ASSINATURA ELETRÔNICA EM TÍTULOS EXECUTIVOS EXTRAJUDICIAIS: GARANTINDO SEGURANÇA JURÍDICA NA ERA DIGITAL

ELETRONIC SIGNATURE ON EXTRAJUDICIAL EXECUTIVO TITLES: GUARANTEING LEGAL SECURITY IN THE DIGITAL AGE

Ademir de Oliveira Costa Júnior[1]
Clarissa Lunardi [2]
Eveline Denardi[3]

Resumo – Este artigo examina a utilização da assinatura eletrônica na constituição de títulos executivos extrajudiciais, com foco nos requisitos estabelecidos pelo art. 784 do Código de Processo Civil de 2015, em especial, em seu § 4º. A pesquisa realiza um levantamento da doutrina, legislação e jurisprudência sobre o tema, analisando os diferentes tipos de assinatura eletrônica e sua validade jurídica. Embora o ordenamento jurídico brasileiro reconheça a validade de diferentes tipos de assinatura eletrônica, o estudo argumenta que a assinatura digital com certificado digital emitido por autoridade certificadora credenciada na Infraestrutura de Chaves Públicas Brasileira apresenta maior segurança jurídica para a constituição de títulos executivos extrajudiciais. A pesquisa conclui que a assinatura digital com certificado ICP-Brasil, por suas características de autenticidade, integridade e não repúdio, garante maior confiabilidade e segurança jurídica na formação e posterior execução de títulos executivos extrajudiciais, minimizando riscos de fraude e questionamentos em juízo.

Palavras-chave: Assinatura eletrônica; título executivo extrajudicial; Código de Processo Civil; Art. 784, CPC; certificado digital; ICP-Brasil; segurança jurídica; validade jurídica.

[1] Possui graduação em Direito pelo Centro Universitário de João Pessoa (2003). É especialista em Direito Processual Civil pela Universidade Mackenzie (2005), Especialista em Direito Empresarial pela Unisinos (2006), Mestre em Direitos Fundamentais pelo Centro Universitário Fieo (2008) e Doutorando em Direito e Ciências Sociais pela Universidad Nacional de Rosario. Atualmente Professor da Escola Paulista de Direito (EPD) e da Universidade Paulista (UNIP). Membro da Associação dos Advogados de São Paulo (AASP). Sócio fundador do escritório Ademir Costa Junior Sociedade de Advogados. Autor de obras e artigos jurídicos. Email: ademir.junior@epd.edu.br.

[2] Graduanda em Direito na Escola Paulista de Direito. Arquivista pela Universidade de Brasília (UnB). Analista Judiciário – Especialista – Arquivista do Tribunal Regional Eleitoral de São Paulo (TRE-SP). E-mail: clarissa.lunardi@tre-sp.jus.br.

[3] Docente na Escola Paulista de Direito (EPD), no Programa de Mestrado "Soluções Extrajudiciais de Conflitos Empresariais" – disciplina Metodologia de Pesquisa e Ensino do Direito; Docente na Fundação Instituto de Administração (FIA), nos Cursos de MBA e Pós-Graduação *Lato Sensu* em Gestão de Fraudes e Compliance – disciplina Metodologia de Desenvolvimento de Projetos; Docente na pós-graduação *lato sensu* do Instituto Presbiteriano Mackenzie; Pesquisadora do CNPq pelo Núcleo Dignidade Humana e Garantias Fundamentais na Democracia, da Faculdade de Direito da PUC-SP; Consultora Acadêmica para a elaboração de textos científicos e revisora técnica-profissional neste segmento; Doutora (2012) e Mestre (2008) em Direito Constitucional pela Pontifícia Universidade Católica de São Paulo (PUC-SP); Graduada em Direito (2004) e em Jornalismo (1998), ambos pela PUC-SP; Foi Diretora da Divisão de Comunicação Institucional da PUC-SP e Coordenadora do Editorial Jurídico da Editora Saraiva. Editora Sênior em Direito. E-mail: evelinedenardi@uol.com.br.

Abstract – This article examines the use of electronic signatures in the constitution of extrajudicial enforcement orders, focusing on the requirements established by article 784 of the Brazilian Code of Civil Procedure, especially its § 4º. The research conducts a survey of doctrine, legislation, and jurisprudence on the subject, analyzing the different types of electronic signatures and their legal validity. Although the Brazilian legal system recognizes the validity of different types of electronic signatures, the study argues that the digital signature with a digital certificate issued by a certification authority accredited by the Brazilian Public Key Infrastructure offers greater legal certainty for the constitution of extrajudicial enforcement orders. The research concludes that the digital signature with an ICP-Brasil certificate, due to its characteristics of authenticity, integrity, and non-repudiation, guarantees greater reliability and legal certainty in the formation and subsequent execution of extrajudicial enforcement orders, minimizing risks of fraud and legal challenges.

Keywords: Electronic signature; digital signature; extrajudicial enforcement order; Brazilian Code of Civil Procedure; ICP-Brasil.

1 Introdução

O presente artigo procura analisar os requisitos da assinatura eletrônica para a constituição de título executivo extrajudicial, e compreender os parâmetros para a sua constituição, com base no art. 784, § 4º, do Código de Processo Civil, o que é crucial para garantir a segurança e a validade jurídica de documentos dessa natureza.

Para alcançar esse objetivo, o estudo analisa os dispositivos legais que regulamentam o tema, a exemplo do CPC/2015 e da Medida Provisória n. 2.200-2/2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira. Adicionalmente, explora-se a doutrina pertinente, abordando os requisitos técnicos e jurídicos da assinatura eletrônica, e a jurisprudência correlata, a fim de proporcionar uma análise abrangente da validade e da eficácia desse instituto no âmbito dos títulos executivos extrajudiciais.

Trata-se de tema relevante no direito brasileiro contemporâneo, à medida que os avanços tecnológicos têm promovido significativas mudanças no campo do direito, notadamente no que diz respeito às provas judiciais.

O uso de meios digitais para a celebração de negócios jurídicos e constituição de obrigações tem sido cada vez mais recorrente na sociedade contemporânea. Nesse contexto, a Lei n. 11.419/2006, que dispõe sobre a informatização do processo judicial, reconhece a validade de documentos e atos

processuais realizados em meio eletrônico, atribuindo-lhes a mesma eficácia dos realizados em suporte físico. Assim, a discussão do valor jurídico da assinatura eletrônica torna-se essencial para conferir segurança jurídica aos atos praticados por meio eletrônico.

2 Título Executivo e suas espécies

A legislação brasileira considera o título executivo um instrumento que comprova a existência de uma obrigação líquida, certa e exigível (Sena, 2018), conferindo ao seu credor o direito de exigir o cumprimento forçado dessa obrigação, por meio de um processo de execução (Cunha *et al*., 2021).

O CPC/2015 lista duas espécies de títulos executivos: judicial (art. 515) e executivos extrajudiciais (art. 784).

Entre os títulos executivos judiciais estão as sentenças proferidas no processo de conhecimento, que reconheçam a existência de obrigação de pagar quantia, de fazer, de não fazer ou de entregar coisa. Essas sentenças transitadas em julgado, ou seja, após o esgotamento de todas as instâncias recursais, conferem ao credor o direito de exigir o cumprimento forçado dessa obrigação por meio de um processo de execução (Sena, 2018), (Valadares, 2022).

Já o título executivo extrajudicial, a exemplo dos cheques, das notas promissórias e dos contratos. Ele possui força executiva ao preencher os critérios que garantam sua validade, eficácia e aptidão, permitindo que o credor execute diretamente a obrigação, sem a necessidade de obter uma sentença judicial condenatória prévia. Essa característica confere maior agilidade e efetividade ao processo de cobrança, beneficiando tanto o credor quanto o devedor.

2.1 Requisitos do Título Executivo Extrajudicial

Conforme estabelece o CPC/2015, um título executivo extrajudicial deve preencher certos critérios que garantam sua validade, eficácia e aptidão para iniciar um processo de execução, dispensando a necessidade de decisão judicial prévia. Entre esses requisitos, destacam-se a liquidez, a certeza e a exigibilidade, aspectos essenciais para o título possuir força executiva.

A liquidez exige que o título contenha valores certos ou facilmente determináveis, assegurando que a obrigação seja quantificável e permitindo que a

execução se realize diretamente. Já a certeza requer que o título prove, de modo inequívoco, a existência de uma obrigação, especificando com clareza as partes envolvidas, ou seja, quem é o devedor, quem é o credor e quais são os termos do acordo. Por fim, a exigibilidade impõe que o título represente uma obrigação passível de cobrança imediata, sem a presença de condições futuras ou incertezas (art. 783 do CPC/2015).

O art. 784 do CPC/2015 lista diversos documentos que se qualificam como títulos executivos extrajudiciais, como instrumentos particulares com assinatura de duas testemunhas, certidões de dívida ativa de entidades públicas, contratos de garantia real como hipoteca, penhor e anticrese, escrituras públicas e instrumentos de transação homologados por advogados e todos os demais títulos aos quais, por disposição expressa, a lei atribuir força executiva.

Esses documentos, por sua autenticidade e características formais, oferecem segurança jurídica e tornam viável a execução sem decisão judicial anterior.

Didier Jr. (2019) observa que os títulos executivos extrajudiciais são fundamentais para a celeridade da execução, dispensando a fase de conhecimento processual quando cumprem os requisitos de certeza, liquidez e exigibilidade. Enfatiza que esses títulos promovem uma “execução imediata”, alinhada ao princípio da eficiência processual.

Em consonância com esse entendimento, o Superior Tribunal de Justiça (STJ) tem reiterado, em decisões recentes, a relevância dos requisitos formais dos títulos executivos extrajudiciais, destacando que a falta de qualquer um deles torna o título inexigível, portanto, impede a execução.

Além desses aspectos, Marinoni e Arenhart (2021) destacam a importância dos requisitos formais que asseguram a validade do título executivo extrajudicial. Argumentam que, além dos critérios de certeza, liquidez e exigibilidade, o título deve respeitar as exigências formais definidas pela legislação, garantindo a regularidade e a aptidão para execução.

Esses requisitos – certeza, liquidez e exigibilidade – somados às condições formais, estabelecem a base para a execução extrajudicial. Eles permitem que o processo seja conduzido com eficiência, possibilitando ao credor alcançar o cumprimento forçado da obrigação de forma célere e efetiva.

De acordo com o art. 784, § 4º, do CPC/2015, “o documento particular assinado eletronicamente e realizado com certificação da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil é considerado título executivo extrajudicial e tem a mesma eficácia probatória dos documentos mencionados nos incisos deste artigo”. Assim, esses documentos possuem força executiva, garantindo segurança jurídica às partes envolvidas.

3 Assinatura Eletrônica e Autenticação Digital

No cenário jurídico atual, a assinatura eletrônica tem desempenhado um papel fundamental na validação de documentos digitais, proporcionando celeridade e segurança às transações. Essa relevância se intensifica com a crescente importância da tecnologia da informação no nosso cotidiano, demandando uma análise criteriosa dos requisitos de validade da assinatura digital, especialmente no âmbito jurídico.

Segundo Menke (2005, p. 42), sob a denominação “assinatura eletrônica”, incluem-se vários métodos de comprovação de autoria empregados no meio virtual. Já a “assinatura digital” refere-se exclusivamente ao procedimento de autenticação baseado na criptografia assimétrica – aquela baseada em um par de duas chaves: uma pública e outra privada – que constitui o fundamento da certificação digital.

No contexto brasileiro, os avanços tecnológicos têm promovido significativas mudanças no campo do direito, especialmente no que tange às provas judiciais. A Lei n. 11.419/2006, que trata da informatização do processo judicial, e a Lei n. 14.063/2020, que regulamenta a assinatura eletrônica, são exemplos emblemáticos dessa transformação.

A discussão sobre a segurança jurídica dos atos praticados por meio digital se torna cada vez mais relevante, considerando o uso crescente desses meios para a realização de negócios jurídicos.

A assinatura eletrônica, no contexto jurídico brasileiro, constitui um termo abrangente que engloba diversos tipos de autenticação digital. Conforme rege a Lei n. 14.063/2020, art. 4º, § 2º: “Considera-se assinatura eletrônica qualquer meio de comprovação de autoria e integridade de documentos em formato eletrônico”.

De acordo com o art. 4º, § 2º, da Lei n. 14.063/2020, “considera-se assinatura eletrônica qualquer meio de comprovação de autoria e integridade de

documentos em formato eletrônico". Três são as principais categorias de classificação: simples, avançada e qualificada, cada uma com níveis distintos de segurança e de confiabilidade.

A assinatura eletrônica simples é a categoria mais básica, aquela que permite identificar o signatário e associar dados de assinatura a documentos eletrônicos, embora com uma segurança reduzida. Por isso, é recomendada para interações de baixo risco, como com entes públicos ou documentos privados que não requerem proteção de sigilo específico (Silva, 2022).

Já a assinatura eletrônica avançada apresenta um nível mais elevado de segurança quando comparada com a assinatura simples, pois contempla mecanismos que garantem a integridade do documento, utiliza certificados não emitidos pela ICP-Brasil ou outro meio reconhecido entre as partes para garantir a autoria e evitar alterações. É comumente utilizada em registros comerciais e transações com entidades públicas, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento (Silva, 2022). Esse é o caso da assinatura eletrônica disponibilizada na plataforma gov.br, regulamentada pelo Decreto n. 10.543/2020.

A assinatura eletrônica avançada seria o equivalente à firma reconhecida por semelhança, ao passo que a assinatura eletrônica qualificada seria a firma reconhecida por autenticidade – ou seja, ambas são válidas, apenas se diferenciando no aspecto da força probatória e no grau de dificuldade na impugnação técnica de seus aspectos de integridade e autenticidade.

Por último, menciona-se a assinatura eletrônica qualificada como forma mais segura, gerada com certificado digital emitido pela ICP-Brasil[4], exigida para atos de maior segurança, como documentos assinados por autoridades ou operações de transferência de imóveis.

A assinatura qualificada tem ampla aceitação nas interações com o setor público e em transações de alto nível de criticidade (Silva, 2022).

[4] Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) **é** uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. No Brasil, o Instituto Nacional de Tecnologia e Informação (ITI) é a Autoridade Certificadora Raiz (AC-Raiz), além de supervisionar e fazer auditoria dos processos.

Essas classificações formam uma hierarquia de segurança e utilidade específica, a depender do nível de proteção demandado para o documento ou transação (Brasil, 2020; Silva, 2022).

Certificação digital é o processo de autenticação e de verificação de identidade *online* por meio de um certificado digital, emitido por uma autoridade certificadora dentro da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

A criação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), por meio da MP n. 2.200-2/2001, trouxe regulamentação para o uso de certificados digitais, validando sua emissão por autoridades certificadoras credenciadas. A ICP-Brasil assegura a autenticidade, a integridade e a validade jurídica dos documentos eletrônicos, conferindo à assinatura digital o mesmo valor jurídico das assinaturas manuscritas (Brasil, 2001).

Conforme rege o art. 10 da MP 2.200-2/2001, os documentos eletrônicos assinados com certificados digitais ICP-Brasil possuem presunção de veracidade e autenticidade e são reconhecidos juridicamente em todo o território nacional. A validação das assinaturas digitais no Brasil é realizada por entidades certificadoras credenciadas na estrutura hierárquica da ICP-Brasil. Já a assinatura cadastrada é validada pelo próprio órgão que gerencia o sistema de processo eletrônico.

Por meio do uso de *softwares* específicos, a assinatura digital – realizada por meio da chave privada do titular do certificado – pode ser validada por intermédio de sua chave pública, fornecida pela AC que emitiu o respectivo certificado. A AC é um terceiro confiável e legalmente autorizado a gerenciar certificados digitais para validação futura da assinatura de documentos eletrônicos.

Por outro lado, a assinatura cadastrada só pode ser validada pelo próprio órgão que gerencia o sistema de processo eletrônico. Mediante a posse da senha utilizada pelo usuário, o órgão pode conferir determinada assinatura e disponibilizar o resultado dessa verificação em um ambiente específico.

3.1 Garantia de autenticidade e de integridade

Com o rápido avanço das tecnologias, a sociedade contemporânea tem experimentado transformações contínuas que impactam diretamente diversas áreas, incluindo como o conhecimento é produzido, armazenado e compartilhado.

Nesse contexto de busca incessante por inovações, a produção de documentos, anteriormente restrita ao meio analógico, passou a se expandir significativamente para o ambiente digital, consolidando-se como uma prática cada vez mais comum e essencial para atender às demandas atuais de eficiência, acessibilidade e sustentabilidade.

O Processo Judicial Eletrônico (PJe) surge como uma importante iniciativa do Poder Judiciário brasileiro para atender às demandas de eficiência, transparência e acesso facilitado aos serviços judiciais. Segundo a Resolução CNJ n. 185/2013, o PJe foi projetado para padronizar processos judiciais digitais, promovendo maior integração entre os tribunais e oferecendo mais segurança e agilidade aos usuários.

O CNJ foi instituído para controlar a atuação administrativa e financeira do Poder Judiciário e, desde então, tem liderado iniciativas voltadas à transformação digital que busca garantir uma tramitação mais célere e segura dos processos judiciais (CNJ, 2023).

A Resolução CNJ n. 185/2013 foi um marco ao estabelecer diretrizes para a implementação e o uso do PJe em todo o Brasil. Esse sistema foi projetado para padronizar os processos judiciais digitais, permitindo maior integração entre os tribunais e oferecendo maior segurança aos usuários.

Segundo o próprio CNJ, o PJe visa reduzir custos operacionais, facilitar o acesso à Justiça e promover a agilidade na tramitação dos processos. Ele é sustentado por pilares como integridade, autenticidade e eficiência, o que torna o sistema uma referência internacional em digitalização judicial.

Segundo Gonçalves (2013), o PJe foi projetado para atender às necessidades de um Poder Judiciário mais dinâmico e conectado às demandas sociais contemporâneas, consolidando-se como um modelo para outros países em termos de inovação tecnológica aplicada à justiça.

A modernização do Poder Judiciário brasileiro por meio da adoção de Processos Judiciais Eletrônicos (PJe) é uma resposta à crescente demanda por eficiência, celeridade e acessibilidade nos processos judiciais.

Esse movimento teve um marco importante com a promulgação da Lei n. 11.419/2006, que regulamenta a informatização do processo judicial e dispõe sobre a digitalização de autos e tramitação de processos eletrônicos.

A legislação determinou que documentos digitalizados e assinaturas eletrônicas qualificadas possuam o mesmo valor jurídico que documentos físicos assinados manualmente, desde que respeitadas as normas de integridade e autenticidade (Brasil, 2006).

Conforme destaca Didier Jr. (2021), a informatização traz benefícios claros, como a diminuição do uso de papel, a economia de recursos, e o acesso mais amplo ao Poder Judiciário, facilitando o acompanhamento de processos por advogados, partes e cidadãos. Além disso, o PJe permite uma integração maior entre os tribunais, reduzindo os prazos de tramitação processual e aumentando a transparência.

A Constituição Federal de 1988, em seu art. 5º, LXXVIII, ao assegurar a todos o direito à “razoável duração do processo”, foi interpretada por Didier Jr. e Marinoni (2020) como um incentivo indireto à digitalização, visando o uso de tecnologias para reduzir a morosidade processual.

As críticas, no entanto, são registradas por Binenbojm (2022), que ressalta os desafios enfrentados quanto à segurança da informação e a adequação de infraestrutura, especialmente nos locais com menor acesso à tecnologia.

A assinatura eletrônica, como componente essencial do Processo Judicial Eletrônico (PJe), contribui decisivamente para a integridade e a autenticidade dos documentos digitais, garantindo que as transações e comunicações sejam seguras e confiáveis.

A Lei n. 14.063/2020 define as assinaturas eletrônicas no Brasil em três tipos: simples, avançada e qualificada, cada qual com um nível crescente de segurança e adequação a diferentes tipos de documentos e transações, especialmente no contexto judicial.

A assinatura qualificada, considerada o padrão mais alto de segurança, é realizada por meio de um certificado digital emitido pela ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira), assegurando a integridade do documento e autenticidade da assinatura (Brasil, 2020). A autenticidade e a integridade de assinaturas eletrônicas são fundamentais no PJe, pois permitem que as partes, advogados e o próprio Poder Judiciário confiem na identidade do signatário e na inviolabilidade do documento assinado.

Segundo Didier Jr. (2021), esses atributos mitigam fraudes e adulterações, viabilizando a substituição de documentos físicos por digitais de forma segura, além

de reduzir o tempo e os custos processuais. O art. 10 da MP n. 2.200-2/2001 e a Resolução n. 185/2013 do CNJ reforçam a importância dessas assinaturas ao exigir que o PJe adote tecnologias de autenticação robustas e padronizadas, que respeitem os princípios de integridade e autenticidade.

A integridade e a autenticidade de documentos eletrônicos são princípios fundamentais para assegurar que esses documentos sejam confiáveis e válidos no meio jurídico. Integridade refere-se à garantia de que o conteúdo do documento eletrônico não foi alterado após sua criação e assinatura. É essencial para assegurar que o documento permaneça idêntico ao original.

Segundo Silva (2022), para preservar essa integridade, são utilizados algoritmos de *hash*, que geram uma espécie de “impressão digital” exclusiva para cada documento. Qualquer modificação no documento altera o *hash*, sinalizando o que houve, portanto, comprometendo a integridade. Isso é um ponto essencial em processos judiciais e em transações comerciais eletrônicas, nas quais é necessário garantir que o conteúdo permaneça imutável desde a sua criação.

Autenticidade diz respeito à verificação da identidade de quem criou ou assinou o documento eletrônico. No Brasil, a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) tem um papel importante na autenticação de assinaturas digitais qualificadas, conferindo-lhes presunção de autenticidade (Medida Provisória n. 2.200-2/2001).

A integridade é garantida, entre outros fatores, pelo uso de tecnologias de *hash*, que algoritmos matemáticos que geram uma “impressão digital” única para cada documento, identificando qualquer alteração no conteúdo após a assinatura. Essa singularidade é garantida com o uso de criptografia. A função criptográfica *hash* SHA-256 é um dos padrões mais utilizados na área de segurança da informação por permitir detecção de adulteração mais eficiente, a exemplo do “efeito avalanche”.

A autenticidade, por outro lado, é assegurada pelo uso de certificados digitais da ICP-Brasil, que estabelecem um vínculo inequívoco entre o signatário e o documento, essencial para a validade jurídica dos atos processuais digitais. Esses mecanismos não só facilitam a transição para processos digitais como asseguram que os documentos eletrônicos possam ser utilizados com a mesma confiança em relação aos documentos físicos, especialmente em contextos jurídicos e comerciais.

Hipótese em que as partes – no legítimo exercício de sua autonomia privada – elegeram meio diverso de comprovação da autoria e integridade de documentos em forma eletrônica, com uso de certificado não emitido pela ICP-Brasil. O Tribunal de Origem considerou a assinatura eletrônica em modalidade avançada insuficiente para evitar abuso ou fraude apesar de constar múltiplos fatores de autenticação, inseridos no relatório de *logs* gerado na emissão dos documentos e das assinaturas eletrônicas.

3.2 Desafios e vulnerabilidades na garantia da integridade e da autenticidade

Embora a assinatura eletrônica represente um avanço significativo na segurança e confiabilidade de documentos digitais, é crucial reconhecer que nenhum sistema é totalmente imune a desafios e vulnerabilidades.

A complexidade inerente aos sistemas criptográficos, a constante evolução das ameaças cibernéticas e a dependência de fatores humanos exigem uma análise crítica dos riscos potenciais e das medidas de mitigação.

Um dos principais desafios reside na gestão segura das chaves criptográficas. A confidencialidade da chave privada é essencial para garantir a autenticidade e o não repúdio da assinatura eletrônica. Caso essa chave seja comprometida, seja por falhas na armazenagem, compartilhamento indevido ou ataques de *phishing*, a integridade do sistema fica comprometida, abrindo espaço para falsificações e alterações indevidas nos documentos.

A arquitetura de certificados inteligentes para aplicações Web3, por exemplo, busca mitigar esses riscos, concentrando-se na proteção da chave privada e na gestão segura de identidades no contexto das finanças descentralizadas.

Outro ponto crítico diz respeito à segurança dos dispositivos utilizados para assinar e verificar os documentos eletrônicos. Computadores, *smartphones* e outros dispositivos conectados à internet estão suscetíveis a malwares, vírus e ataques de *hackers*. A infecção por códigos maliciosos pode comprometer a integridade do processo de assinatura, permitindo que terceiros capturem chaves privadas, alterem o conteúdo dos documentos ou insiram assinaturas falsas sem o conhecimento do usuário. (O’Neill, 2016)

A evolução constante das ameaças cibernéticas representa um desafio adicional. Ataques de engenharia social, exploração de vulnerabilidades em

softwares e técnicas de criptoanálise estão em constante desenvolvimento, exigindo atualizações frequentes nos sistemas de segurança e conscientização pelos usuários.

A implementação de múltiplos fatores de autenticação, *firewalls* robustos e sistemas de detecção e prevenção de intrusões são medidas essenciais para fortalecer a segurança e minimizar os riscos.

Fundamental, portanto, destacar que a segurança da informação não se limita a aspectos técnicos. O fator humano desempenha um papel crucial na prevenção de falhas e ataques. A falta de conscientização sobre os riscos cibernéticos, o descuido com senhas, a facilidade em clicar em *links* suspeitos e a falta de atualização dos sistemas operacionais e aplicativos são portas de entrada para criminosos virtuais. Investir em treinamento e campanhas de conscientização para os usuários é tão importante quanto implementar soluções tecnológicas avançadas.

A intenção do legislador foi criar níveis diferentes de força probatória das assinaturas eletrônicas (em suas modalidades simples, avançada ou qualificada), conforme o método tecnológico de autenticação utilizado pelas partes, e – ao mesmo tempo – conferir validade jurídica a qualquer das modalidades, considerando a autonomia privada e a liberdade das formas de declaração de vontades entre os particulares.

O reconhecimento da validade jurídica e da força probante dos documentos e das assinaturas emitidos em meio eletrônico caminha em sintonia com o uso de ferramentas tecnológicas que permitem inferir (ou auditar) de forma confiável a autoria e a autenticidade da firma ou do documento.

Se o documento eletrônico que materializa o ato processual, por qualquer razão, for adulterado, ou seja, ainda que um único caractere seja mudado, suprimido ou acrescentado, a assinatura digital se perde[5]. Nesse sentido, a assinatura digital garante a integridade de conteúdo da peça processual. Além disso, como a chave privada está armazenada exclusivamente em dispositivo criptográfico de propriedade do titular do certificado e só este conhece o código PIN para usar a chave e assinar o documento, a autenticidade está garantida.

[5] Atualmente, os programas de criptografia são formulados de modo a cifrar um documento eletrônico e marcá-lo com uma assinatura digital, de modo que, qualquer alteração no documento, a chave pública não mais o abrirá, indicando a falsificação (RAMOS, 2011).

Por outro lado, na assinatura com *login* e senha, a chave precisa ser compartilhada com um terceiro ou armazenada em um servidor de arquivos para viabilizar a conferência posterior da assinatura, ou seja, essa chave não fica sob o exclusivo domínio do subscritor do documento.

O controle de autenticidade, isto é, a garantia de que a pessoa que preencheu ou assinou o documento é realmente a mesma, depende dos métodos de autenticação utilizados no momento da assinatura, incluindo o número e a natureza dos fatores de autenticação (por exemplo, “login”, senha, códigos enviados por mensagens eletrônicas instantâneas ou gerados por aplicativos e leitura biométrica facial).

Se o documento eletrônico for alterado, será possível detectar a adulteração, portanto, a integridade está garantida. Já a autenticidade fica comprometida em função do potencial conhecimento da chave por terceiros, o que impede se atribua inequivocamente a autoria do documento à pessoa que supostamente o assinou.

A busca por soluções mais robustas e resilientes é um processo contínuo. A criptografia quântica, a computação em nuvem segura e o uso de *blockchain* para registro e verificação de assinaturas eletrônicas são exemplos de tecnologias promissoras que podem contribuir para elevar o nível de segurança e confiabilidade dos documentos eletrônicos no futuro.

4 Doutrina e jurisprudência

A doutrina jurídica também enxerga a assinatura eletrônica como um instrumento essencial para o avanço do direito digital. Segundo Didier Jr. (2020), a assinatura eletrônica não só moderniza o sistema jurídico como promove o princípio da eficiência processual. Observa que, o uso de assinaturas digitais certificadas elimina a necessidade de reconhecimento de firma e reduz o risco de fraudes documentais, favorecendo a celeridade e a segurança das relações jurídicas.

Marinoni e Arenhart (2021) complementam essa visão apontando que a assinatura eletrônica permite maior acessibilidade ao sistema de justiça, uma vez que facilita a tramitação de documentos a distância e desburocratiza os processos.

Barbagalo (2021), ao destacar o papel revolucionário das assinaturas digitais no contexto jurídico atual, observa que instrumentos garantem autenticidade e segurança em documentos eletrônicos, fatores indispensáveis para o avanço das relações contratuais em meio digital. Enfatiza como as assinaturas eletrônicas se

enquadram no contexto de adaptação do direito às novas tecnologias, conferindo aos negócios jurídicos maior eficiência e modernidade, sem prescindir da segurança jurídica necessária à estabilidade das relações legais. Além disso, a obra aborda os desafios regulatórios e tecnológicos impostos pela incorporação desses instrumentos, apresentando soluções práticas para sua implementação no cotidiano jurídico.

Damin (2020), por sua vez, explora as bases legais e operacionais da assinatura digital como elemento central do Direito Digital no Brasil. A autora argumenta que a adoção desse mecanismo simplifica processos judiciais e contratuais, proporcionando agilidade e sustentabilidade, especialmente ao reduzir a dependência de documentos físicos. Além disso, Damin contextualiza o papel da Medida Provisória n. 2.200-2/2001 e da Lei n. 14.063/2020 como marcos legais que sustentam a validade jurídica e a segurança dos documentos eletrônicos, destacando como essas ferramentas têm contribuído para transformar a prática jurídica e promover a confiança no ambiente digital.

Scavone Júnior (2022) aborda de forma abrangente o impacto das tecnologias digitais no campo jurídico, com destaque para as assinaturas eletrônicas. O autor sublinha que a principal contribuição dessas assinaturas está na sua capacidade de conferir autenticidade e integridade aos documentos eletrônicos, elementos essenciais para a confiança nas transações realizadas no meio digital. Scavone analisa ainda como a certificação digital fortalece a segurança dos contratos eletrônicos, fomentando a evolução das práticas contratuais e oferecendo aos juristas ferramentas modernas para lidar com litígios e negociações no ambiente digital.

No mesmo sentido, Carvalho (2023) apresenta uma análise técnica e jurídica sobre a implementação e os benefícios das assinaturas eletrônicas no Brasil ao defender que esses instrumentos são cruciais para estabelecer confiança nas transações eletrônicas, ao garantir que tanto a autoria quanto a integridade dos documentos digitais sejam verificáveis.

O autor explora, ainda, os diferentes níveis de certificação digital (simples, avançada e qualificada) e seus impactos no cenário jurídico, argumentando que a adoção dessas ferramentas é um caminho sem volta para a modernização do direito e a promoção da eficiência processual.

No julgamento do Recurso Especial (REsp) n. 1.495.920/MG, relatado pelo Ministro Luis Felipe Salomão, o Superior Tribunal de Justiça (STJ) analisou a validade jurídica de contratos de empréstimo firmados em meio eletrônico, especificamente quanto à possibilidade de serem considerados títulos executivos extrajudiciais. A decisão destacou que, embora os contratos assinados digitalmente por meio da infraestrutura de chaves públicas brasileiras (ICP-Brasil) possuam elevados padrões de segurança e autenticidade, sua força executiva está vinculada ao cumprimento dos requisitos formais previstos na legislação. Nesse sentido, o STJ reafirmou o princípio da tipicidade dos títulos executivos, conforme disposto no CPC/2015, estabelecendo que somente os documentos que atendem aos critérios expressamente definidos pela lei podem ser reconhecidos como tal.

O tribunal concluiu que, embora o meio digital ofereça confiabilidade para a celebração de contratos, sua eficácia executiva depende do cumprimento de exigências como a assinatura e a presença de testemunhas, quando aplicável. Assim, reforçou-se a necessidade de observância rigorosa aos requisitos formais para que um documento eletrônico possa ser considerado título executivo extrajudicial, conforme rege o art. 784 do CPC/2015 (STJ, REsp 1.495.920/MG, 2017).

O REsp 2.150.278/PR, de relatoria da Min. Nancy Andrighi, em setembro de 2024, trata da validade da assinatura eletrônica e da autenticidade de documentos eletrônicos em uma ação de execução de título extrajudicial.

A decisão aborda a possibilidade de as partes optarem por um meio de autenticação eletrônico diferente da certificação emitida pela Infraestrutura de Chaves Públicas Brasileira (ICPBrasil) para a validação dos documentos eletrônicos em contextos pré-processuais. O tribunal reafirma que a lei não exige exclusividade da ICP-Brasil, desde que os métodos de autenticação e de integridade dos documentos sejam confiáveis.

A decisão também destaca que a assinatura eletrônica avançada, em que múltiplos fatores de autenticação são utilizados, pode ser válida, equiparando-a a uma firma reconhecida por semelhança. Já a assinatura digital qualificada, realizada com certificado emitido pela ICP-Brasil, é equiparada à firma reconhecida por autenticidade.

A Ministra enfatizou que a recusa à validade de um título de crédito eletrônico apenas por não utilizar a certificação ICP-Brasil configuraria um formalismo excessivo, e a Lei n. 14.620/2023, ao alterar o art. 784 do CPC/2015, reconhece a possibilidade de utilizar qualquer modalidade de assinatura eletrônica, desde que a integridade seja confirmada pela entidade autenticadora.

O Agravo Interno nos Embargos de Declaração no Agravo em Recurso Especial (AgInt nos EDcl no AREsp 2052895 / SP), de relatoria do Min. Marco Aurélio Bellizze, trata da intempestividade do recurso especial e da validade de contratos eletrônicos. Em relação ao mérito, a decisão destaca que os contratos eletrônicos, em razão das peculiaridades de sua celebração, não necessitam de assinatura de duas testemunhas para serem considerados válidos e passíveis de execução. O Superior Tribunal de Justiça já se posicionou no sentido de que contratos celebrados eletronicamente, com o uso de novos meios de verificação de autenticidade e presença, possuem força executiva, mesmo sem as assinaturas testemunhais tradicionais. A executividade desses contratos é garantida pelos modernos mecanismos de autenticação e segurança.

Outro caso do TJDFT, Acórdão n. 1832371, de relatoria de Carlos Pires Soares Neto, envolveu a tentativa de execução de um distrato de contrato de franquia assinado digitalmente pelas partes e por testemunhas, sem identificação do provedor de assinatura digital.

O Tribunal de Justiça do Distrito Federal e Territórios (TJDFT) ressaltou que a Medida Provisória n. 2.200-2/2001 permite o uso de assinaturas eletrônicas com certificados não emitidos pela ICP-Brasil, desde que sejam reconhecidos como válidos pelas partes ou aceitos por quem o documento é oposto. Além disso, a Lei n. 14.063/2020 categoriza assinaturas eletrônicas em três níveis (simples, avançadas e qualificadas), cada um conferindo graus distintos de confiabilidade.

Para que o distrato fosse considerado título executivo extrajudicial, era necessário comprovar sua certeza, liquidez e exigibilidade, além de demonstrar a autoria e a integridade do documento eletrônico, o que não foi feito pela apelante. Assim, o Tribunal manteve a decisão de origem e negou provimento ao recurso.

O Recurso Especial n. 2159442-PR (2024/0267355-0), de relatoria da Min. Nancy Andrighi, aborda a validade jurídica das assinaturas eletrônicas, mesmo quando estas são emitidas por uma entidade não credenciada no sistema ICP-Brasil.

O caso envolve a disputa sobre a veracidade de uma assinatura eletrônica utilizada em um título de crédito, cuja certificação foi realizada por uma pessoa jurídica de direito privado não vinculada à ICP-Brasil. A questão central é se essa circunstância comprometeria a presunção de autenticidade e a força probatória do documento eletrônico.

A Ministra, ao analisar o caso, defendeu a ideia de que a legislação brasileira, especialmente a Medida Provisória n. 2.200-2/2001, confere validade jurídica às assinaturas eletrônicas, independentemente de serem certificadas por uma entidade vinculada ao ICP-Brasil, desde que as partes envolvidas reconheçam sua validade e os métodos de autenticação sejam confiáveis.

A decisão também reforça que, segundo o art. 10, § 2º, da MPV 2200/2001, o controle da autenticidade e da integridade de documentos eletrônicos depende do uso de meios tecnológicos adequados, como criptografia e fatores múltiplos de autenticação. A Ministra destacou ainda que, a impugnação da veracidade da assinatura eletrônica deve ser realizada pela parte a quem o documento for oposto, e não pelo juiz, conforme prevê o CPC/2015 em seu art. 411, I.

A jurisprudência estabelecida no recurso especial reconhece que a presunção de autenticidade dos documentos digitais deve prevalecer, a não ser que se prove o contrário de forma técnica. Com isso, o recurso foi provido para que a ação de busca e apreensão fosse processada, reconhecendo a validade das assinaturas eletrônicas e a integridade do título de crédito eletrônico, mesmo sem o credenciamento da entidade certificadora no ICP-Brasil.

5 Conclusão

A assinatura eletrônica, impulsionada pela crescente digitalização das relações jurídicas, consolidou-se como ferramenta essencial para garantir a autenticidade, a integridade e a validade jurídica de documentos eletrônicos. Embora existam diferentes tipos de assinatura eletrônica, a legislação e a jurisprudência brasileiras convergem para a adoção da assinatura digital com certificação ICP-Brasil como padrão que confere segurança jurídica equivalente à dos documentos físicos, simplificando sua aceitação em processos judiciais.

A opção pela assinatura digital certificada, além de facilitar a aceitação em processos judiciais, atende às peculiaridades do documento digital, assegurando os

requisitos de segurança, autenticidade e integridade. Essa escolha, em consonância com o princípio da eficiência processual, impulsiona a modernização do sistema jurídico brasileiro, consolidando a assinatura digital com certificação ICP-Brasil como instrumento essencial para o avanço do direito digital.

A relevância da assinatura digital com certificação ICP-Brasil reside, em grande parte, na sua capacidade de garantir a autenticidade e a integridade dos documentos eletrônicos. A autenticidade, como visto, refere-se à certeza da identidade do signatário, enquanto a integridade garante que o documento não sofreu alterações após a sua assinatura.

Nesse sentido, o uso de certificados digitais emitidos por entidades credenciadas junto à ICP-Brasil garante a confiabilidade da assinatura, pois estabelece um vínculo único e inequívoco entre o documento e o seu signatário. A criptografia assimétrica, tecnologia que fundamenta a ICPBrasil, atribui chaves públicas e privadas aos usuários, as quais são utilizadas para assinar e verificar a autenticidade das assinaturas digitais.

A jurisprudência brasileira, acompanhando a evolução tecnológica e legislativa, tem reconhecido a validade e a eficácia da assinatura digital com certificação ICP-Brasil, consolidando sua equivalência à assinatura física em diversos contextos. Diversos julgados, exemplo dos mencionados neste artigo, demonstram a tendência dos tribunais em aceitar a assinatura digital como prova documental, especialmente em processos eletrônicos.

Em suma, a adoção da assinatura digital com certificação ICP-Brasil no Brasil representa um passo significativo na modernização do sistema jurídico, impulsionando a desmaterialização dos documentos e contribuindo para a construção de um ambiente jurídico mais eficiente, seguro e adaptado à realidade digital. A segurança jurídica proporcionada por esse tipo de assinatura, aliada à sua conformidade com a legislação e à jurisprudência pátria, consolida sua importância para o desenvolvimento de um sistema judicial mais célere, eficiente e acessível.

REFERÊNCIAS

BARBAGALO, Erica Brandini. **Contratos eletrônicos**. São Paulo: Saraiva, 2021.

BINENBOJM, G. **Direito administrativo e transformação digital do Judiciário**. Rio de Janeiro: FGV, 2022.

BRASIL. **Código de Processo Civil**. Lei n. 13.105, de 16 mar. 2015. Brasília: Presidência da República, 2015. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 18 nov. 2024.

BRASIL. **Lei n. 11.419**, de 19 dez. 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/L11419.htm. Acesso em: 10 set. 2024.

BRASIL. **Lei n. 14.063**, de 23 set. 2020. Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos. Disponível em: www.planalto.gov.br/ccivil_03/_ato20192022/2020/lei/l14063.htm. Acesso em: 18 nov. 2024.

BRASIL. **Medida Provisória n. 2.200-2**, de 24 ago. 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/2001/2200-2.htm. Acesso em: 09 set. 2024.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial n. 1.495.920/MG**. Rel. Min. Luis Felipe Salomão, j. 14-03-2017. Disponível em: https://www.stj.jus.br. Acesso em: 19 set. 2024.

BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Especial n. 2.150.278/PR**. Rel. Min. Nancy Andrighi, j. 24-09-2024. Disponível em: https://www.stj.jus.br. Acesso em: 18 set. 2024.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial n. 2159442-PR** (2024/0267355-0). Relatora: Ministra Nancy Andrighi. Recurso Especial. Processual Civil. Ação de Busca e Apreensão. Indeferimento Inicial. Extinção. Cédula de Crédito Bancária. Endosso. Emissão e Assinatura Eletrônicos. Validação Jurídica de Autenticidade e Integridade. Entidade Autenticadora Eleita pelas Partes sem Credenciamento no Sistema ICP-Brasil. Possibilidade. Assinatura Eletrônica. Modalidades. Força Probatória. Juiz. Impugnação de Ofício. Inviabilidade. Ônus das Partes. Julgado em 2024. Diário da Justiça Eletrônico, 13 jun. 2024. Disponível em: www.stj.jus.br. Acesso em: 22 ago. 2024.

BRASIL. Superior Tribunal de Justiça (STJ). **Agravo Interno nos Embargos de Declaração no Agravo em Recurso Especial n. 2052895/SP**. Rel. Min. Marco Aurélio Bellizze, j. 10-06-2024. Disponível em: https://www.stj.jus.br. Acesso em: 18 nov. 2024.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios (TJDFT). **Acórdão n. 1832371**. Rel. Carlos Pires Soares Neto. Disponível em: https://www.tjdft.jus.br. Acesso em: 18 nov. 2024.

CARVALHO, Cristiano Sobral de. **Certificação Digital e Assinaturas Eletrônicas**. Rio de Janeiro: Forense, 2023.

DAMIN, Anna Maria Prebianca Hennies. A assinatura digital no Brasil: validade e aspectos jurídicos. **Revista de Direito Digital**, v. 8, n. 2, p. 45-67, 2020.

DINAMARCO, Cândido Rangel. **Execução civil**. São Paulo: Malheiros, 2003.

DIDIER JR., Fredie. **Curso de Direito Processual Civil**: processo de execução. 19. ed. Salvador: JusPodivm, 2019.

DIDIER JR., Fredie. **Curso de Direito Processual Civil**: processo de execução. 20. ed. Salvador: JusPodivm, 2020.

DIZER O DIREITO. Assinatura Eletrônica e os Tipos de Autenticação Digital no Brasil. **Dizer o Direito**, 2022. Disponível em: https://dizerodireito.com.br. Acesso em: 17 out. 2024.

FERREIRA, Miguel. **Introdução à preservação digital**: conceitos, estratégias e atuais consensos. Portugal: Escola de Engenharia da Universidade do Minho, 2006.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. **Manual do Processo de Execução**. 8. ed. São Paulo: RT, 2021.

MARQUES, José Luiz Dias. **O direito na era digital**. Belo Horizonte: Del Rey, 2022.

O'NEILL, Máire. Insecurity by design: today's IoT device security problem. **Architecture of smart certificates for web3 applications against cyberthreats in financial industry**. Submitted on 3 nov. 2023.

SCAVONE JÚNIOR, Luiz Antônio. **Direito digital e internet**. São Paulo: RT, 2022.

SAYÃO, Luís Fernando. Repositórios digitais confiáveis para a preservação de periódicos eletrônicos científicos. **Periódico Ponto de Acesso**, UFBA, Salvador, v. 4, n. 3, p. 68-94, dez. 2010.

SILVA, J. A. Assinaturas Eletrônicas e Certificação Digital no Direito Brasileiro. São Paulo, **Revista Jurídica**, 2022.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **REsp 1.326.088/SP**, Rel. Min. Luis Felipe Salomão, j. 10 abr. 2019. Disponível em: www.stj.jus.br. Acesso em: 16 fev. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **REsp 2.150.278/PR**. Rel. Min. Nancy Andrighi, j. 24-9-2024.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **AgRg no AREsp 670.369/SP**. Rel. Min. Marco Aurélio Bellizze, j. 27-05-2015.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO (TJ-SP). **Apelação Cível 1005042-89.2020.8.26.0100**. Rel. Des. João Carlos Saletti, j. 15-6-2021.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS (TJ-DFT). **Processo 0722309-7.2021.8.07.0001**. Rel. Des. Josaphá Francisco dos Santos, j. 24-11-2021.

VERI, Márcia. **Certificação Digital e Autenticação de Documentos no Brasil**. São Paulo: Thomson Reuters, 2021.