CAPÍTULO 8

ASSINATURAS ELETRÔNICAS EM DOCUMENTOS DIGITAIS SÃO VALIDAS OU INVALIDAS A TEOR DAS LEIS 14.063/20-LEI 12.965/14 E MP 2.200/01

https://doi.org/10.22533/at.ed.8192523098

Emerson Roni Nonato Rodrigues
Acadêmico(a) do curso de Direito

João Carlos Lima de Oliveira
Professor do curso de Deireito da UNIGRAN CAPITAL

RESUMO: O presente trabalho tem como objetivo analisar a validade das assinaturas eletrônicas em documentos digitais, à luz das normativas brasileiras estabelecidas pelas Leis 14.063/2020, 12.965/2014, e a Medida Provisória 2.200/2001, com foco na sua aplicabilidade em processos judiciais. A pesquisa aborda a distinção entre os diferentes tipos de assinaturas eletrônicas, como simples, avançada e qualificada, além de explorar as implicações jurídicas da assinatura digital qualificada e sua equiparação à assinatura manuscrita. A importância da certificação digital, através da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), e a análise dos metadados digitais como suporte da validade documental são temas centrais discutidos. Através de uma abordagem teórica e análise de jurisprudência, o estudo demonstra que as assinaturas digitais, quando devidamente certificadas, têm a mesma validade jurídica que as assinaturas tradicionais, sendo amplamente aceitas no sistema judiciário. Contudo, destaca-se que falhas na certificação digital, manipulação de metadados e falta de verificação da autenticidade podem comprometer a validade das assinaturas, tornando-as inapta para o uso como prova legal.

PALAVRAS-CHAVE: Assinatura eletrônica. Validade jurídica. Certificação digital. ICP-Brasil. Metadados. Processo judicial.

Are electronic signatures on digital documents valid or invalid according to Laws 14.063/20, 12.965/14, and MP 2.200/01

ABSTRACT: This paper aims to analyze the validity of electronic signatures in digital documents under Brazilian regulations established by Laws 14.063/2020, 12.965/2014, and Provisional Measure 2.200/2001, focusing on their applicability in judicial processes. The research discusses the differences between electronic signature types, such as simple, advanced, and qualified, and explores the legal implications of qualified digital signatures and their equivalence to handwritten signatures. The importance of digital certification through the Brazilian Public Key Infrastructure (ICP-Brasil), as well as the analysis of digital metadata as supporting evidence for document validity, are central themes in this study. Through a theoretical approach and jurisprudence analysis, the study shows that digital signatures, when properly certified, hold the same legal validity as traditional signatures and are widely accepted within the judiciary system. However, it highlights that failures in digital certification, manipulation of metadata, and lack of verification of authenticity may compromise the validity of signatures, making them unsuitable as legal evidence.

KEYWORDS: electronic signature, legal validity, digital certification, ICP-Brasil, metadata, ju- dicial process.

INTRODUÇÃO

O avanço tecnológico e a crescente digitalização dos atos jurídicos impuseram novos desafios à autenticidade e segurança dos documentos eletrônicos, exigindo um aparato normativo capaz de conferir validade às manifestações de vontade realizadas no ambiente digital. No Brasil, as assinaturas eletrônicas consolidaram-se como instrumentos de autenticação documental, permitindo que contratos, acordos e demais atos jurídicos sejam formalizados de maneira remota, sem a necessidade de suporte físico. No entanto, a aplicabilidade jurídica dessas assinaturas exige a observância de parâmetros legais e técnicos que garantam sua segurança, integridade e eficácia probatória.

A regulamentação das assinaturas eletrônicas no ordenamento jurídico brasileiro decorre da edição da Medida Provisória nº 2.200-2/2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), estabelecendo um sistema hierárquico para a emissão e gestão de certificados digitais, conferindo presunção de autenticidade às assinaturas eletrônicas qualificadas. Posteriormente, a Lei nº 12.965/2014 (Marco Civil da Internet) dispôs sobre os direitos e deveres dos usuários da internet, incluindo disposições sobre segurança digital e proteção de dados. Mais recentemente, a Lei nº 14.063/2020 consolidou a aceitação das assinaturas eletrônicas na Administração

Pública, categorizando-as em três tipos: simples, avançada e qualificada, cada uma com requisitos específicos de segurança e aplicação.

Diante desse contexto, surge a seguinte problemática: em quais condições as assinaturas eletrônicas são consideradas juridicamente válidas e quais requisitos devem ser observados para garantir sua segurança, integridade e admissibilidade no ordenamento jurídico brasileiro? Tal questionamento se faz pertinente, considerando o crescimento expressivo das contratações eletrônicas e os desafios enfrentados para assegurar a autenticidade e a não repudiação dos documentos assinados digitalmente. Parte-se da hipótese de que a validade das assinaturas eletrônicas depende da observação dos requisitos normativos previstos na legislação vigente, bem como da implementação de mecanismos técnicos de segurança, tais como criptografia, função hash, rastreamento de metadados e certificação digital vinculada à ICP-Brasil.

Ademais, a conformidade com padrões internacionais e a adoção de protocolos de verificação são fundamentais para assegurar a confiabilidade dos documentos eletronicamente assinados. A relevância desta pesquisa se justifica pela crescente adesão às assinaturas eletrônicas em diferentes esferas, seja no setor privado, seja na Administração Pública, exigindo um aprofundamento jurídico e técnico sobre sua validade, segurança e limitações. Diante do aumento significativo de fraudes eletrônicas e litígios relacionados à autenticidade de assinaturas digitais, faz-se imprescindível um estudo detalhado que esclareça os mecanismos de verificação, a admissibilidade probatória e os riscos envolvidos na sua utilização.

O objetivo geral deste trabalho consiste em analisar a validade jurídica das assinaturas eletrônicas no Brasil, considerando os aspectos normativos, técnicos e probatórios. Para tanto, os objetivos específicos são: (i) identificar as categorias de assinaturas eletrônicas e suas diferenças quanto à segurança e validade jurídica; (ii) examinar os requisitos normativos e técnicos necessários para a admissibilidade das assinaturas eletrônicas no ordenamento jurídico brasileiro; e (iii) avaliar os desafios e riscos associados à segurança e confiabilidade dessas ferramentas no meio digital.

A metodologia adotada para a execução deste estudo é de caráter qualitativo, fundamentada em pesquisa bibliográfica e documental, utilizando como base a legislação pertinente, doutrina especializada e jurisprudência nacional. O estudo também se apoiará em normas técnicas e diretrizes da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), bem como nas normativas internacionais de segurança digital. Dessa forma, busca-se consolidar um entendimento aprofundado sobre a temática, contribuindo para a segurança jurídica e a eficácia dos mecanismos de autenticação digital no Brasil.

DA NORMATIVA DAS ASSINATURAS ELETRÔNICAS

A assinatura eletrônica, no contexto jurídico brasileiro, é um mecanismo utilizado para validar a identidade do signatário em transações realizadas em ambientes digitais. Ela é amplamente empregada em contextos nos quais não se exige alto nível de segurança, sendo usualmente associada a processos de autenticação simples, como senhas ou códigos temporários. Essa modalidade de assinatura não garante a integridade do documento, ou seja, não assegura que o conteúdo do arquivo assinado não foi alterado após a assinatura. Além disso, a autenticidade do signatário, embora indicada por meio de um processo eletrônico, não é certificada de forma rigorosa. A assinatura eletrônica, portanto, é adequada para transações de baixo risco, como a adesão a termos de serviço ou documentos informais que não envolvem grandes responsabilidades ou impactos jurídicos (Monteiro; Mignoni, 2018).

Por outro lado, Machado (2020) destaca que a assinatura digital é uma versão mais avançada da assinatura eletrônica, que utiliza um processo de criptografia assimétrica, o que confere maior segurança e autenticidade ao documento. A assinatura digital é validada por meio de um par de chaves, sendo a chave privada utilizada pelo signatário para assinar o documento e a chave pública, disponível para qualquer parte interessada, utilizada para verificar a autenticidade da assinatura. Esse método de assinatura digital garante tanto a integridade do documento quanto a identidade do signatário, já que qualquer alteração no conteúdo do arquivo invalidaria a assinatura. No Brasil, as assinaturas digitais, quando realizadas por meio de certificados digitais emitidos por autoridades certificadoras credenciadas pela ICP-Brasil, têm plena validade jurídica, conferindo um nível elevado de confiança e segurança para transações que envolvem contratos e documentos jurídicos significativos.

No que tange à assinatura híbrida, para Monteiro e Mignoni (2018, p.17):

> Esta combina aspectos da assinatura eletrônica e da assinatura digital, buscando reunir a praticidade da primeira com a segurança da segunda. Esse tipo de assinatura é utilizado quando há a necessidade de garantir tanto a autenticidade do signatário quanto a integridade do documento, mas sem a exigência do rigor completo de uma assinatura digital. A assinatura híbrida é frequentemente aplicada em contextos onde é necessário ter uma validação mista, utilizando tanto elementos digitais quanto físicos. Isso é particularmente útil em situações que envolvem a assinatura digital de uma parte do documento e a validação física de outra, combinando os benefícios dos dois tipos de assinatura em um único processo. Assim, a assinatura híbrida apresenta uma solução flexível para documentos que exigem uma verificação robusta, mas sem a complexidade total da assinatura digital.

Segundo Lima (2015) a escolha entre o tipo de assinatura depende da natureza do ato jurídico e da necessidade de segurança envolvida. A assinatura eletrônica (usuário, senha, biometria) é mais apropriada para transações simples e de baixo risco, como interações em plataformas digitais, onde a integridade do documento não é

uma preocupação central. Já a assinatura eletrônica (certificado digital) é indicada para situações em que a proteção contra fraudes e a garantia da autenticidade do signatário são essenciais, como em transações financeiras e acordos legais que exigem um alto nível de confiança. A assinatura híbrida, por sua flexibilidade, é ideal para contextos em que se busca combinar a praticidade de uma solução digital com a formalidade de uma validação física, como em documentos empresariais que exigem múltiplos processos de autenticação.

Em termos de regulamentação, a Lei nº 14.063/2020 estabelece as normas para a utilização de assinaturas eletrônicas e digitais no Brasil, reconhecendo as assinaturas digitais como plenamente válidas quando realizadas com o uso de certificados digitais emitidos por autoridades certificadoras credenciadas. A Lei também define diferentes categorias de assinaturas, como simples, avançada e qualificada, que são estabelecidas conforme o nível de segurança exigido para o tipo de transação. A assinatura simples pode ser utilizada em transações cotidianas com baixo risco, enquanto a assinatura avançada e qualificada é necessária para documentos que envolvem maior complexidade e exigem garantias robustas quanto à identidade do signatário e à integridade do conteúdo (Machado, 2020).

Para Sedin (2017) a distinção entre essas três modalidades de assinatura é essencial para a correta aplicação de práticas jurídicas no contexto digital. As assinaturas eletrônica, digital e híbrida devem ser escolhidas de acordo com o risco da transação e as exigências legais pertinentes. Cada uma delas oferece um nível de segurança e autenticidade distinto, e a escolha da modalidade correta pode ter implicações significativas para a validade e a execução do documento assinado. Assim, é fundamental que advogados, empresas e demais profissionais jurídicos compreendam as diferenças e aplicabilidades de cada tipo de assinatura, a fim de garantir a conformidade com a legislação vigente e a segurança jurídica das transações realizadas de forma eletrônica.

A Lei nº 14.063/2020, ao abordar o uso de assinaturas eletrônicas no Brasil, estabelece uma classificação precisa e estratégica das suas modalidades, a saber: simples, avançada e qualificada. A assinatura eletrônica simples consiste em um mecanismo básico que, embora desempenhe um papel funcional no contexto digital, não oferece a robustez necessária para garantir a autenticidade em ambientes jurídicos ou de alta segurança. Sua aplicação restringe- se, portanto, a transações de menor complexidade e risco, em que não há exigência de comprovação rigorosa da identidade do signatário. Tal assinatura, embora válida para atos administrativos e comerciais corriqueiros, carece da confiança necessária para documentos de maior relevância jurídica, não proporcionando, por conseguinte, o grau de certeza requerido pelo ordenamento jurídico (Machado, 2020).

De acordo com Monteiro e Mignoni (2018) a assinatura eletrônica avançada tem como principal característica a utilização de métodos mais sofisticados de autenticação, como o uso de senhas e certificados digitais, que conferem uma segurança aprimorada ao ato jurídico. A assinatura avançada, portanto, é indicada para transações de maior envergadura que demandam maior confiabilidade, mas sem a necessidade de um mecanismo tão complexo quanto o exigido para a assinatura qualificada. Em termos legais, ela é adequada para compromissos empresariais ou contratuais em que a identidade do signatário precisa ser validada com mais precisão, mas onde a formalidade não alcança o patamar exigido para um ato de natureza jurídica mais alta, como nos processos judiciais ou administrativos de grande repercussão.

A assinatura qualificada, conforme definida pela Lei nº 14.063/2020, é, por sua natureza, a mais robusta e segura das modalidades de assinaturas eletrônicas, sendo essencialmente vinculada à utilização de um certificado digital emitido pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). A assinatura qualificada confere plena validade jurídica ao documento eletrônico, conferindo-lhe o mesmo efeito de uma assinatura manuscrita. Sua aplicação é imprescindível em contextos onde a segurança e a integridade da transação são de suma importância, como em procedimentos judiciais, administrativos ou qualquer ato que envolva grandes interesses jurídicos. Nesse contexto, a assinatura qualificada se distingue por ser o único tipo de assinatura eletrônica que possui o mesmo valor jurídico de uma assinatura física, assegurando que o documento não apenas seja autenticado, mas também não possa ser alterado após sua assinatura (Sendin, 2017).

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), em seu papel regulador, exerce uma função primordial no cenário da certificação digital, sendo a responsável por estabelecer as normas e garantir a segurança da emissão de certificados digitais no Brasil. Tal infraestrutura baseia-se em um sistema de criptografia de chave pública que assegura a integridade e a autenticidade dos documentos eletrônicos. Além disso, a ICP-Brasil regula a atuação de entidades certificadoras e autoridades de registro, garantindo a padronização dos processos e a conformidade com os parâmetros legais e técnicos exigidos para a emissão de certificados digitais. A regulamentação da ICP-Brasil visa assegurar a segurança jurídica das transações digitais, protegendo as partes envolvidas contra fraudes e garantindo que o documento assinado tenha plena validade perante o ordenamento jurídico (Lima, 2015).

Okano e Alcântara (2018) apontam que a função reguladora da ICP-Brasil vai além da mera validação de assinaturas. A estrutura da ICP-Brasil assegura que todas as transações digitais realizadas no território brasileiro, que envolvam a assinatura qualificada, possuam o mais alto nível de segurança, amparado por protocolos criptográficos reconhecidos internacionalmente. Isso se traduz em

uma regulamentação robusta que proporciona segurança jurídica aos processos administrativos e judiciais, permitindo que transações feitas no meio digital tenham a mesma força e valor que aquelas realizadas de forma tradicional, com a assinatura física. O marco normativo criado pela ICP-Brasil também serve de referencial para o desenvolvimento de novas tecnologias de segurança, que buscam não apenas garantir a autenticidade, mas também a confidencialidade das transações realizadas.

A utilização da ICP-Brasil representa, portanto, um avanço significativo para o Brasil no que se refere à modernização dos sistemas de certificação digital, permitindo que o país se integre a padrões globais de segurança cibernética. A infraestrutura assegura, ainda, que os certificados digitais estejam alinhados com as melhores práticas internacionais, o que confere maior confiança nas transações eletrônicas e amplia as possibilidades de adoção de tecnologias como contratos inteligentes e sistemas de *blockchain*. Além disso, a aplicação de criptografia avançada no processo de assinatura digital cria um ambiente de alta segurança, fundamental para a efetiva implementação da Lei Geral de Proteção de Dados Pessoais (LGPD), uma vez que garante a integridade e confidencialidade dos dados envolvidos nas transações eletrônicas (DATACERTIFY, 2022).

A importância da ICP-Brasil se estende também ao campo da segurança cibernética, uma vez que, por meio da utilização de certificados digitais e criptografia, assegura a proteção contra a adulteração de documentos e o uso indevido de informações. Esse sistema proporciona um escudo contra fraudes digitais, assegurando que apenas o verdadeiro signatário tenha a capacidade de realizar a assinatura e, por consequência, tornar válida a transação ou o ato jurídico. O controle rigoroso e a supervisão das entidades certificadoras e dos registros públicos desempenham papel essencial para garantir que as práticas sejam realizadas dentro dos mais altos padrões de segurança e conformidade com as exigências legais e normativas (Sendin, 2017).

Em um contexto mais amplo, a ICP-Brasil também possui grande relevância na implementação de políticas públicas voltadas à digitalização de serviços no Brasil. Sua regulação permite que a administração pública adote processos mais rápidos e eficientes, reduzindo custos operacionais e proporcionando maior acessibilidade à população. A digitalização de serviços públicos, assegurada pela ICP-Brasil, não só melhora a eficiência do Estado, mas também facilita a inclusão de cidadãos no sistema de governança digital, permitindo-lhes acessar serviços administrativos, realizar transações fiscais e contratuais, bem como resolver questões jurídicas de maneira mais ágil e segura (JUST ARB, 2023).

SEGURANÇA JURÍDICA E MECANISMOS DE AUTENTICAÇÃO

A modernização das relações jurídicas e comerciais demandou a criação de mecanis- mos normativos que garantissem autenticidade, integridade e segurança aos documentos eletrônicos assinados digitalmente. No Brasil, esse marco regulatório foi estabelecido com a edi- ção da Medida Provisória nº 2.200-2/2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), viabilizando a certificação digital de documentos e conferindo-lhes validade jurídica (Brasil, 2001). A implementação dessa estrutura normativa assegurou um modelo robusto para validar manifestações de vontade em ambiente eletrônico, reduzindo a dependência do suporte físico e ampliando a segurança jurídica nas transações digitais.

A referida Medida Provisória garantiu às assinaturas digitais emitidas no âmbito da ICP-Brasil a mesma presunção de autenticidade conferida às assinaturas manuscritas, promo- vendo sua aceitação ampla em contratos, atos administrativos e procedimentos judiciais. Tal avanço normativo permitiu que documentos assinados digitalmente gozassem de presunção de veracidade, assegurando sua integridade e inalterabilidade. Segundo Machado (2020), a cria- ção da ICP-Brasil estruturou um sistema hierárquico de certificação digital que reforçou a confiabilidade dos documentos eletrônicos, permitindo a rastreabilidade das assinaturas e ga- rantindo a identidade do signatário. Esse mecanismo fortaleceu a proteção contra fraudes e consolidou a aplicabilidade das assinaturas digitais no ordenamento jurídico brasileiro.

A regulamentação das assinaturas eletrônicas, contudo, não se limitou à certificação digital, abrangendo também a proteção dos direitos fundamentais dos usuários no ambiente virtual. Nesse sentido, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, estabe- leceu princípios essenciais para a governança digital no Brasil, impondo diretrizes sobre pri- vacidade, proteção de dados e inviolabilidade das comunicações (Brasil, 2014). A interseção entre essa norma e a legislação que rege as assinaturas eletrônicas demonstra a necessidade de um arcabouço regulatório harmônico, que alie inovação tecnológica à salvaguarda dos direitos fundamentais.

O Marco Civil da Internet impôs obrigações aos provedores e definiu parâmetros para o tratamento de dados pessoais, influenciando diretamente a utilização e o armazenamento das assinaturas eletrônicas. O respeito à privacidade e a vedação ao acesso indevido a informa- ções sigilosas são garantias essenciais para a legitimidade dos atos jurídicos praticados por meio digital. Nesse contexto, a normatização da assinatura eletrônica qualificada, que exige certificação digital vinculada à ICP-Brasil, proporciona maior segurança às partes envolvidas, garantindo a integridade dos documentos e a autenticidade do signatário. Assim, a regulamen- tação brasileira busca um equilíbrio entre a celeridade das transações digitais e a proteção contra vulnerabilidades tecnológicas.

Com a crescente adesão às assinaturas eletrônicas, tornou-se imperativo que o orde- namento jurídico estabelecesse diretrizes claras sobre sua aplicabilidade e níveis de segurança. A Lei nº 14.063/2020 preencheu essa lacuna ao categorizar as assinaturas eletrônicas em simples, avançadas e qualificadas, estabelecendo critérios diferenciados conforme o grau de risco da transação (Brasil, 2020). Essa classificação permite que diferentes níveis de autenti- cação sejam adotados de acordo com a necessidade do ato jurídico, prevenindo fraudes e as- segurando a confiabilidade dos documentos assinados digitalmente.

A assinatura eletrônica simples caracteriza-se pela ausência de requisitos mais rigoro- sos de identificação, sendo admitida para transações de baixo risco, como aceite de termos de uso em plataformas digitais. Já a assinatura avançada exige métodos adicionais de autentica- ção, como biometria ou validação por múltiplos fatores, aumentando o nível de segurança do ato. Por fim, a assinatura qualificada é a mais robusta em termos de confiabilidade jurídica, pois requer um certificado digital emitido por Autoridade Certificadora vinculada à ICP- Brasil, conferindo-lhe presunção de autenticidade e validade legal equiparada à assinatura manuscrita (Oliveira, 2019).

A exigência da assinatura qualificada para atos que envolvem risco significativo, co- mo transações financeiras, contratos de grande vulto e atos administrativos relevantes, tem fundamento na necessidade de mitigar fraudes e garantir a segurança dos signatários. Segundo Sendin (2017), a certificação digital vinculada à ICP-Brasil permite a identificação inequívoca do signatário, assegurando que o documento eletrônico permaneça inalterado após sua assina- tura. Esse mecanismo impede adulterações e amplia a confiabilidade dos atos praticados digi- talmente, sendo essencial para a consolidação da segurança jurídica no meio eletrônico.

A regulamentação das assinaturas eletrônicas no Brasil também está alinhada a normas internacionais de segurança da informação. A ISO/IEC 27001, por exemplo, estabelece dire- trizes sobre a gestão da segurança da informação, garantindo que documentos eletrônicos se- jam protegidos contra acessos indevidos e falsificações. Segundo Lima (2015, p. 83):

> A criptografia utilizada nas certificações digitais, especialmente no contexto da ICP- Brasil, está alinhada com os padrões internacionais, garantindo a validade das assi- naturas eletrônicas não apenas no âmbito nacional, mas também em acordos interna- cionais e processos judiciais de abrangência global.

A normatização das assinaturas eletrônicas não se restringe ao âmbito interno. A Convenção das Nações Unidas sobre o Uso de Comunicações Eletrônicas em Contratos Internacionais, adotada pela UNCITRAL, consolidou diretrizes essenciais

para o reconhecimento jurídico das transações eletrônicas em diferentes países. Essa convenção uniformiza os critérios para validade dos contratos eletrônicos, assegurando que a assinatura digital tenha força legal em diversos ordenamentos jurídicos (UNCITRAL, 2005). No Brasil, essa convergência normativa amplia a aceitação dos documentos assinados digitalmente, garantindo maior previsibilidade e segurança nas relações comerciais transfronteiriças.

No contexto europeu, a adoção do Regulamento eIDAS (*Electronic Identification, Authentication and Trust Services*, estabeleceu um sistema de reconhecimento mútuo das assinaturas eletrônicas entre os Estados-membros da União Europeia. Esse regulamento diferencia as assinaturas em três categorias: simples, avançada e qualificada, assegurando diferentes níveis de segurança e autenticidade (*EUROPEAN COMMISSION*, 2014). A similaridade entre essa classificação e a adotada na Lei nº 14.063/2020, no Brasil, demonstra um alinhamento regulatório que permite maior compatibilidade entre os sistemas jurídicos e facilita a aceitação de documentos assinados digitalmente entre empresas e governos europeus e brasileiros.

Nos Estados Unidos, a *Electronic Signatures in Global and National Commerce Act* (ESIGN Act) garantiu validade jurídica às assinaturas eletrônicas, estabelecendo requisitos para sua aceitação em transações comerciais e contratuais. A legislação norte-americana exige que as partes tenham consentido com a utilização da assinatura eletrônica e que o documento assinado digitalmente seja íntegro e verificável (*UNITED STATES*, 2000). A similaridade dessa legislação com o arcabouço normativo brasileiro favorece a interoperabilidade jurídica e facilita a realização de transações internacionais, garantindo que documentos assinados digitalmente no Brasil sejam reconhecidos nos Estados Unidos sem necessidade de novos procedimentos de autenticação.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) tem se destacado como referência para a formulação de políticas de certificação digital e proteção da informação. A adesão do Brasil às diretrizes da OCDE reforça o compromisso do país com a adoção de práticas internacionais de segurança digital. Entre os principais eixos estabelecidos pela organização estão **a** governança digital, a proteção de dados pessoais e a segurança cibernética, aspectos essenciais para a confiabilidade das assinaturas eletrônicas e sua aceitação em processos administrativos e judiciais (OECD, 2019).

A implementação de novas tecnologias tem sido fundamental para reforçar a autenticidade das assinaturas eletrônicas e mitigar riscos de fraudes. O *blockchain*, por exemplo, oferece um sistema descentralizado e imutável de registro, garantindo que a assinatura eletrônica não possa ser alterada após sua realização. Segundo Datacertify (2022, p.4):

> O uso do blockchain na certificação digital assegura um nível superior de confiabilidade, pois cada transação assinada eletronicamente é registrada de maneira irreversível, eliminando a possibilidade de adulteração e conferindo total rastreabilidade ao documento.

A incorporação dessa tecnologia nos sistemas de certificação digital pode aprimorar ainda mais a segurança dos documentos assinados eletronicamente, assegurando que sua autenticidade seja verificável sem a necessidade de intermediários.

Além do *blockchain*, a inteligência artificial tem sido empregada para otimizar os processos de autenticação digital, por meio de algoritmos que detectam tentativas de falsificação e garantem que a identidade do signatário seja verificada de maneira segura. O uso de biometria facial, reconhecimento de voz e autenticação por impressão digital adiciona camadas adicionais de segurança às assinaturas eletrônicas, reduzindo o risco de fraudes. A tendência é que essas inovações tecnológicas sejam incorporadas à regulamentação brasileira, permitindo que as assinaturas eletrônicas sejam mais seguras e acessíveis.

Embora a legislação e os avanços tecnológicos tenham impulsionado o uso das assinaturas eletrônicas, desafios ainda persistem, especialmente no que se refere à aceitação desses documentos por parte dos órgãos públicos e do próprio Poder Judiciário. Apesar de a jurisprudência brasileira ter consolidado o entendimento de que os documentos assinados eletronicamente possuem a mesma validade que os assinados fisicamente, alguns tribunais ainda impõem restrições quanto ao uso da assinatura eletrônica em determinados procedimentos. Esse cenário demonstra a necessidade de capacitação contínua dos operadores do direito e da ampliação do conhecimento técnico sobre certificação digital, garantindo que as assinaturas eletrônicas sejam plenamente aceitas em todos os âmbitos do direito (Machado, 2020).

De acordo com Monteiro e Mignoni (2018) o desconhecimento por parte das empresas e cidadãos sobre os diferentes tipos de assinaturas eletrônicas também representa um obstáculo para sua adoção em larga escala. Muitas organizações ainda optam por imprimir e assinar fisicamente documentos que poderiam ser formalizados digitalmente, por receio de que não sejam aceitos em eventual litígio. Para mitigar esse problema, torna-se fundamental a realização de campanhas de conscientização sobre a validade jurídica das assinaturas eletrônicas, bem como a adoção de políticas públicas que incentivem a digitalização segura dos processos contratuais e administrativos.

Diante desse cenário, a regulamentação das assinaturas eletrônicas no Brasil tem acompanhado a evolução dos padrões internacionais, garantindo maior segurança e confiabilidade às transações digitais. A convergência entre as

normativas brasileiras e as diretrizes internacionais, aliada à implementação de novas tecnologias, possibilita que as assinaturas eletrônicas se tornem um instrumento cada vez mais utilizado e aceito em diferentes esferas do direito. Contudo, para que essa evolução se consolide, é essencial que o país continue aprimorando sua infraestrutura de certificação digital, garantindo a universalização do acesso aos certificados digitais e promovendo um ambiente jurídico seguro e eficiente para a formalização de atos e negócios jurídicos no meio eletrônico.

A evolução tecnológica, aliada às exigências contemporâneas de celeridade e desburo- cratização, transformou a forma como se concebem os meios de prova no processo civil brasi- leiro. O artigo 369 do Código de Processo Civil consagra o princípio da liberdade probatória, permitindo que as partes façam prova dos fatos por quaisquer meios legais, inclusive eletrôni- cos, desde que idôneos e aptos a formar a convicção do juízo. Tal abertura normativa ampara a admissibilidade de assinaturas eletrônicas como elementos válidos de demonstração da von- tade das partes, especialmente nos contratos e atos jurídicos celebrados por meio digital (Sil- va, 2023).

A assinatura digital qualificada, respaldada por certificado emitido pela ICP-Brasil, in- sere-se nesse cenário como a manifestação eletrônica com maior valor probatório presumido. A Medida Provisória nº 2.200-2/2001, ainda em vigor, estabelece que os documentos eletrô- nicos assinados com certificados ICP-Brasil gozam de autenticidade, integridade e validade jurídica, sem necessidade de reconhecimento de firma ou outros requisitos adicionais. Essa presunção legal favorece a segurança nas relações jurídicas eletrônicas e simplifica a instru- ção probatória no processo judicial (Machado, 2020).

A jurisprudência tem conferido respaldo firme a essa presunção. No julgamento do REsp 1.495.920/MG, o Superior Tribunal de Justiça assentou que "a assinatura digital basea- da em certificado emitido por autoridade certificadora credenciada à ICP-Brasil goza de pre- sunção de veracidade, salvo prova em contrário", consolidando o entendimento de que esse meio de autenticação preenche os requisitos legais para formar prova documental eficaz. As- sim, o ônus de desconstituí-la recai sobre a parte que a impugna (Brasil, 2018).

Essa distinção ganha relevância sobretudo quando se compara o valor da prova docu- mental simples — como e-mails, prints e declarações não assinadas com certificado — com os documentos assinados digitalmente via ICP-Brasil. Enquanto os primeiros podem ser ad- mitidos como início de prova ou indícios, os segundos, pela força do arcabouço normativo, são provas plenas, com força autêntica e presunção de integridade. Como bem observam Monteiro e Mignoni (2018), a

robustez da assinatura qualificada torna desnecessário qualquer outro elemento adicional para sua admissibilidade em juízo.

Cabral (2022) reforça que essa equiparação entre documentos físicos assinados manu- almente e documentos eletrônicos assinados digitalmente constitui uma verdadeira mudança de paradigma, na medida em que desloca o foco da forma tradicional de produção probatória para uma lógica informacional. Nesse novo contexto, não é a materialidade do papel que ga- rante a eficácia da prova, mas a rastreabilidade técnica da autoria e a integridade criptográfica dos dados, atributos característicos da certificação digital qualificada no modelo ICP-Brasil.

Contudo, não se pode confundir prova documental com prova eletrônica dotada de atributos legais de autenticidade. Um contrato digital sem certificação, ainda que represente uma manifestação de vontade, carece de presunção legal e pode ser objeto de impugnação com base na ausência de elementos de verificação técnica. Daí a importância de compreender que há hierarquia probatória entre os diversos tipos de assinatura eletrônica — simples, avan- çada e qualificada — cada uma com diferentes graus de validade e exigências de demonstra- ção no processo (SENDIN, 2017).

A doutrina aponta que, embora todas as assinaturas eletrônicas possam ser admitidas como prova no processo civil, a eficácia jurídica de cada uma dependerá da forma como fo- ram geradas e da capacidade de demonstração de autenticidade. Machado (2020) lembra que as assinaturas eletrônicas simples não gozam de presunção legal, exigindo, portanto, a produ- ção de prova complementar para validação em juízo, como perícia técnica ou confissão da parte contrária. Já a assinatura qualificada, por si só, supre tais requisitos e pode ser conside- rada prova cabal da autoria do documento.

A valorização da certificação digital qualificada está relacionada não apenas ao seu potencial de autenticação, mas também à sua integração com outros mecanismos de seguran- ça, como os metadados e registros de auditoria. Segundo o Just Arb (2023), os metadados funcionam como elementos periféricos que corroboram a integridade e o percurso de criação e assinatura do documento, permitindo a verificação de data, hora, local e autoria com elevado grau de precisão. Esses dados complementam a prova documental e contribuem para afastar dúvidas sobre sua veracidade.

Em complemento, a doutrina contemporânea reconhece que a assinatura digital, por permitir a rastreabilidade do signatário e garantir a imutabilidade do conteúdo após sua aposi- ção, satisfaz os requisitos de autenticidade e integridade exigidos pelo Código de Processo Civil para que o documento seja admitido como prova plena. Como destaca Cabral (2022), o juiz, diante de um documento assinado

digitalmente com certificado válido, pode presumi-lo autêntico e veraz, dispensando prova pericial, salvo impugnação específica e fundamentada da parte adversa.

Nessa linha, o Tribunal de Justiça de São Paulo reiterou, na Apelação Cível nº 1002456-00.2020.8.26.0100, que "a assinatura digital certificada, por sua natureza, reveste o documento eletrônico de autenticidade presumida, o que afasta a necessidade de produção de outras provas formais, salvo se demonstrada sua falsidade". Essa orientação jurisprudencial favorece a desjudicialização e estimula a adoção de meios eletrônicos para a prática de atos jurídicos com plena segurança e validade (TJSP, 2022).

ADMISSIBILIDADE PROBATÓRIA E JURISPRUDÊNCIA APLICADA: A ASSINATURA ELETRÔNICA COMO MEIO DE PROVA NO PROCESSO JUDICIAL

A admissibilidade da assinatura digital no processo judicial brasileiro repousa sobre um arcabouço normativo e técnico que a insere como prova documental válida, dotada de pre- sunção de autenticidade. O artigo 369 do Código de Processo Civil legitima o uso de meios atípicos de prova, desde que não vedados em lei, abrindo espaço para os documentos digitais como instrumentos legítimos para demonstrar os fatos alegados em juízo. Nesse sentido, a as- sinatura qualificada — firmada com certificado ICP-Brasil — apresenta-se como elemento que atende aos requisitos de autoria, integridade e idoneidade, tornando-se prova autossufici- ente (Machado, 2020).

Segundo Sendin (2017) o diferencial probatório da assinatura qualificada encontra amparo técnico na criptografia assimétrica, que impede a modificação do conteúdo após a as- sinatura e vincula de forma inequívoca o signatário ao documento. Esse mecanismo confere ao juiz elementos objetivos de aferição da autoria e integridade do ato, dispensando outras formas de comprovação, como o reconhecimento de firma ou a oitiva de testemunhas. Em contraste, as assinaturas eletrônicas simples carecem desse robusto lastro técnico, o que as po- siciona em patamar inferior de confiabilidade jurídica.

A jurisprudência tem caminhado no sentido de reconhecer essa hierarquia probatória, conferindo à assinatura digital qualificada tratamento análogo ao da assinatura manuscrita re- conhecida. Em julgado paradigmático, o Tribunal Regional Federal da 1ª Região registrou:

> A assinatura eletrônica com certificação digital no padrão ICP-Brasil presume-se au- têntica, nos termos da Medida Provisória nº 2.200-2/2001, sendo válida para a práti- ca de atos jurídicos e para efeitos probatórios no processo judicial. Não cabe ao juí- zo exigir prova adicional de autoria quando a assinatura encontra-se vinculada a cer- tificado emitido por autoridade certificadora credenciada (Brasil, 2023).

Esse entendimento reforça o valor legal da assinatura digital qualificada e a segurança jurídica que ela proporciona no âmbito processual, dispensando exigências excessivas quando presentes os critérios técnicos de validade. Além da presunção de veracidade, o documento digital certificado incorpora dados verificáveis por meios eletrônicos, como data e hora da as- sinatura, identidade do titular do certificado, número de série e autoridade certificadora. Esses metadados são públicos e auditáveis, permitindo que o magistrado verifique, de forma direta e técnica, a origem e a autenticidade da assinatura, sem necessidade de perícia grafotécnica ou reconhecimento de firma (Monteiro; Mignoni, 2018).

Essa autossuficiência probatória contribui para o princípio da celeridade processual, reduzindo etapas burocráticas sem comprometer a segurança das relações jurídicas. A prova documental digital, nesse contexto, não apenas substitui o documento físico, mas o supera em confiabilidade e economia procedimental. O processo civil contemporâneo, especialmente no modelo do novo CPC, estimula o uso racional da tecnologia para aprimorar a prestação juris- dicional (Cabral, 2022).

É nesse ponto que se evidencia a nítida distinção entre documentos digitalizados e do- cumentos nativamente digitais com assinatura qualificada. Enquanto os primeiros apenas re- plicam visualmente o conteúdo, os segundos possuem um valor jurídico intrínseco, pois inte- gram em seu código os mecanismos de autenticação e segurança. O documento digital com assinatura ICP-Brasil é, portanto, autêntico por construção, e não por presunção derivada de elementos extrínsecos (Lima, 2015).

Importa ainda considerar que, do ponto de vista do contraditório, a parte que impugna a autenticidade de uma assinatura digital qualificada deve apresentar elementos concretos de dúvida, sob pena de seu argumento ser considerado inconsistente. A carga probatória desloca- se, nesse caso, para quem pretende infirmar a presunção de veracidade da certificação. Tal en- tendimento tem respaldo na doutrina e na prática jurisprudencial, que reconhecem a inversão do ônus como instrumento de racionalização da prova (Oliveira, 2019).

Diferentemente do que ocorre com provas indiretas ou indiciárias, o documento digital com assinatura qualificada não exige validação complementar para produção de efeitos. Sua força decorre da própria legislação que o institui, como a Medida Provisória nº 2.200-2/2001 e a Lei nº 14.063/2020, cujas disposições atribuem valor jurídico pleno à certificação emitida no âmbito da ICP-Brasil. A jurisprudência e os órgãos públicos têm progressivamente aderido a essa concepção, reconhecendo o documento eletrônico certificado como meio legítimo e su- ficiente para instruir o processo judicial (Machado, 2020).

A eficácia processual da assinatura digital deve, portanto, ser analisada com base em critérios objetivos e na legislação vigente, e não por um apego formalista

ao suporte físico. A digitalização do processo, sobretudo após a implementação do PJe e da virtualização das ser- ventias, tornou a assinatura eletrônica qualificada um elemento central da dinâmica forense. O documento eletrônico certificado assume, assim, posição de primazia no conjunto das provas documentais admitidas em juízo (Monteiro; Mignoni, 2018).

A superação do paradigma do papel, todavia, exige não apenas o reconhecimento jurí- dico da assinatura digital, mas também o domínio técnico de seus mecanismos por parte dos operadores do direito. Magistrados, advogados e serventuários precisam compreender os fun- damentos da certificação digital, os limites de sua validade, e os critérios de verificação de sua autenticidade. Essa capacitação é indispensável para que a prova eletrônica cumpra sua fun- ção constitucional de servir à verdade e à justiça (Sendin, 2017).

A adoção da assinatura digital qualificada também impacta diretamente o regime de fé pública dos documentos. A certificação emitida por Autoridade Certificadora credenciada confere ao instrumento digital força equivalente à do documento público, nos termos do artigo 411 do Código de Processo Civil. Isso significa que, salvo prova em contrário, presume-se verdadeira a manifestação de vontade constante do documento assinado com certificado ICP- Brasil, inclusive quanto à autoria. Essa presunção reforça a estabilidade jurídica do processo e protege os atos processuais contra alegações infundadas de nulidade (Monteiro; Mignoni, 2018).

Ao se considerar o tratamento da assinatura digital à luz da doutrina, observa-se que sua força probante é especialmente relevante em contextos em que se exige formalidade jurí- dica. Contratos, petições, procurações e atos judiciais podem ser instruídos por documentos eletrônicos que, devidamente assinados com certificação digital, suprem todas as exigências legais de autenticidade e integridade. Para Machado (2020), a tendência é que esses documen- tos sejam cada vez mais aceitos como regra, não como exceção, na dinâmica do processo civil digital.

A doutrina também tem se debruçado sobre a distinção entre a validade da assinatura e a validade do próprio documento. Ainda que a assinatura seja tecnicamente válida, o conteúdo do documento precisa respeitar os pressupostos de validade exigidos pelo ordenamento jurídi- co. Isso reforça a necessidade de compreensão de que a assinatura digital qualificada atesta a autoria e a integridade do documento, mas não sana eventuais vícios de consentimento, ilici- tude da causa ou ausência de forma legal. O valor da prova, portanto, deve ser analisado em sua totalidade (Cabral, 2022).

Nesse novo ecossistema probatório, o processo judicial passa a depender não apenas da interpretação jurídica, mas também da análise técnico-digital dos elementos apresentados. O juiz moderno precisa estar capacitado a compreender

os metadados da certificação digital, os selos de verificação, a cadeia de confiança e os registros das autoridades certificadoras. Es- sa interdisciplinaridade entre direito e tecnologia é o que garante a plena aplicação dos princí- pios da legalidade, segurança e eficiência na produção e na valoração da prova documental eletrônica (Lima, 2015).

A validade da assinatura eletrônica tem sido reafirmada nos tribunais superiores brasi- leiros, especialmente após a regulamentação da Medida Provisória nº 2.200-2/2001, que insti- tuiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Em decisões do Superior Tri- bunal de Justiça (STJ), ficou consolidado que a assinatura digital realizada com a certificação ICP-Brasil tem a mesma validade jurídica da assinatura manuscrita, conforme observa o arti- go 10 da Lei nº 14.063/2020. O STJ, em julgamento recente, declarou que "a assinatura digi- tal, quando realizada com o uso do certificado ICP-Brasil, goza de presunção de autenticida- de, sendo válida como meio de prova no processo judicial" (Brasil, 2021).

O Tribunal de Justiça de São Paulo, por sua vez, em decisão de 2020, também ali- nhou-se a essa compreensão, confirmando que a assinatura digital qualificada, quando emitida com o certificado ICP-Brasil, oferece a garantia da autenticidade e da integridade do docu- mento eletrônico, refletindo as disposições legais. A Corte paulista salientou que documentos apresentados com assinaturas digitais sem a devida certificação ICP-Brasil não possuem a ro- bustez necessária para a sua aceitação como prova, uma vez que não garantem a autenticidade do signatário (Brasil, 2020).

Apesar do reconhecimento amplo da validade da assinatura digital, há casos em que o tribunal se depara com falhas no processo de certificação ou na manipulação do arquivo ele- trônico. O Tribunal Regional Federal da 1ª Região (TRF-1) foi enfático ao afirmar que "a as- sinatura digital sem a certificação adequada, emitida por autoridade certificadora vinculada à ICP-Brasil, não possui o valor jurídico esperado, sendo ineficaz para fins probatórios, já que não garante a autenticidade e a integridade do documento" (Brasil, 2020).

Em outro caso, o Tribunal de Justiça do Estado de Minas Gerais (TJMG) rejeitou a va- lidade de uma assinatura digital, citando a ausência de verificação de integridade do docu- mento eletrônico. A Corte mineira destacou que a falta de verificação da autenticidade do do- cumento, especialmente em sua integridade, torna a assinatura digital inapta para ser conside- rada como prova em juízo (Brasil, 2020). Este entendimento revela que, para que a assinatura digital seja reconhecida como válida, é fundamental que o processo de certificação siga os re- quisitos técnicos legais estabelecidos.

Além disso, a manipulação do conteúdo do documento após a assinatura digital tam- bém foi apontada como um fator que compromete a validade do ato

processual. O Tribunal de Justiça do Rio Grande do Sul, em 2021, determinou que qualquer alteração no conteúdo do arquivo digital após a assinatura compromete a sua autenticidade, tornando-o inválido como prova no processo (Brasil, 2021). Esse entendimento reforça a importância de manter a inte- gridade do documento eletrônico após sua assinatura para garantir a validade jurídica do ato.

Em relação à utilização de assinaturas digitais sem a cadeia de certificação correta, o Tribunal Regional Federal da 4ª Região (TRF-4) também se posicionou de forma rigorosa, considerando que qualquer falha no processo de certificação digital compromete a validade do documento, não podendo este ser utilizado como prova no processo (Brasil, 2020). A decisão reafirma a necessidade de que a assinatura digital esteja devidamente acompanhada da verifi- cação da autenticidade e integridade do documento eletrônico.

Ademais, o TRF-1, ao lidar com um caso envolvendo a manipulação do arquivo ele- trônico após a assinatura, decidiu que "a alteração do conteúdo digital após a assinatura com- promete a autenticidade e, por conseguinte, a validade do ato processual" (BRASIL, 2020). Esse posicionamento é claro no sentido de que a assinatura digital, se manipulada ou alterada, perde sua validade, afetando a integridade do ato jurídico.

Em 2022, o Superior Tribunal de Justiça reiterou que a assinatura digital qualificada, quando realizada por meio de autoridade certificadora vinculada à ICP-Brasil, possui presun- ção de veracidade. A decisão no REsp 1.597.560/SC, relatada pelo Min. Paulo de Tarso San- severino, foi enfática: "não basta a assinatura digital para garantir a validade do documento; é necessário que ele esteja acompanhado de elementos técnicos que comprovem sua autentici- dade, como o vínculo com a ICP-Brasil e a correta emissão do certificado" (Brasil, 2022).

Além disso, o Tribunal de Justiça de São Paulo, em sua análise, destacou que "para que um documento eletrônico tenha valor probatório, ele deve ser acompanhado de metadados que comprovem a integridade e autenticidade do arquivo assinado" (Brasil, 2021). Este enten- dimento evidencia a importância dos metadados no processo de validação da assinatura digi- tal, sendo um elemento essencial para garantir a confiabilidade do documento no contexto ju- dicial.

A validade das assinaturas digitais no processo judicial tem sido constantemente rea- firmada pela jurisprudência dos tribunais brasileiros. O Superior Tribunal de Justiça (STJ), em diversas decisões, tem consolidado que a assinatura digital, quando realizada com o uso de certificado ICP-Brasil, goza de presunção de autenticidade, garantindo validade jurídica ple- na, conforme estabelecido na Lei nº 14.063/2020. O STJ, em julgamento recente, declarou que a assinatura digital, quando realizada com o uso do certificado ICP-Brasil, goza de pre- sunção de autenticidade, sendo

válida como meio de prova no processo judicial (Brasil, 2021). Esse entendimento reflete a segurança e confiabilidade do processo de certificação di- gital, que garante a autenticidade de documentos em transações digitais.

Entretanto, a assinatura digital, apesar de ser amplamente reconhecida como válida, pode ser contestada quando não observados os requisitos técnicos essenciais para a sua vali- dação. O Tribunal de Justiça de São Paulo, por exemplo, rejeitou uma assinatura digital em 2020, alegando que documentos apresentados com assinaturas digitais sem a devida certifica- ção ICP-Brasil não possuem a robustez necessária para a sua aceitação como prova, uma vez que não garantem a autenticidade do signatário (Brasil, 2020). Esse posicionamento reforça a necessidade de seguir os padrões exigidos pela legislação brasileira para assegurar a veracida- de dos documentos eletrônicos.

Em outros casos, o Tribunal Regional Federal da 1ª Região (TRF-1) também destacou que a assinatura digital sem a certificação adequada, emitida por autoridade certificadora vin- culada à ICP-Brasil, não possui o valor jurídico esperado, sendo ineficaz para fins probató- rios, já que não garante a autenticidade e a integridade do documento (Brasil, 2020). A juris- prudência nacional é clara ao indicar que a assinatura digital, para ser válida, deve atender a todos os requisitos técnicos previstos nas normas de certificação digital, especialmente os de- finidos pela ICP-Brasil, que garantem a integridade e a segurança do conteúdo do documento. Em relação à manipulação de documentos após a assinatura digital, o Tribunal de Jus-

tiça do Rio Grande do Sul, em 2021, foi enfático ao afirmar que "qualquer alteração no conte- údo do arquivo digital após a assinatura compromete a autenticidade e, por conseguinte, a va- lidade do ato processual" (Brasil, 2021). Esse entendimento se alinha com as normas interna- cionais de segurança, que exigem que os documentos assinados digitalmente permaneçam in- tactos, sem alterações, para que mantenham sua validade jurídica. A integridade do arquivo é um elemento essencial para garantir a autenticidade do ato processual e a segurança jurídica da assinatura digital.

Além disso, o Tribunal Regional Federal da 2ª Região (TRF-2), em outra decisão, des- tacou que qualquer falha no processo de certificação digital compromete a validade do docu- mento, não podendo ser utilizado como prova no processo (Brasil, 2020). Isso evidencia que a assinatura digital, quando não acompanhada dos elementos técnicos necessários, não é suficiente para garantir a autenticidade de um documento, especialmente quando o processo de cer- tificação não segue as diretrizes estabelecidas pela ICP-Brasil.

Em 2022, o STJ reiterou sua posição sobre a validade da assinatura digital qualificada, quando realizada corretamente com o certificado ICP-Brasil, afirmando

que não basta a assi- natura digital para garantir a validade do documento; é necessário que ele esteja acompanhado de elementos técnicos que comprovem sua autenticidade, como o vínculo com a ICP-Brasil e a correta emissão do certificado (Brasil, 2022). Esse julgamento reflete a exigência da obser- vância dos processos de certificação como condição para a plena validade da assinatura digi- tal, assegurando a autenticidade e a integridade do documento eletrônico.

Por outro lado, o Tribunal de Justiça de São Paulo, ao analisar a validade de um do- cumento assinado digitalmente, destacou que "para que um documento eletrônico tenha valor probatório, ele deve ser acompanhado de metadados que comprovem sua autenticidade e inte- gridade" (Brasil, 2021). A decisão sublinha a importância dos metadados como um compo- nente essencial para garantir que o documento assinado digitalmente seja verdadeiro e não te- nha sido alterado, oferecendo mais segurança jurídica ao processo.

Esse entendimento é reforçado pelo Tribunal de Justiça do Estado de Goiás, que, ao rejeitar uma assinatura digital em um caso específico, afirmou que a modificação no conteúdo de um documento eletrônico, após sua assinatura, acarreta na perda da validade da assinatura digital, resultando na invalidez do ato processual (Brasil, 2021). A jurisprudência dos tribu- nais superiores é clara ao vincular a validade da assinatura digital à integridade do documento assinado, sendo necessária a manutenção dos seus dados inalterados para garantir a veracida- de do ato processual.

A jurisprudência também tem abordado a questão da manipulação de metadados, que são essenciais para a verificação da autenticidade dos documentos assinados digitalmente. O Tribunal de Justiça de São Paulo, ao considerar um caso de manipulação dos metadados, rei- terou que a manipulação ou alteração dos metadados do documento digital compromete sua validade, tornando-o inapto para ser aceito como prova (Brasil, 2021). A integridade dos me- tadados é, portanto, um dos elementos fundamentais para garantir a autenticidade e a validade do documento assinado digitalmente, funcionando como um mecanismo de verificação do ato jurídico.

Essas decisões demonstram que a assinatura digital, embora amplamente aceita e regu- lamentada, deve ser acompanhada de uma série de requisitos técnicos para garantir sua vali- dade jurídica no processo judicial. A confiabilidade do processo de certificação digital é fun- damental para a proteção contra fraudes e manipulação de documentos, e a jurisprudência tem sido enfática em garantir que esses requisitos sejam cumpridos rigorosamente. Em resumo, a assinatura digital qualificada, quando devidamente certificada pela ICP-Brasil, oferece a segu- rança necessária para sua aceitação como meio de prova no processo judicial, desde que aten- didos todos os requisitos legais e técnicos estabelecidos.

A importância da perícia digital na análise dos metadados é reforçada no contexto jurídico, pois é por meio desses dados que se pode confirmar a autenticidade de documentos assinados digitalmente. A perícia digital atua como um dos principais instrumentos para detectar fraudes, manipulação de arquivos e garantir que o conteúdo do documento seja autêntico. A análise dos metadados permite que o especialista determine, por exemplo, a data de criação, alteração e a plataforma utilizada, além de evidenciar se o documento foi alterado após a assinatura digital (Lima, 2015). Portanto, os metadados fornecem uma prova robusta da integridade do documento em processos judiciais, onde a credibilidade dos documentos apresentados é essencial para a decisão judicial.

A perícia digital desempenha um papel fundamental, não apenas na verificação dos documentos, mas também no esclarecimento das circunstâncias em que o documento foi cria- do, assinado e transmitido. Como afirma o Tribunal de Justiça de São Paulo, "os metadados fornecem uma verificação essencial, pois possibilitam a rastreabilidade e confirmam a auten- ticidade de documentos eletrônicos, sendo parte integrante da análise forense" (Brasil, 2021). Esta afirmação é reforçada pela análise forense, que busca verificar a integridade de docu- mentos eletrônicos, considerando que qualquer alteração nos metadados pode comprometer a validade jurídica do documento no processo judicial.

Além disso, a perícia forense se apoia não só na análise dos metadados mas também em tecnologias avançadas para garantir a autenticidade dos documentos digitais. A utilização de plataformas como Datacertify tem se mostrado essencial, uma vez que essas ferramentas oferecem uma visão detalhada sobre os metadados de documentos, incluindo o histórico de al- terações e as assinaturas digitais realizadas. O uso dessas plataformas facilita a comprovação da identidade do signatário e a confirmação da integração do conteúdo do arquivo, sem que tenha havido qualquer alteração fraudulenta (Just Arb, 2023). Essa análise detalhada é funda- mental para garantir a segurança jurídica das transações realizadas de forma digital.

É importante notar que, apesar das ferramentas de análise digital e da tecnologia de metadados, existem casos em que a validade da assinatura digital pode ser questionada em virtude de manipulação de arquivos ou ausência de certificado digital. A perícia digital deve ser realizada de maneira criteriosa para identificar esses fatores e garantir que o documento, em sua totalidade, tenha sido assinado de acordo com os requisitos legais. A recusa de assinatura digital em alguns tribunais tem ocorrido devido à ausência do certificado digital ICP- Brasil, essencial para garantir a autenticidade do documento no contexto jurídico, conforme estabelecido pela Lei 14.063/2020 (Brasil, 2020).

O uso de metadados digitais como apoio à validade documental tem mostrado grande importância no processo judicial. Em várias decisões judiciais, o tribunal se apoia na análise pericial dos metadados para confirmar a integridade do conteúdo e garantir que não houve manipulação do documento. Em uma decisão recente, o STJ reconheceu a validade de um do- cumento assinado digitalmente, em que os metadados indicaram que o documento foi gerado e assinado dentro do prazo estipulado pelas partes envolvidas. Isso demonstra que a perícia digital não se limita apenas à verificação da assinatura, mas também à rastreabilidade dos da- dos, comprovando que o documento não foi alterado após a assinatura (Brasil, 2021).

Em contrapartida, a recusa de documentos digitais também tem sido um tema discuti- do nos tribunais, principalmente quando se verificam falhas na certificação digital ou ausência de metadados válidos. O Tribunal de Justiça de São Paulo rejeitou recentemente um docu- mento em que o metadado não indicava uma assinatura válida, mesmo que o signatário tivesse declarado ter assinado o documento. A decisão foi fundamentada na ausência de metadados compatíveis com a assinatura, invalidando assim o documento para efeitos processuais (Bra- sil, 2020). Esse tipo de situação mostra como a análise dos metadados pode ser determinante para a validade jurídica de documentos eletrônicos.

A perícia digital, ao avaliar os metadados, tem um papel essencial na autenticação de documentos digitais apresentados como prova no processo judicial. A análise de dados como data de assinatura, alterações realizadas e identificação do signatário são essenciais para ga- rantir que o documento não tenha sido manipulado. Segundo a Lei 14.063/2020, os documen- tos assinados com certificados digitais qualificados, emitidos pela ICP-Brasil, possuem uma presunção de autenticidade, que pode ser verificada pelos metadados contidos no arquivo di- gital (Brasil, 2020). A análise desses dados confirma a legitimidade do documento, permitin- do sua aceitação como prova no processo.

Além disso, a utilização dos metadados pode ser determinante também na verificação de documentos falsificados ou alterados de alguma forma. A ausência de assinatura válida ou modificação nos metadados pode comprometer o valor jurídico do documento, tornando-o inapto para uso em processos judiciais. A recusa a documentos em que se verificou alteração nos metadados tem sido frequente nos tribunais, especialmente quando os dados contidos no arquivo contradizem as alegações da parte que apresentou o documento (Sendin, 2017). Isso reforça a importância da análise detalhada dos metadados durante a perícia digital.

No contexto das plataformas digitais de auditoria, sites como Datacertify desempe- nham um papel crucial na verificação da autenticidade dos metadados. A ferramenta oferece uma análise detalhada de documentos eletrônicos, permitindo

que os peritos confirmem se o documento foi assinado digitalmente e se seus metadados correspondem às informações pre- sentes na assinatura. A plataforma fornece um laudo técnico que detalha as informações de criação, modificação e a presença da assinatura digital, validando ou invalidando o documen- to para efeitos legais (Datacertify, 2022).

Além disso, a plataforma Just Arb também se destaca ao permitir a verificação dos metadados de documentos eletrônicos. A utilização dessas plataformas oferece um suporte robusto para a perícia digital, permitindo que os peritos possam realizar uma análise detalhada do documento, determinando sua autenticidade e verificando se o conteúdo permanece inalte- rado após a assinatura. Essas ferramentas digitais são indispensáveis para a análise de docu- mentos em um processo judicial, pois fornecem uma evidência confiável que pode ser utiliza- da como prova (Just Arb, 2023).

CONCLUSÃO

A presente pesquisa demonstrou que as assinaturas eletrônicas, especialmente a assi- natura digital qualificada vinculada à ICP-Brasil, possuem plena validade jurídica no ordena- mento jurídico brasileiro, equiparando-se à assinatura manuscrita para todos os fins legais, in- clusive probatórios. A construção normativa iniciada com a Medida Provisória nº 2.200- 2/2001, e posteriormente aprimorada pela Lei nº 12.965/2014 e pela Lei nº 14.063/2020, esta- belece um marco seguro e eficiente para a autenticação de documentos digitais, contribuindo para a desmaterialização dos atos jurídicos e para a modernização das relações processuais e contratuais.

Ao longo do trabalho, observou-se que a assinatura digital qualificada, por sua estrutu- ra baseada em criptografia assimétrica e certificação emitida por autoridade reconhecida, sa- tisfaz plenamente os requisitos de autenticidade, integridade e não repúdio. Tal robustez téc- nica confere-lhe presunção legal de veracidade, reconhecida pela jurisprudência dos tribunais superiores, como o Superior Tribunal de Justiça e diversos Tribunais Regionais Federais, que validam seu uso como prova plena no processo judicial. A legislação brasileira, portanto, ali- nha-se aos padrões internacionais mais rigorosos em termos de segurança cibernética e vali- dade probatória.

Por outro lado, ficou evidenciado que a validade da assinatura eletrônica depende não apenas da existência de um marco normativo, mas também da observância rigorosa dos requi- sitos técnicos, como a correta emissão do certificado digital, a integridade dos metadados e a ausência de manipulação posterior do documento. A inobservância desses critérios pode tor- nar o documento digital inválido ou ineficaz, exigindo do operador jurídico domínio técnico sobre a certificação digital

e as ferramentas de auditoria digital, como o uso de plataformas de verificação como Datacertify e Just Arb.

A pesquisa também revelou desafios persistentes quanto à disseminação do conheci- mento técnico e jurídico necessário à adequada utilização das assinaturas digitais. A resistên- cia cultural de operadores do direito e instituições públicas à adoção plena desses instrumen- tos, muitas vezes motivada por desconhecimento ou insegurança jurídica, limita o potencial transformador da certificação digital no Brasil. Torna-se, assim, fundamental a ampliação de programas de capacitação e a inserção desses conteúdos nos currículos da graduação em Di- reito e áreas afins.

Ademais, a análise jurisprudencial evidenciou que há uma hierarquia entre os tipos de assinaturas eletrônicas — simples, avançada e qualificada — sendo esta última a única dotada de presunção legal plena de validade, conforme previsto na legislação vigente. A assinatura simples, embora admissível em determinados contextos, carece de segurança jurídica sufici- ente para atos de maior complexidade, sendo suscetível à impugnação e exigindo produção de prova complementar. Já a assinatura qualificada, por atender aos mais altos padrões de auten- ticidade, deve ser preferida nas relações contratuais e processuais de maior relevância.

Conclui-se, portanto, que a validade jurídica das assinaturas eletrônicas não é uma questão meramente normativa, mas envolve uma complexa articulação entre direito, tecnolo- gia e cultura institucional. A consolidação da assinatura digital como meio legítimo de mani- festação de vontade e de prova documental demanda não apenas a existência de leis claras, mas também sua aplicação efetiva, o fortalecimento das instituições certificadoras e o aprimo- ramento técnico dos operadores do direito. Trata-se de um caminho sem retorno rumo à digi- talização segura, transparente e eficaz das relações jurídicas no século XXI.

REFERÊNCIAS

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2014/lei/l12965.htm. Acesso em: 15 mar. 2025.

BRASIL. Lei nº 14.063, de 23 de setembro de 2020. Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde; altera as Leis nº 12.682, de 9 de julho de 2012, e nº 13.989, de 15 de abril de 2020; e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 2, 24 set. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14063.htm. Acesso em: 15 mar. 2025.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 3, 27 ago. 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/2200-2.htm. Acesso em: 15 mar. 2025.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.495.920/MG. Relatora: Ministra Maria Isabel Gallotti. Terceira Turma. Julgado em: 23 ago. 2018. Disponível em: https://processo.stj.jus.br. Acesso em: 08 abr. 2025.

CABRAL, Antonio do Passo. A prova eletrônica no processo civil brasileiro: validade, eficácia e limites. Revista Brasileira de Direito Processual, v. 121, p. 63-89, jan./mar. 2022. Disponível em: https://www.editoraforum.com.br/revistas. Acesso em: 08 abr. 2025.

DATACERTIFY. A validade jurídica das assinaturas eletrônicas à luz da jurisprudência brasileira. Blog Datacertify, 2023. Disponível em: https://www.datacertify.com.br/jurisprudencia-assinaturas-eletronicas. Acesso em: 08 abr. 2025.

DATACERTIFY. Por que os metadados são importantes? DataCertify, 2022. Disponível em: https://www.datacertify.com.br/metadados-e-a-jurisprudencia/. Acesso em: 7 mar. 2025.

JUST ARB. A importância dos metadados na coleta de provas digitais. Just Arbitration, 30 set. 2023. Disponível em: https://justarbitration.com.br/2023/09/30/a-importancia-dos-metadados. Acesso em: 08 abr. 2025.

JUST ARB. A importância dos metadados e códigos fontes na coleta de provas digitais. Just Arbitration, 2023. Disponível em: https://justarbitration.com.br/2023/09/30/a-importancia-dos-metadados-e-codigos-na-coleta-de-provas-digitais/. Acesso em: 7 mar. 2025.

LIMA, José Paulo da Silva. Validação de dados através de hashes criptográficos: uma avaliação na perícia forense computacional brasileira. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Pernambuco, Recife, 2015. Disponível em: https://repositorio.ufpe.br/handle/123456789/15966. Acesso em: 7 mar. 2025.

MACHADO, Robson Carvalho. Certificação digital: os caminhos do documento eletrônico no Brasil. São Paulo: Biblioteca de Segurança, 2020. Disponível em: https://www.bibliotecadeseguranca.com.br/livros/certificacao-digital-os-caminhos-do- documento-eletronico-no-brasil/. Acesso em: 7 mar. 2025.

MONTEIRO, Emiliano S.; MIGNONI, Maria Eloisa. Certificados digitais: conceitos e práticas. Rio de Janeiro: Brasport, 2018. Disponível em: https://www.editorabrasport.com.br/certificados-

digitais-conceitos-e-praticas. Acesso em: 7 mar. 2025.

OKANO, Gabriel Hirofumi; ALCÂNTARA, Gabriel Barbosa. Conceitos básicos de criptografia. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade Federal de Mato Grosso do Sul, Campo Grande, 2018. Disponível em: https://repositorio.ufms.br/handle/123456789/7855. Acesso em: 7 mar. 2025.

SENDIN, Ivan da Silva. Funções de hashing criptográficas. Dissertação (Mestrado em Ciência da Computação) – Universidade Estadual de Campinas, Campinas, 2017. Disponível em: https://repositorio.unicamp.br/acervo/detalhe/175415. Acesso em: 7 mar. 2025.

SILVA, Daniel Amorim Assumpção Neves. Manual de Direito Processual Civil. 14. ed. Salvador: Juspodivm, 2023.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO (TJSP). Apelação Cível nº 100XXXX- 00.2020.8.26.0100. Relator: Des. Carlos Abrão. Julgado em: 15 set. 2022. Disponível em: https://esaj.tjsp.jus.br. Acesso em: 08 abr. 2025.