para a realização de negócios jurídicos, onde a manifestação de vontade do consumidor deve estar embasada na transparência, informação, segurança e boa-fé.

CONCLUSÃO

Diante dos novos desafios que o ambiente digital apresenta para a validade e eficácia dos negócios jurídicos, é importante o estudo das formas legítimas de manifestação de vontade do consumidor, isso em razão da sua vulnerabilidade na própria relação jurídica, conforme reconhecido pelo Código de Defesa

do Consumidor, como também diante da ambiência digital, em que as relações são discutidas, formadas e executadas sem tangibilidade. A pesquisa procurou discutir a validade e eficácia da assinatura eletrônica em documentos digitais, especialmente nas relações de consumo investigando a sua relevância e função, as regulações existentes, a validade e eficácia dos contratos digitais e a proteção do consumidor quanto à assinatura eletrônica.

Sobre a questão da relevância e função da assinatura eletrônica, verifica-se a interação dinâmica entre a segurança jurídica e a inovação tecnológica, especialmente no âmbito das relações contratuais digitais e a validade destas assinaturas. Foi enfatizada a importância da segurança jurídica como alicerce para a confiança, estabilidade e previsibilidade nas relações jurídicas, reconhecendo, simultaneamente, a necessidade de adaptabilidade frente às rápidas mudanças tecnológicas. Deve-se observar um equilíbrio entre segurança jurídica e justiça, propondo-se que, embora a segurança jurídica deva prevalecer na maioria dos casos, a justiça deve ser a prioridade em situações de injustiça flagrante.

Com isso, a adaptação das normativas jurídicas à realidade digital é uma necessidade para a própria segurança da relação jurídica, sublinhando-se a necessidade de reinterpretação e ponderação normativa para assegurar a validade e eficácia dos contratos digitais. A incorporação e regulação de novas formas de relacionamento contratual pelo direito são vistas como essenciais para capturar e reconhecer autenticamente a manifestação de vontade em ambientes digitais.

A segurança jurídica, longe de ser um obstáculo à inovação, deve ser vista como um pilar adaptável que apoia a evolução do direito e da sociedade em face da digitalização das relações contratuais. As assinaturas eletrônicas, como expressões de vontade no ambiente digital, necessitam de validação e eficácia jurídica num sistema que acolha as transformações tecnológicas, mantendo a estabilidade e confiança vitais às relações contratuais.

Além disso, a aplicabilidade dos princípios contratuais clássicos no contexto digital exige uma adaptação na sua interpretação e aplicação. A autonomia da vontade, a vinculação contratual, a boa-fé e o consentimento livre e esclarecido mantêm-se como pilares, enfatizando a importância de mecanismos que assegurem um consentimento genuinamente informado e a preservação da justiça e equidade nas transações digitais.

A transição do papel para o digital, portanto, reflete não apenas uma evolução tecnológica, mas também desafios jurídicos e éticos significativos. A validade e eficácia das assinaturas eletrônicas, ancoradas nos princípios contratuais adaptados à era digital, são fundamentais para manter a confiança e a justiça nas modernas relações contratuais, exigindo uma evolução do direito

contratual em harmonia com as tecnologias digitais para garantir que os princípios contratuais continuem a fornecer um sólido alicerce jurídico no século XXI.

Sobre o aspecto regulatório, foi apontada a crescente importância da regulamentação das assinaturas eletrônicas e documentos digitais no cenário internacional, destacando as iniciativas e desafios específicos no Mercosul, Estados Unidos e Europa. No contexto do Mercosul, a cooperação regional e o reconhecimento mútuo das assinaturas eletrônicas são apontados como passos positivos para a integração digital, visando aumentar a eficiência e a segurança jurídica nas transações comerciais. Nos Estados Unidos, a discussão se concentra na influência das regulamentações americanas, como o *E-Sign Act* e o UETA, ressaltando a importância da conformidade regulatória para empresas brasileiras que desejam operar neste mercado, e destaca a proteção ao consumidor e a segurança dos dados. A Europa é examinada através do prisma do Regulamento eIDAS, que estabelece um marco regulatório para a identificação eletrônica e as assinaturas digitais, promovendo a interoperabilidade e a segurança nas transações eletrônicas transfronteiriças.

Deve-se considerar a necessidade de harmonização das leis sobre assinaturas e documentos eletrônicos para facilitar o comércio eletrônico e as transações digitais de forma segura e eficiente em um ambiente global. A cooperação internacional e o desenvolvimento de padrões comuns são essenciais para superar barreiras técnicas e jurídicas, promovendo um ambiente digital confiável e integrado, que apoia o crescimento econômico e a inovação tecnológica.

A Lei Modelo da UNCITRAL sobre Comércio Eletrônico e a Medida Provisória nº 2.200-2/2001 do Brasil, juntamente com a implementação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), representam avanços significativos no reconhecimento e validade jurídica das transações eletrônicas e das assinaturas eletrônicas. Essas iniciativas refletem um esforço global e nacional para adaptar os sistemas jurídicos às realidades do comércio eletrônico, promovendo a harmonização das legislações, a segurança das transações eletrônicas, e a eficiência operacional. A Lei Modelo da UNCITRAL promove a unificação progressiva das legislações, reduzindo barreiras jurídicas e aumentando a segurança e previsibilidade das operações eletrônicas, enquanto a ICP-Brasil estabelece um sistema confiável para a autenticação de documentos eletrônicos no Brasil, alinhando o país com padrões internacionais de segurança digital.

Estas duas referências normativas têm em comum a ênfase na segurança jurídica e na validade das assinaturas eletrônicas, sendo fundamental para a confiança do mercado e o desenvolvimento sustentável do comércio eletrônico global. Além disso, destaca-se a importância da flexibilidade regulatória para

adaptar-se às novas tecnologias e às diversas legislações nacionais, sem necessidade de constantes revisões legislativas. A inclusão digital de países em desenvolvimento e a promoção de um ambiente jurídico estável e previsível para as transações eletrônicas contribuem significativamente para o desenvolvimento de relações econômicas internacionais mais harmoniosas e eficientes.

A eficácia e a segurança dos diferentes tipos de certificados digitais, particularmente aqueles emitidos pela ICP-Brasil, são fundamentais para garantir a autenticidade, integridade, e validade jurídica dos documentos eletrônicos, estabelecendo uma base sólida para o crescimento econômico e a modernização do país. A discussão sobre a teoria geral da vontade e sua adaptação ao meio digital reforça a necessidade de entender as implicações jurídicas e tecnológicas das assinaturas eletrônicas, assegurando que as transações digitais sejam realizadas de maneira segura e eficiente, promovendo a confiança e a inclusão digital no cenário global.

Também é de se considerar a importância da interdisciplinaridade entre o Direito e a tecnologia para superar esses desafios, sugerindo que soluções tecnológicas avançadas, aliadas a uma reflexão jurídica adaptada à realidade digital, são fundamentais. O conceito de cidadania digital é introduzido como essencial para promover um acesso irrestrito à internet e a proteção de direitos fundamentais na era digital, apoiando a construção de um ambiente digital justo e equitativo.

A integração efetiva entre princípios jurídicos tradicionais e inovações tecnológicas é vital para o desenvolvimento e implementação de contratos digitais que sejam não apenas eficientes, mas também justos, seguros e respeitadores dos direitos fundamentais dos usuários. Este equilíbrio entre inovação e tradição jurídica abre caminhos para futuras pesquisas e práticas que fortaleçam a segurança jurídica e a proteção do consumidor na era digital, refletindo um compromisso contínuo com a melhoria da cidadania digital e a alfabetização digital em uma sociedade cada vez mais conectada.

A ênfase na cidadania digital e na alfabetização digital é um caminho que deve ser seguido para garantir que os indivíduos possam participar efetivamente e de maneira informada no ambiente digital, assegurando a validade e a eficácia das suas manifestações de vontade em contratos digitais. A jurisprudência e a legislação têm evoluído para reconhecer a equivalência entre assinaturas digitais e manuscritas, fortalecendo a segurança jurídica e a confiança nas transações eletrônicas, ao mesmo tempo que enfrentam os desafios de validade contratual e resolução de disputas em um contexto globalizado.

A introdução de contratos inteligentes, apoiada pela tecnologia blockchain e potencialmente ampliada pela inteligência artificial, representa um avanço significativo na automatização e execução de acordos contratuais, prometendo

eficiência, segurança e transparência. No entanto, essas inovações também trazem desafios relacionados à segurança, governança e à superação de barreiras legais e práticas para sua implementação eficaz.

Além disso, a detecção e o tratamento de vícios da vontade em contratos digitais exigem uma abordagem renovada, considerando as peculiaridades do ambiente digital e a necessidade de proteger os consumidores contra práticas predatórias e injustas. A adoção da teoria da confiança como um meio de abordar esses vícios representa um passo positivo na proteção dos direitos dos consumidores, enfatizando a importância da boa-fé e da transparência nas relações contratuais digitais.

Sobre a validade e eficácia dos contratos digitais, conclui-se que a inserção de tecnologias digitais na celebração de contratos jurídicos representa um avanço notável, oferecendo facilidades e enfrentando desafios únicos. A legislação brasileira, incluindo o Código Civil de 2002 e legislações complementares, reconhece a validade e eficácia desses contratos digitais, abordando aspectos fundamentais como capacidade, objeto, causa, consenso e forma. No entanto, a natureza digital desses contratos traz desafios específicos, como a autenticidade, integridade e confiabilidade dos documentos digitais, além da segurança das transações eletrônicas.

A jurisprudência brasileira desempenha um papel de destaque na adaptação e reconhecimento da validade dos contratos digitais, reconhecendo medidas como o uso de assinaturas eletrônicas qualificadas para assegurar a segurança jurídica. Ainda assim, a plena implementação e aceitação dos contratos digitais dependem da superação de desafios tecnológicos, culturais e legais.

Elementos clássicos de validade contratual, como a capacidade das partes, a licitude do objeto e a forma do contrato, mantêm sua relevância no ambiente digital, exigindo adaptações específicas para essa nova realidade. A legislação brasileira e a prática judicial mostram um comprometimento em adaptar-se às inovações tecnológicas, garantindo que os contratos digitais sejam tão robustos e confiáveis quanto os tradicionais.

A equivalência funcional entre documentos digitais e tradicionais é enfatizada, com o uso de assinaturas digitais baseadas em criptografia de chave pública sendo reconhecido legalmente no Brasil. Esse reconhecimento alinha o país com práticas internacionais de segurança e validação eletrônica, destacando a importância de uma base legal confiável para a autenticação digital.

Além da validade, é relevante garantir que os negócios jurídicos digitais produzam os efeitos desejados, considerando a segurança dos dados, a autenticidade das partes e a clareza das informações. A proteção efetiva do consumidor

em transações online requer esforços para garantir que os consumidores estejam plenamente informados e que suas escolhas sejam respeitadas.

A proteção do consumidor neste novo ambiente digital envolve a compreensão de que o avanço do comércio eletrônico e a adoção crescente de tecnologias digitais, surgem desafios significativos relacionados à proteção de dados, à segurança das transações e à garantia dos direitos dos consumidores. A legislação, como a LGPD no Brasil, e outras regulamentações globais, procuram mitigar esses riscos nas relações de consumo, estabelecendo um quadro legal para a segurança e transparência das transações digitais.

Neste cenário, a atuação de agências reguladoras e órgãos de defesa do consumidor é fundamental na implementação e fiscalização das normativas que visam proteger os interesses dos consumidores no ambiente digital. Além disso, a responsabilidade das empresas em adotar práticas de mercado responsáveis e em conformidade com as leis de proteção ao consumidor é reconhecida, incluindo a importância da transparência e do tratamento adequado de dados pessoais.

A pesquisa indica a necessidade de uma abordagem multifacetada que inclui não somente legislação robusta e regulamentação eficaz, mas também a educação do consumidor sobre seus direitos e riscos associados às transações digitais. A evolução tecnológica, incluindo o uso de autenticação de dois fatores, blockchain e criptografia quântica, apresenta métodos promissores para aumentar a segurança, mas também levanta questões sobre inclusão digital e usabilidade.

A integração de novas tecnologias, como IA, IoT, e análise de grandes volumes de dados, transforma o cenário dos contratos digitais, oferecendo eficiências operacionais e desafiando simultaneamente a autonomia e a privacidade dos consumidores. A inclusão digital emerge como uma questão que exige o desenvolvimento de políticas públicas e designs tecnológicos que promovam o acesso equitativo e a literacia digital, garantindo que os benefícios das inovações digitais sejam acessíveis a todos.

A pesquisa sublinha a importância de uma colaboração contínua entre legisladores, reguladores, empresas e consumidores para adaptar as estratégias de proteção ao consumidor ao ambiente digital em evolução. Este esforço conjunto é essencial para garantir que os direitos dos consumidores sejam efetivamente protegidos em um cenário cada vez mais digitalizado, corporificado e interconectado, onde novas tecnologias oferecem tanto oportunidades quanto desafios para a validade e eficácia das assinaturas eletrônicas nos contratos digitais.

REFERÊNCIAS

ADAMS, Carlisle; LLOYD, Steve. **Understandig public-key infrastructure: concepts, standards, and deployment considerations**. Indianapolis: New Riders, 1999.

AITH, Fernando; DALLARI, Analluza. **18. Aspectos e Desafios de Compliance com a Lgpd na Digitalização de Um Estabelecimento de Saúde** In: AITH, Fernando; DALLARI, Analluza. Lgpd na Saúde Digital. São Paulo (SP):Editora Revista dos Tribunais. 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/lgpd-na-saude-digital/1620615596. Acesso em: 3 de Dez. de 2023.

ALVES. José Carlos Moreira. **A parte geral do projeto de código civil brasileiro**. 2ª ed. São Paulo: Saraiva, 2003.

ALVOREDA, Gustavo Laudanna. **Riscos no uso indiscruminaod de dados biométricos**. 2019. Disponível em : https://www.migalhas.com.br/amp/depeso/301528/riscos-no-uso-indiscriminado-de-dados-biometricos. Acesso em 08 de dez. de 2023.

AMAZON. **Pedidos usando o recurso comprar agora**. Disponível em : https://www.amazon.com.br/gp/help/customer/display.html?nodeId=GU224Z5TL5RBQTJA. Acesso em 28 de nov. de 2023.

AMERICAN BAR ASSOCIATION. **Comment Concerning Use of Electronic Signatures and Third-Party Opinion Letters**. 2020. Disponível em: https://www.americanbar.org/groups/business_law/resources/business-law-today/2020-april/comment-concerning-use-of-electronic-signatures/. Acesso em 20 de nov. de 2023.

AQUINES, Tiago. **Idosos são alvo fácil de empréstimos consignados irregulares; saiba como fugir dos golpes**. 2018. Disponível em: https://www.jusbrasil.com.br/noticias/idosos-sao-alvo-facil-de-emprestimos-consignados-irregulares-saiba-como-fugir-dos-golpes/695547829. Acesso em 04 de dez. de 2023.

ASSOCIAÇÃO DOS MAGISTRADOS DO ESTADO DE RONDÔNIA. **ICP-Brasil oferece segurança e redução de custos**. 2010. Disponível em https://www.jusbrasil.com.br/noticias/artigo-icp-brasil-oferece-seguranca-e-reducao-de-custos/2543502. Acesso em 22 de nov. de 2023.

AZEVEDO, Antonio Junqueira de. **Negócio jurídico: existência, validade e eficácia**. 4. ed. São Paulo: Saraiva, 2002.

BENINCASA, Felipe. **Assinatura digital simples, avançada e qualificada? Entenda**. 2023. Disponível em: https://blog.validcertificadora.com.br/assinatura-digital-simples-avancada-e-qualificada/. Acesso em 29 de nov. de 2023.

BENJAMIN, Antonio Herman V; MARQUES, Cláudia Lima; BESSA, Leonardo Roscoe. **Manual de direito do consumidor** [livro eletrônico]. 9ª ed. São Paulo: Thomson Reuters Brasil, 2021.

BIONI, Bruno Ricardo; LUCIANO, Maria. **O consentimento como processo: em busca do consentimento válido**. In: BIONI, Bruno Ricardo (coord.). Tratado de proteção de dados pessoais. Rio de Janeiro Forense, 2021.

BRANCHER, Paulo Marcos Rodrigues. **Comércio Eletrônico**. 2018. Disponível em: https: //enciclopediajuridica.pucsp.br/verbete/258/edicao-1/comercio-eletronico. Acesso em 21 de nov. de 2023.

BRASIL. Ministério da Justiça. **Convenção de Budapeste é promulgada no Brasil**. 2023. Disponível em : https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em 21 de nov. de 2023.

BRASIL. STJ. **AgInt no AREsp 1691485 / PE**. Disponível em : https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27AINTARESP%27.clas.+e+@num=%271691485 %27)+ou+(%27AgInt%20no%20AREsp%27+adj+%271691485 %27).suce.)&thesaurus=JURIDICO&fr=veja. Acesso em 30 de nov. de 2023.

BRASIL. STJ. **Informativo nº 507**. 2012. Disponível em : https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=%270507 %27.cod. Acesso em 30 de nov. de 2023.

BRASIL. STJ. **Resolução nº 01/2010**. Disponível em : https://bdjur.stj.jus.br/jspui/bitstream/2011/27153/Res%20_1_2010_PRE.pdf. Acesso em 30 de nov. de 2023.

BRASIL. STJ. **REsp 1.495.920/DF**, Rel. Ministro Paulo de Tarso Sanseverino, Terceira Turma, julgado em 15/5/2018, DJe 7/6/2018.

BRASIL. TJPR. **Processo nº 0006574-55.2022.8.16.0193**. Disponível em https://www.jusbrasil.com.br/jurisprudencia/tj-pr/1895301701. Acesso em 30 de nov. de 2023.

BRASIL. Tribunal de Justiça do Estado de Minas Gerais. **AC: 10000211464193001 MG**, Relator: Habib Felippe Jabour, Data de Julgamento: 31/08/2021, Câmaras Cíveis / 18ª CÂMARA CÍVEL, Data de Publicação: 01/09/2021.

BRASIL. Tribunal de Justiça do Estado de São Paulo. **AC: 10436015120208260224 SP 1043601-51.2020.8.26.0224**, Relator: Maria Lúcia Pizzotti, Data de Julgamento: 27/08/2021, 30ª Câmara de Direito Privado, Data de Publicação: 27/08/2021.

BRASIL. TRT DA 6ª REGIÃO. **Visual Law: iniciativa piloto usa linguagem gráfica para facilitar compreensão de um julgamento**. 2021. Disponível em : https://www.trt6.jus.br/portal/noticias/2021/07/21/visual-law-iniciativa-piloto-usa-linguagem-grafica-para-facilitar-compreensao-de. Acesso em 23 de nov. de 2023.

BURNETT, Steve; PAINE, Stephen. **RSA security´s official guide to cryptography.** Nova Iorque: McGraw-Hill, 2001.

CABRAL, Antonio do Passo. **Segurança jurídica e regras de transição nos processos judicial e administrativo. intordução ao art. 23 da LINDB**. 2a edição. Salvador Editora JusPodium 2021.

CÂMARA DOS DEPUTADOS. **Câmara aprova acordo de reconhecimento mútuo de certificados de assinatura digital no Mercosul**. 2023. Disponível em : https://www.camara.leg.br/noticias/1008469-camara-aprova-acordo-de-reconhecimento-mutuo-de-certificados-de-assinatura-digital-no-mercosul. Acesso em 20 de nov. de 2023.

CAMUS, Albert. **O mito de sísifo**. Rio de Janeiro: Record, 2018.

CARNEIRO LEÃO, Emmanuel. **Heráclito e a aprendizagem do pensamento**. Kléos nº 1. Páginas 113-142. 1997. Disponível em : https://www.pragma.ifcs.ufrj.br/kleos/K1/scan/CarneiroLeao.pdf. Acesso em 10 de dez. de 2023.

COELHO, Fábio. **Curso de Direito Comercial: Contratos, Falência e Recuperação de Empresas**. São Paulo (SP):Editora Revista dos Tribunais. 2020. Disponível em: https://www.jusbrasil.com.br/doutrina/curso-de-direito-comercial-contratos-falencia-e-recuperacao-de-empresas/1188258344. Acesso em: 4 dez. 2023.

DELBEN, Ana Cleusa; MANUELA, Ana. **A causa do negócio jurídico. Trabalho publicado nos Anais do XIX Encontro Nacional do CONPEDI realizado em Fortaleza - CE nos dias 09, 10, 11 e 12 de Junho de 2010**. Disponível em: http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/fortaleza/3727.pdf. Acesso em 27 de nov. de 2023.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**. 1 Teoria geral do direito civil. 29ª ed. São Paulo: Saraiva, 2012.

DODT, Cláudio. **Computação quântica e seus efeitos na criptografia**. 2021. Disponível em: https://tiinside.com.br/10/09/2021/computacao-quantica-e-seus-efeitos-na-criptografia/. Acesso em 07 de dez. de 2023.

DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. Páginas 03-20. In: BIONI, Bruno Ricardo (coord.). Tratado de proteção de dados pessoais. Rio de Janeiro Forense, 2021.

DRESCH, Leonardo Antônio; FREITAS, Cinthia Obladen de Almendra Freitas. **A violação da privacidade a partir de dados pessoais obtidos do aceite dos termos de uso e o impacto da lei geral de proteção de dados**. In TOALDO et al. Org. Tecnologia e Direito. Páginas 249-266. Rio de Janeiro: Pembroke Collins, 2021.

DUARTE, Breno. **Ônus da prova e convencimento judicial no processo civil brasileiro**. Curitiba: Juruá, 2020.

DUTENKEFER, Vinícius; LEAL, William. **Direito do Consumidor: a evolução tecnológica e seus desafios**. 2018. Disponível em https://www.migalhas.com.br/depeso/276641/direito-do-consumidor--a-evolucao-tecnologica-e-seus-desafios. Acesso em 01 de dez. de 2023.

ELLUL, Jacques. **Le bluff technologique**. Paris: Hachette, 1988. Edição digital EPUB.

ESTADOS UNIDOS : FDA. **Code of federal regulations title 21**. 2023. Disponível em : https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=11.1. Acesso em 20 de nov. de 2023.

ESTADOS UNIDOS. **Electronic signatures in global and national commerce act**. Disponível em: https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf. Acesso em 20 de nov. de 2023.

ESTADOS UNIDOS: FDIC. **Consumer Compliance Examination Manual**. 2023. Disponível em : https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/index.html. Acesso em 20 de nov. de 2023.

EZRACHI, A. & STUCKE, M. **Virtual competition**. Cambridge, MA et al.: Harvard University Press, 2016. Apud: GRUNDMANN, Stefan ; HACKER, Philipp. Digital technology as a challenge to european contract law. From the existing to the future architecture. 2019. Disponível em : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3003885. Acesso em 26 de nov. de 2023.

FEITOSA, Douglas de Lima; GARCIA, Leandro Sumida. **Sistemas de Reputação: Um Estudo sobre Confiança e Reputação no Comércio Eletrônico Brasileiro**. 2015. Disponível em http://www.anpad.org.br/rac. Acesso em 01 de dez. de 2023.

FERNANDES, Priscila Gonçalves. **O direito e a internet. Comércio eletrônico**. Artigo Científico apresentado como exigência de conclusão de Curso de Pós-Graduação Lato Sensu da Escola de Magistratura do Estado do Rio de Janeiro. 2012. Disponível em : https://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/1semestre2012/trabalhos_12012/priscilagoncalvesfernandes.pdf. Acesso em 21 de nov. de 2023.

FILOMENO, José Geraldo Brito. **Alterações do código de defesa do consumidor - Críticas às propostas da comissão especial do Senado Federal**. 2012. Disponível em: https://bdjur.stj.jus.br/jspui/bitstream/2011/72700/alteracoes_codigo_defesa_filomeno.pdf. Acesso em 01 de dez. de 2023.

FINKELSTEIN, Maria Eugênia Reis; SOCCO NETO, Fernando. **Manual de direito do consumidor**. Rio de Janeiro: Elsevier, 2010.

FRAZÃO, Ana; CUEVA, Ricardo. **12. Risco, Compliance e Proteção de Dados** In: FRAZÃO, Ana; CUEVA, Ricardo. Compliance e Políticas de Proteção de Dados. São Paulo (SP):Editora Revista dos Tribunais. 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/compliance-e-politicas-de-protecao-de-dados/1506551345. Acesso em: 5 de Dez. de 2023.

FRAZÃO, Ana; CUEVA, Ricardo. **39. Desafios do Compliance de Dados para o Setor Financeiro: Pix, Open Banking e a Lei Geral de Proteção de Dados** In: FRAZÃO, Ana; CUEVA, Ricardo. Compliance e Políticas de Proteção de Dados. São Paulo (SP):Editora Revista dos Tribunais. 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/compliance-e-politicas-de-protecao-de-dados/1506551345. Acesso em: 5 de Dez. de 2023.

FREIRE, Raquel. **Autenticação de dois fatores: o que é e para que serve o recurso.** Artigo site Techtudo. 2021. Disponível em : https://www.techtudo.com.br/noticias/2021/08/autenticacao-de-dois-fatores-o-que-e-e-para-que-serve-o-recurso.ghtml. Acesso em 02 de dez. de 2023.

GARBI, Carlos Alberto. **A evolução do contrato e o seu controle judicial**. 2020. Disponível em https://www.migalhas.com.br/amp/coluna/novos-horizontes-do-direito-privado/331920/a-evolucao-do-contrato-e-o-seu-controle-judicial. Acesso em 19 de nov. de 2023.

GARCIA, André Pinto. **ICP-Brasil oferece segurança e redução de custos**. 2010. Disponível em: https://www.jusbrasil.com.br/noticias/artigo-icp-brasil-oferece-seguranca-e-reducao-de-custos-por-andre-pinto-garcia/2540950. Acesso em 22 de nov. de 2023.

GILLIES, Lorna E. **Electronic commerce and international private law: A Study of Electronic Consumer Contracts**. Empshire: Ashgate, 2008.

GILMORE, Grant. **The death of contract**. Columbus : Ohio State University Press, 1974.

GOLDWASSER, Shafi; BELLARE, Mihir. **Lecture Notes on Cryptography**. 2008. Disponível em: https://cseweb.ucsd.edu/~mihir/papers/gb.pdf#page=168. Acesso em 19 de nov. de 2023.

GOMES, Orlando. **Contratos**. Rio de Janeiro, Forense, 2009.

GONÇALVES, Camila de Jesus Mello. **Princípio da boa-fé: Perspectivas e aplicações**. Rio de Janeiro: Elsevier, 2008.

GOOGLE. **Restrições de idade das contas google**. Disponível em : https://support.google.com/accounts/answer/1350409?hl=pt-BR. Acesso em 28 de nov. de 2023.

GOUVEIA, Lúcio Grassi de. **Interpretação criativa e realização do direito**. Recife: Bargaço, 2000.

GOUVEIA, Lúcio Grassi de; BREITENBACH, Fábio Gabriel. **Sistema de precedentes no novo código de processo civil brasileiro: um passo para o enfraquecimento da jurisprudência lotérica dos tribunais**. Páginas 491-520. In: DIDIER, Fredie et al (coord.). Precedentes. Salvador: Juspodivum, 2015.

GRUNDMANN, Stefan ; HACKER, Philipp. **Digital technology as a challenge to european contract law. From the existing to the future architecture.** 2019. Disponível em : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3003885. Acesso em 26 de nov. de 2023.

HARRALSON, Heidi H. Developments in handwritting and signature identification in the digital age. Oxford: Elsevier, 2013.

HARTMANN, Ivar Alberto Martins. O acesso à internet como direito fundamental. 2017. Disponível em : https://egov.ufsc.br/portal/sites/default/files/ivar_hartmann.pdf. Acesso em 08 de dez. de 2023.

HEIN, Cathrin; HEIN, Christoph; WELLBROCK, Wanja. **Rechtliche Herausforderungen von Blockchain-Anwendungen Straf-, Datenschutz- und Zivilrecht**. Wiesbaden: Springer Gabler, 2019.

HINE, Christine. **A internet 3E: uma internet incorporada, corporificada e cotidiana**. Tradução Carolina Parreira e Beatriz Accioly Lins. Disponível em : https://www.revistas.usp.br/cadernosdecampo/article/view/181370/168259. Acesso em 26 de fev. de 2024.

HOBSBAWM, Eric. **Da Revolução Industrial inglesa ao imperialismo**. Tradução de Donaldson Magalhães Garschagen. 5. ed. Rio de Janeiro: Forense Umversitária, 2000.

HUBER, Peter. **Der inhalt des Schuldverhältnisses**. Páginas 123-158. In Staudingers, J. von. Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen. Eckpfeiler des Zivilrechts. Berlin: Sellier – de Gruyter, 2008.

IDEC - Instituto Brasileiro de Defesa do Consumidor. **Telemarketing abusivo: saiba o que as empresas não podem fazer com você**. 2022. Disponível em: https://idec.org.br/dicas-e-direitos/telemarketing-abusivo-saiba-o-que-empresas-nao-podem-fazer-com-voce. Acesso em 28 de jan. de 2024.

IFOOD. **Como se cadastrar no iFood para pedir seu delivery.** Disponível em : https://www.news.ifood.com.br/como-se-cadastrar-no-ifood-cliente/. Acesso em 28 de nov. de 2023.

JUNIOR, Nelson. **Soluções práticas de direito: direito civil: parte geral e responsabilidade civil.** São Paulo (SP): Editora Revista dos Tribunais. 2014. Disponível em: https://www.jusbrasil.com.br/doutrina/solucoes-praticas-de-direito-direito-civil-parte-geral-e-responsabilidade-civil/1327487122. Acesso em: 5 de Dez. de 2023.

KATZ, Jonathan; LINDELL, Yehuda. **Introduction to modern cryptography**. 2ª ed. NewYork : CRC Press, 2015. Livro digital.

KEYNES, John M. **O fim do laissez-faire**. Disponível em : https://edisciplinas.usp.br/pluginfile.php/4312431/mod_resource/content/1/KEYNES%2C%20John%20M.%20-%20O%20fim%20do%20laissez-faire%201926.pdf. Acesso em: 28 de jan. de 2024.

LAMY, M., & AKAOUI, F. R. V. (2018). **Vícios do consentimento nos contratos de saúde.** Revista Brasileira De Direito Civil, 18, 17. Disponível em https://rbdcivil.ibdcivil.org.br/rbdc/article/view/304. Acesso em 28 de jan. de 2024.

LANGENBACH, C.J.; ULRICH, O (org). **Elektronische signaturen: kulturelle rahmenbedingungen einer technischen entwicklung**. Berlin-Heidelberg: Springer, 2002

LEHFELD, Lucas de Souza; CONTIN, Alexandre Celioto; SIQUEIRA, Oniye Nashara; BARUFI, Renato Britto**. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD**. 2020. Revista Eletrônica Pesquiseduca Revista do Programa de Educação - Universidade Católica de Santos. Disponível em : https://periodicos.unisantos.br/pesquiseduca/article/download/1029/902/2789. Acesso em 08 de dez. de 2023.

LEPAN, Nicholas, **Visualizing the Length of the Fine Print, for 14 Popular Apps**, 2020. Disponivel em: https://www.visualcapitalist.com/terms-of-service-visualizing-the-length-of-internet-agreements/. Acesso em 23 de nov. de 2023.

LIMA, Rogério Montai de. **Relações contratuais na internet e proteção jurídica do consumidor**. Dissertação apresentada ao Programa de Mestrado em Direito da Universidade de Marília, como exigência parcial para a obtenção do grau de Mestre em Direito. 2007. Disponível em : http://www.dominiopublico.gov.br/download/teste/arqs/cp063050.pdf. Acesso em 21 de nov. de 2023.

LO Swee Won; WANG Yu e LEE, David Kuo Chuen. **Blockchain and smart contracts. Design thinkin and programmin for fintech**. Singapura: World Scientific Publishing, 2021.

LUCIANO, Cláudia Regina Damasceno. **Metadados em ambientes de data warehouse utilizando tecnologia xml**. 2004. Disponível em : https://repositorio.ufsc.br/bitstream/handle/123456789/183811/Metadados.pdf?sequence=-1&isAllowed=y. Acesso em 02 de dez. de 2023.

MALONE, Mike. **Everything you should know about certificates and PKI but are too afraid to ask**. 2023. Disponível em : https://smallstep.com/blog/everything-pki/. Acesso em 19 de nov. de 2023.

MARQUES, Claudia et al**. Contratos de Serviços em Tempos Digitais**. São Paulo (SP):Editora Revista dos Tribunais. 2021. Disponível em: https://www.jusbrasil.com.br/doutrina/contratos-de-servicos-em-tempos-digitais/1314940703. Acesso em: 5 de Dez. de 2023.

MARQUES, Claudia. **Comentários ao Código de Defesa do Consumidor**. São Paulo (SP):Editora Revista dos Tribunais. 2019. Disponível em: https://www.jusbrasil.com.br/doutrina/comentarios-ao-codigo-de-defesa-do-consumidor/1199048235. Acesso em: 5 de Dez. de 2023.

MARZULLO, Renata Zappelli; OLIVEIRA, André Ribeiro de e MONAT, André Soares. **Visualização de contratos eletrônicos: uma proposta de artefato com base em Proposições de Design**. 2021. Disponível em https://estudosemdesign.emnuvens.com.br/design/article/download/1146/462. Acesso em 23 de nov. de 2023.

MENKE, Fabiano. **Assinatura eletrônica (ICP-Brasil). In Enciclopédia jurídica da PUCSP,** tomo IV. São Paulo: Pontifícia Universidade Católica de São Paulo, 2018.

MERCADOLIVRE. **Registro**. Disponível em : https://www.mercadolivre.com.br/hub/registration?from_landing=true&contextual=unified_normal&entity=no_apply. Acesso em 28 de nov. de 2023.

MERCOSUL. **Acordo de reconhecimento mútuo de assinaturas digitais no Mercosul**. 2019. Disponível em : https://www.mercosur.int/pt-br/acordo-de-reconhecimento-mutuo-de-assinaturas-digitais-no-mercosul/. Acesso em 20 de nov. de 2023.

META. **Termos de Serviço**. Disponível em : https://pt-br.facebook.com/legal/terms. Acesso em 28 de nov. de 2023.

MORIN, Edgar. **Introduction à la pensée complexe**. Paris: Éditions du Seuil, 2005.

NASCIMENTO, Anderson. **O que é phisching**. 2014. Disponível em : https://canaltech.com.br/seguranca/o-que-e-phishing/. Acesso em 02 de dez. de 2023.

NUBANK. **Cadastro nubank: como fazer pelo aplicativo**. Disponível em: https://blog.nubank.com.br/cadastro-nubank-como-fazer-pelo-aplicativo/. Acesso em 28 de nov. de 2023.

OCDE. **Emerging privacy enhancing technologies current regulatory and policy approaches**. 2023. Disponível em : https://www.oecd-ilibrary.org/docserver/bf121be4-en.pdf?expires=1701785800&id=id&accname=guest&checksum=384335830E61743FC3B7F3B94365D542. Acesso em 05 de dez. de 2023.

ONU. **Resolução da Assembleia Geral nº 51/162, de 16 de dezembro de 1996**. Disponível em : https://documents-dds-ny.un.org/doc/UNDOC/GEN/N97/763/57/PDF/N9776357.pdf?OpenElement. Acesso em 21 de nov. de 2023.

OUYANG, Liwei; ZHANG, Wenwen; WANG, Fei-Yue. **Intelligent contracts: Making smart contracts smart for blockchain intelligence.** 2022. Disponível em https://doi.org/10.1016/j.compeleceng.2022.108421. Acesso em 24 de nov. de 2023.

PEREIRA, Ana; CARVALHO, André; GIRON, Vinicius. **Cultura Organizacional em Compliance**. São Paulo (SP):Editora Revista dos Tribunais. 2021. Disponível em: https://www.jusbrasil.com.br/doutrina/cultura-organizacional-em-compliance/1294656306. Acesso em: 5 de Dez. de 2023.

PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil**. Vol III, 10ª ed. Rio de Janeiro: Forense, 2001.

PETRILLO, Antonella; FELICE, Fabio De; CIOFFI, Raffaele; ZOMPARELLI, Federico. **Fourth industrial revolution: current Practices, challenges, and opportunities**. 2018. Disponível em : https://www.researchgate.net/publication/323464589_Fourth_Industrial_Revolution_Current_Practices_Challenges_and_Opportunities. Acesso em 19 de nov. de 2023.

PIMENTEL, Alexandre Freire. **A internet, a lex algorítmica e a regulamentação das big techs**. 2023c. Disponível em : https://www.conjur.com.br/2023-jun-30/alexandre-pimentel-internet-lex-algoritmica-big-techs/. Acesso em 07 de dez. de 2023.

PIMENTEL, Alexandre Freire. **Cidadania digital e o estado algorítmico de direito**. 2023. Disponível em : https://www.conjur.com.br/2023-nov-21/cidadania-digital-e-o-estado-algoritmico-de-direito/. Acesso em 24 de nov. de 2023.

PIMENTEL, Alexandre Freire. **Tratado sobre as tics – direito e processo tecnológico.** Volume 3. Recife: Editora Publius, 2023a.

PIMENTEL, Alexandre Freire. **Tratado sobre as tics – direito e processo tecnológico**. Volume 4. Recife: Editora Publius, 2023b.

PIMENTEL, Alexandre Freire. **Tratado sobre as tics – direito e processo tecnológico**. Volume 2. Recife: Editora Publius, 2023d.

PINHEIRO, Patrícia; WEBER, Sandra; NETO, Antonio. **1. Transformação Digital da Sociedade** In: PINHEIRO, Patrícia; WEBER, Sandra; NETO, Antonio. Fundamentos dos Negócios e Contratos Digitais. São Paulo (SP):Editora Revista dos Tribunais. 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/fundamentos-dos-negocios-e-contratos-digitais/1481214684. Acesso em: 8 de Dez. de 2023.

PINHEIRO, Patrícia; WEBER, Sandra; NETO, Antonio. **6. A Evolução da Assinatura Eletrônica** In: PINHEIRO, Patrícia; WEBER, Sandra; NETO, Antonio. Fundamentos dos Negócios e Contratos Digitais. São Paulo (SP):Editora Revista dos Tribunais. 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/fundamentos-dos-negocios-e-contratos-digitais/1481214684. Acesso em: 3 de Dez. de 2023.

POLIDO, Fabrício Bertini Pasquot e SILVA, **Lucas Sávio Oliveira da. Contratos Internacionais Eletrônicos e o Direito Brasileiro: entre a insuficiência normativa doméstica e as soluções globais**. 2017. Disponível em: https://www.scielo.br/j/seq/a/sSGy3LVq7bYfSVjgMvd6tmM/#. Acesso em 21 de nov. de 2023.

PROCON-SP. **Guia de Comercio Eletrônico** SP. 2021. Disponível em https://www.procon.sp.gov.br/wp-content/uploads/2022/07/GuiadeComercioEletroniconovologEPDC2021ELEICOES2022.pdf. Acesso em 05 de dez. de 2023.

RADBRUCH, Gustav. **Five minutes of legal philosophy**. Tradução de Bonnie Litschewski paulos e Stanley L. Paulson. Oxford Journal of Legal Studies, Vol. 26, No. 1 (2006), pp. 13-15 doi: 10. 1093/ojls/gqi042. Disponível em : https://wystap.pl/wp-content/files/Radbruch_Extreme_Injustice.pdf. Acesso em 28 de nov. de 2023.

RAPPORT, Nigel; OVERING, Joanna. **Social and cultural anthropology. The key concepts.** London : Routledge, 2000.

REED, Thomas Vernon. **Digitized lives : culture, power, and social change in the internet era**. 2ª ed. New York : Routledge, 2019

REVOREDO, Tatiana. **Segurança cibernética de blockchains e protocolos de consenso**. MIT Thechnology Review. 2021. Disponível em : https://mittechreview.com.br/seguranca-cibernetica-de-blockchains-e-protocolos-de-consenso/. Acesso em 08 de dez. de 2023.

RIBEIRO, Gleisse. **OMC e as iniciativas para a regulamentação dos contratos via internet.** 2011. Disponível em : https://egov.ufsc.br/portal/sites/default/files/anexos/32687-40164-1-PB.pdf. Acesso em 21 de nov. de 2023.

RODRIGUES, Kauê. O que é UX/UI **Design? Um guia completo para iniciantes**. 2023. Disponível em https://blog.cubos.academy/ux-ui-design-guia-completo/. Acesso em 23 de nov. de 2023.

ROSENZWEIG, Stan. **How you can turn ordinary telemarketing into extraordinary income**. Oregon: Quality Books, 2000.

ROßNAGEL, A., PFITZMANN, A. **Der beweiswert von e-mail**. Neue Juristenwochenschrift, 2003. Disponível em : https://dud.inf.tu-dresden.de/literatur/RoPf_03.pdf. Acesso em 29 de nov. de 2023.

RUGGIERO, Roberto de. **Instituições de Direito Civil**. Atualizado por Paulo Robeerto Benasse. Tradução da 6ª edição italiana por Paolo Capitanio, 1ª edição, Volume 3. Campinas: Bookseller.

SARLET, Ingo Wolfgang. **Fundamentos constitucionais: o direito fundamental à proteção de dados**. Páginas 21-60. In: BIONI, Bruno Ricardo (coord.). Tratado de proteção de dados pessoais. Rio de Janeiro Forense, 2021.

SCHREIBER, Anderson et al. **Código civil comentado: doutrina e jurisprudência.** 3.ed. Rio de Janeiro: Forense, 2021.

SCHWAB, Dieter; LÖHNIG, Martin. **Einführung in das Zivilrecht**. 19. Ed. München: C.F. Müller, 2012.

SCOTT, Kevin. **O futuro da inteligência artificial: de amaça a recurso**. Rio de Janeiro: HarperCollins Brasil, 2023.

SERASA. **Primeiro acordo internacional assinado com certificação digital**. 2020. Disponível em: https://serasa.certificadodigital.com.br/blog/mercado/primeiro-acordo-internacional-assinado-com-certificacao-digital/. Acesso em 20 de nov. de 2023.

SILVA, Caroline costa da. **Forma do negócio jurídico**. 2015. Disponível em : https://www.jusbrasil.com.br/artigos/forma-do-negocio-juridico/326326746. Acesso em 27 de nov. de 2023.

SINGH, Simon. **The code book. How to make it, break it, Hack it, crack it**. Nova Iorque: Delacorte Press, 2001.

SNOWDEN, Edward. **Eterna vigilância**. Tradução Sandra Martha Dolinsky. São Paulo: Planeta do Brasil, 2019.

STOLZE, Pablo; PAMPLONA FILHO, Rodolfo. **Manual de direito civil.** Volume único. 4. ed. São Paulo : Saraiva Educação, 2020. Edição digital EPUB.

SULEYMAN, Mustafa; BHASKAR, Michael. **A próxima onda: inteligência artificial, poder e o maior dilema do século XXI**. Tradução Alessandra Bonrruquer. Rio de Janeiro: Editora Record, 2023.

TANG, Zheng Sophia. **Electronic consumer contracts in the conflict of laws**. 2ª ed. Portland : Hart Publishing, 2015.

TARTUCE, Flávio. **Direito civil: lei de introdução e parte geral. Volume 1**. 15. ed. Rio de Janeiro: Forense, 2019.

TEIXEIRA, Pedro S. **Golpe que leva cliente a inserir cartão na máquina mira shippings e postos de gasolina.** Artigo da Folha de São Paulo do dia 27 de nov. de 2023. Disponível em : https://www1.folha.uol.com.br/tec/2023/11/golpe-que-leva-cliente-a-inserir-cartao-na-maquina-mira-shoppings-e-postos-de-gasolina.shtml. Acesso em 02 de dez. de 2023.

TEIXEIRA, Sergio Torres; COSTA, Pâmella Giuseppina Parisi; ORENGO, Beatriz Souto. **Novas tecnologias e direito: uma análise do acesso à justiça na era digital**. Disponível em : https://www.e-publicacoes.uerj.br/redp/article/view/63093/42388. Acesso em 07 de dez. de 2023.

TERRÉ, François ; SIMLER, Philippe ; LEQUETTE, Yves ; CHÉNEDÉ, François. **Droit civil. Les obrigations**. 12ª ed. Paris : Dalloz, 2019.

THEODORO JÚNIOR, Humberto. **Comentários ao novo código civil**. Volume 3. Rio de Janeiro: Forense, 2003.

TURNER, Dawn M. **Understanding EIDAS**. 2016. Disponível em : https://www.cryptomathic.com/news-events/blog/understanding-eidas. Acesso em 20 de nov. de 2023.

UNIÃO EUROPÉIA. **Regulação nº 910/2014 do Parlamento e do Conselho Europeu**. Disponível em : https://web.archive.org/web/20190726213601/https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN#d1e791-73-1. Acesso em 19 de nov. de 2023.

UNIFORM LAW COMMISSION. **Electronic Transaction Act**. 1999. Disponível em : https://www.uniformlaws.org/committees/community-home?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034. Acesso em 20 de nov. de 2023.

VALENTE, Leonardo. **Documento eletrônico: aceitação jurídica nas relações de comércio eletrônico**. 2012. Disponível em : https://www.gov.br/iti/pt-br/assuntos/noticias/iti-na-midia/documento-eletronico-aceitacao-juridica-nas-relacoes-de-comercio-eletronico. Acesso em 21 de nov. de 2023.

VENOSA, Sílvio de Salvo. **Código civil interpretado**. 3ª ed. São Paulo: Editora Atlas, 2013.

WATSON, Alan. **The making oft he civil law**. Cambridge: Harvard University Press, 1981.


ESMAPE
Escola Judicial de Pernambuco