



SUPERIOR TRIBUNAL DE JUSTIÇA

RECURSO ESPECIAL Nº 2150278 - PR (2024/0212892-1)

RELATORA : **MINISTRA NANCY ANDRIGHI**
RECORRENTE : COOPERATIVA DE CREDITO DE LIVRE ADMISSAO TRES FRONTEIRAS -
SICOOB TRES FRONTEIRAS
ADVOGADOS : MARCELO RICARDO URIZZI DE BRITO ALMEIDA - PR030715
ALESSANDRA CELANT - PR057984
RECORRIDO : RHL LTDA
RECORRIDO : HELOISA CEZARINO MARTINS
RECORRIDO : RODRIGO BIANCO
ADVOGADO : ROMANO CAPPONI JÚNIOR - PR058481

EMENTA

RECURSO ESPECIAL. PROCESSUAL CIVIL. AÇÃO DE EXECUÇÃO DE TÍTULO EXTRAJUDICIAL. INDEFERIMENTO INICIAL. EXTINÇÃO. CÉDULA DE CRÉDITO BANCÁRIA. 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 PROBANTE. IMPUGNAÇÃO. ÔNUS DAS PARTES. ATOS ENTRE PARTICULARES E ATOS PROCESSUAIS EM MEIO ELETRÔNICO. NÍVEIS DE AUTENTICAÇÃO. DISTINÇÃO. CONSTITUIÇÃO E ATESTE DE TÍTULOS EXECUTIVOS EXTRAJUDICIAIS EM MEIO ELETRÔNICO.

1. Ação de execução de título extrajudicial, ajuizada em 23/03/2022, da qual foi extraído o presente recurso especial, interposto em 06/02/2024 e concluso ao gabinete em 19/06/2024.

2. O propósito recursal consiste em saber se as normas que regem o processo eletrônico exigem o uso exclusivo de certificação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), para fins de conferir autenticidade aos documentos produzidos e assinados eletronicamente entre as partes em momento pré-processual. Interpretação dos arts. 10, § 2º, da MPV 2200/2001 e 784, § 4º, do CPC.

3. A intenção do legislador foi de 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, levando em consideração a autonomia privada e a liberdade das formas de declaração de vontades entre os particulares.

4. 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. Precedentes.

5. O controle de autenticidade (i.e., a garantia de que a pessoa quem 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 (v.g., "login", senha, códigos enviados por mensagens eletrônicas instantâneas ou gerados por aplicativos, leitura biométrica facial, papiloscópica, etc.).

6. O controle de integridade (i.e., a garantia de que a assinatura ou o conteúdo do documento não foram modificados no trajeto entre a emissão, validação, envio e recebimento pelo destinatário) é feito por uma fórmula matemática (algoritmo) que cria uma "impressão digital virtual" cuja singularidade é garantida com o uso de criptografia, sendo a função criptográfica "hash" SHA-256 um dos padrões mais utilizados na área de segurança da informação por permitir detecção de adulteração mais eficiente, a exemplo do denominado "efeito avalanche".

7. 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 (Sisbr/Sicoop), tendo o Tribunal de Origem considerado a assinatura eletrônica em modalidade avançada incompatível com a exigência do uso de certificado digital no sistema ICP-Brasil para prática de atos processuais no âmbito do processo judicial eletrônico apesar de constar múltiplos fatores de autenticação, constantes do relatório de assinaturas eletrônicas gerado na emissão dos documentos em momento pré-processual.

8. A refutação da veracidade da assinatura eletrônica e dos documentos sobre os quais elas foram eletronicamente apostas - seja no aspecto de sua integridade, seja no aspecto de sua autoria - deve ser feita por aquele a quem a norma do art. 10, § 2º, da MPV 20200/2001 expressamente se dirigiu, que é a "pessoa a quem for oposto o documento", que é a mesma pessoa que admite o documento como válido (i.e., o destinatário). Essa é, aliás, a norma do art. 411, I, do CPC, ao criar a presunção de autenticidade do documento particular quando a parte contra quem ele for produzido deixar de impugná-lo.

9. A pessoa a quem o legislador refere é uma das partes na relação processual (no caso de execução de título de crédito, o emitente e seus avalistas), o que - por definição - exclui a pessoa do juiz, sob pena de se incorrer no tratamento desigualitário, vetado pela norma do art. 139, I, do CPC.

10. 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.

11. Negar validade jurídica a um título de crédito, emitido e assinado de forma eletrônica, simplesmente pelo fato de a autenticação da assinatura e da integridade documental ter sido feita por uma entidade sem credenciamento no sistema ICP-Brasil seria o mesmo que negar validade

jurídica a um cheque emitido pelo portador e cuja firma não foi reconhecida em cartório por autenticidade, evidenciando um excessivo formalismo diante da nova realidade do mundo virtual.

12. Os níveis de autenticação dos documentos e assinaturas dos atos pré-processuais, praticados entre particulares em meio eletrônico, não se confundem com o nível de autenticação digital, exigido para a prática de atos processuais.

13. A Lei 14620/2023, ao acrescentar o § 4º ao art. 784 do CPC, passou a admitir - na constituição e ateste de títulos executivos extrajudiciais em meio eletrônico - qualquer modalidade de assinatura eletrônica desde que sua integridade seja conferida pela entidade provedora desse serviço, evidenciando a ausência de exclusividade da certificação digital do sistema ICP-Brasil.

14. Recurso especial conhecido e provido para determinar a devolução dos autos à origem a fim de que se processe a ação de execução de título extrajudicial.

ACÓRDÃO

Vistos e relatados estes autos em que são partes as acima indicadas, acordam os Ministros da TERCEIRA TURMA, por unanimidade, conhecer do recurso especial e lhe dar provimento, com majoração de honorários, nos termos do voto da Sra. Ministra Relatora.

Os Srs. Ministros Humberto Martins (Presidente), Ricardo Villas Bôas Cueva, Marco Aurélio Bellizze e Moura Ribeiro votaram com a Sra. Ministra Relatora.

Brasília, 24 de setembro de 2024.

MINISTRA NANCY ANDRIGHI
Relatora



SUPERIOR TRIBUNAL DE JUSTIÇA

RECURSO ESPECIAL Nº 2150278 - PR (2024/0212892-1)

RELATORA : **MINISTRA NANCY ANDRIGHI**
RECORRENTE : COOPERATIVA DE CREDITO DE LIVRE ADMISSAO TRES FRONTEIRAS -
SICOOB TRES FRONTEIRAS
ADVOGADOS : MARCELO RICARDO URIZZI DE BRITO ALMEIDA - PR030715
ALESSANDRA CELANT - PR057984
RECORRIDO : RHL LTDA
RECORRIDO : HELOISA CEZARINO MARTINS
RECORRIDO : RODRIGO BIANCO
ADVOGADO : ROMANO CAPPONI JÚNIOR - PR058481

EMENTA

RECURSO ESPECIAL. PROCESSUAL CIVIL. AÇÃO DE EXECUÇÃO DE TÍTULO EXTRAJUDICIAL. INDEFERIMENTO INICIAL. EXTINÇÃO. CÉDULA DE CRÉDITO BANCÁRIA. 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 PROBANTE. IMPUGNAÇÃO. ÔNUS DAS PARTES. ATOS ENTRE PARTICULARES E ATOS PROCESSUAIS EM MEIO ELETRÔNICO. NÍVEIS DE AUTENTICAÇÃO. DISTINÇÃO. CONSTITUIÇÃO E ATESTE DE TÍTULOS EXECUTIVOS EXTRAJUDICIAIS EM MEIO ELETRÔNICO.

1. Ação de execução de título extrajudicial, ajuizada em 23/03/2022, da qual foi extraído o presente recurso especial, interposto em 06/02/2024 e concluso ao gabinete em 19/06/2024.

2. O propósito recursal consiste em saber se as normas que regem o processo eletrônico exigem o uso exclusivo de certificação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), para fins de conferir autenticidade aos documentos produzidos e assinados eletronicamente entre as partes em momento pré-processual. Interpretação dos arts. 10, § 2º, da MPV 2200/2001 e 784, § 4º, do CPC.

3. A intenção do legislador foi de 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, levando em consideração a autonomia privada e a liberdade das formas de declaração de vontades entre os particulares.

4. 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. Precedentes.

5. O controle de autenticidade (i.e., a garantia de que a pessoa quem 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 (v.g., "login", senha, códigos enviados por mensagens eletrônicas instantâneas ou gerados por aplicativos, leitura biométrica facial, papiloscópica, etc.).

6. O controle de integridade (i.e., a garantia de que a assinatura ou o conteúdo do documento não foram modificados no trajeto entre a emissão, validação, envio e recebimento pelo destinatário) é feito por uma fórmula matemática (algoritmo) que cria uma "impressão digital virtual" cuja singularidade é garantida com o uso de criptografia, sendo a função criptográfica "hash" SHA-256 um dos padrões mais utilizados na área de segurança da informação por permitir detecção de adulteração mais eficiente, a exemplo do denominado "efeito avalanche".

7. 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 (Sisbr/Sicoop), tendo o Tribunal de Origem considerado a assinatura eletrônica em modalidade avançada incompatível com a exigência do uso de certificado digital no sistema ICP-Brasil para prática de atos processuais no âmbito do processo judicial eletrônico apesar de constar múltiplos fatores de autenticação, constantes do relatório de assinaturas eletrônicas gerado na emissão dos documentos em momento pré-processual.

8. A refutação da veracidade da assinatura eletrônica e dos documentos sobre os quais elas foram eletronicamente apostas - seja no aspecto de sua integridade, seja no aspecto de sua autoria - deve ser feita por aquele a quem a norma do art. 10, § 2º, da MPV 20200/2001 expressamente se dirigiu, que é a "pessoa a quem for oposto o documento", que é a mesma pessoa que admite o documento como válido (i.e., o destinatário). Essa é, aliás, a norma do art. 411, I, do CPC, ao criar a presunção de autenticidade do documento particular quando a parte contra quem ele for produzido deixar de impugná-lo.

9. A pessoa a quem o legislador refere é uma das partes na relação processual (no caso de execução de título de crédito, o emitente e seus avalistas), o que - por definição - exclui a pessoa do juiz, sob pena de se incorrer no tratamento desigualitário, vetado pela norma do art. 139, I, do CPC.

10. 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.

11. Negar validade jurídica a um título de crédito, emitido e assinado de forma eletrônica, simplesmente pelo fato de a autenticação da assinatura e da integridade documental ter sido feita por uma entidade sem credenciamento no sistema ICP-Brasil seria o mesmo que negar validade

jurídica a um cheque emitido pelo portador e cuja firma não foi reconhecida em cartório por autenticidade, evidenciando um excessivo formalismo diante da nova realidade do mundo virtual.

12. Os níveis de autenticação dos documentos e assinaturas dos atos pré-processuais, praticados entre particulares em meio eletrônico, não se confundem com o nível de autenticação digital, exigido para a prática de atos processuais.

13. A Lei 14620/2023, ao acrescentar o § 4º ao art. 784 do CPC, passou a admitir - na constituição e ateste de títulos executivos extrajudiciais em meio eletrônico - qualquer modalidade de assinatura eletrônica desde que sua integridade seja conferida pela entidade provedora desse serviço, evidenciando a ausência de exclusividade da certificação digital do sistema ICP-Brasil.

14. Recurso especial conhecido e provido para determinar a devolução dos autos à origem a fim de que se processe a ação de execução de título extrajudicial.

RELATÓRIO

Cuida-se de recurso especial interposto por COOPERATIVA DE CREDITO DE LIVRE ADMISSAO TRES FRONTEIRAS - SICOOB TRES FRONTEIRAS, fundamentado nas alíneas "a" e "c" do permissivo constitucional.

Recurso especial interposto em: 06/02/2024.

Concluso para o gabinete em: 19/06/2024.

Ação: de execução de título extrajudicial, ajuizada em 23/03/2022 por COOPERATIVA DE CREDITO DE LIVRE ADMISSAO TRES FRONTEIRAS - SICOOB TRES FRONTEIRAS em desfavor da devedora principal RHL LTDA, bem como de seus avalistas HELOISA CEZARINO MARTINS e RODRIGO BIANCO, decorrente de dívida fundada em Cédula de Crédito Bancário, documentada e assinada eletronicamente pela plataforma Sisbr/Sicoob.

Decisão: após oportunizar emenda à inicial para a autora "esclarecer e comprovar, que os registros apresentados como assinaturas têm validade jurídica para fins processuais, em conformidade com a exigência prevista na Lei do Processo Eletrônico e validado pelo sistema IPC-BRASIL (sic) - Infraestrutura de Chaves Públicas Brasileira" (e-STJ fl. 102), tendo a autora juntado o relatório de validação das mesmas no âmbito da plataforma de sua propriedade e desenvolvimento, o Juiz de 1º Grau indeferiu a inicial e extinguiu o processo sem

resolução do mérito sob fundamento de que "a parte não demonstrou a validade da assinatura para fins processuais, em conformidade com a exigência prevista na Lei do Processo Eletrônico, não demonstrando o credenciamento da Autoridade Certificadora" (e-STJ fls. 112-116).

Acórdão: negou provimento à apelação, nos termos da seguinte ementa:

APELAÇÃO CÍVEL. AÇÃO DE EXECUÇÃO DE TÍTULO EXTRAJUDICIAL. CÉDULA DE CRÉDITO BANCÁRIO. TÍTULO ASSINADO ELETRONICAMENTE POR MEIO DE PLATAFORMA PRIVADA NÃO CADASTRADA NO ICP-BRASIL. ART. 1º, §2º, III, DA LEI N.º 11.419/2006. AUTENTICIDADE DA ASSINATURA. VERIFICAÇÃO. IMPOSSIBILIDADE. EXTINÇÃO DA EXECUÇÃO. MANUTENÇÃO.

1. Nos termos dos precedentes desta Corte, não é possível a execução de cédula de crédito bancário assinada eletronicamente por meio de plataforma privada não cadastrada no ICP – BRASIL.

2. Apelação cível conhecida e não provida. (e-STJ fl. 397)

Embargos de declaração: foram rejeitados com prequestionamento do art. 784, § 4º, do CPC (e-STJ fl. 416).

Recurso especial: aduz dissídio e violação aos arts. 10, § 2º, da MPV 2200/2001, 11 da Lei 11419/2006 e 784, § 4º, do CPC.

Informa que a execução tem como objeto Cédula de Crédito Bancário decorrente de renegociação de dívida no valor de R\$ 57.963,11 (cinquenta e sete mil, novecentos e sessenta e três reais e onze centavos), tendo a cártula sido assinada digitalmente pelas partes pelo método de validação contratualmente eleito e admitido como válido por elas, o qual consiste em uso de "login" e senha, possibilitando verificação da identidade pelos nomes dos signatários, especificação do IP, carimbos de hora ("time stamps") e código "hash" que garante a cadeia de custódia documental.

Ressalta que a validação das assinaturas foi feita por meio da plataforma Sisbr/Sicoob (Plataforma de Serviços Financeiros do Sicoob).

Entende que os documentos produzidos na forma eletrônica quando juntados ao processo eletrônico com garantia de origem e de identificação de seus signatários devem ser considerados originais para todos os fins legais.

Sustenta que se trata de negócio entre particulares com uso de assinatura eletrônica sem necessidade ou obrigatoriedade de se validar por meio de autoridade certificadora no sistema da ICP-Brasil.

Destaca ter disponibilizado relatório técnico contendo as principais informações coletadas no momento da assinatura do documento, de modo a conferir grau de segurança adequado à autenticidade (certeza de autoria) e à integridade documental (certeza do conteúdo), havendo garantia da legitimidade das assinaturas.

Insurge-se contra o fato de que os recorridos e executados sequer foram citados, inexistindo, assim, oposição ou impugnação quanto à forma de celebração do contrato e assinatura da cártula.

Reforça a recente modificação na legislação processual civil, admitindo qualquer modalidade de assinatura eletrônica com dispensa do uso de certificado emitido no âmbito da ICP-Brasil, para fins de se conferir executividade a títulos extrajudiciais.

Colaciona julgado do TJDFT no qual se admite assinatura eletrônica efetuada em plataforma de autenticação disponibilizada pela instituição financeira sem credenciamento no sistema ICP-Brasil, todavia, cujas informações de validação como protocolo de assinatura com código para verificação, nome, tipo, identificação, geolocalização, horário, e IP foram consideradas suficientes a atestar veracidade da assinatura eletrônica.

Requer reforma da decisão impugnada com declaração de validade da assinatura digital do contrato pactuado entre as partes.

É o relatório.

VOTO

O propósito recursal consiste em saber se as normas que regem o processo eletrônico exigem o uso exclusivo de certificação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), para fins de conferir autenticidade aos documentos produzidos e assinados eletronicamente entre as partes em momento

pré-processual.

1. DA VALIDADE JURÍDICA DOS DOCUMENTOS E ASSINATURAS ELETRÔNICAS

1. O objeto do presente recurso orbita na busca da interpretação mais razoável sobre o alcance e o sentido da MPV 2200/2001 e da Lei 11419/2006 em seus dispositivos que tratam da validade jurídica dos documentos e assinaturas produzidos em meio eletrônico.

1.1. DA INTENÇÃO DO LEGISLADOR QUANDO DA EDIÇÃO DA MPV 2200/2001

1. A validade dos documentos eletrônicos está positivada nas seguintes normas da MPV 2200/2001:

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

2. A MPV 2200/2001, apesar de não ter sido convertida em lei ordinária, acabou tendo sua vigência perenizada por força do art. 2º da EC 32/2001, a qual, segundo entendimento pacificado nesta Corte Superior, "garantiu, de forma expressa, a vigência de medidas provisórias editadas antes de seu advento" (EREsp 572.562/RS, Corte Especial, DJ de 28/03/2005). Tendo a MPV 2200/2001 sido editada em 24/08/2001, e a EC 32/2001 publicada em 11/09/2001, permanece a medida vigente até o presente, razão pela qual deve ser resgatada a vontade do legislador quando de sua primeira edição.

3. Na Exposição de Motivos Interministerial da primeira edição da MPV 2200/2001, é possível verificar a preocupação do legislador com a atribuição de

validade jurídica aos documentos eletrônicos "sem alterar a legislação aplicável aos documentos em papel escrito", sobretudo por causa da "enorme demanda reprimida no que se refere ao uso seguro do meio eletrônico nas relações que envolvem a prática de atos de troca de informações, inclusive quando destinadas a fins econômicos, como ocorre nas transações comerciais".

4. Assim, a ideia de se adotar um sistema de certificação eletrônica tem por finalidade "garantir a segurança na prática de atos em meio eletrônico, dando-lhes expressa validade legal, capaz de propiciar melhora no processo de troca de informações, tanto no setor público quanto no privado, para quaisquer fins, e servindo, inclusive, para incentivar o chamado comércio eletrônico, com efeitos benéficos para a economia e toda a sociedade", de forma a "conferir maior segurança e tranquilidade às relações jurídicas que forem estabelecidas valendo-se deste meio" (MPV 2200/2001, Exposição de Motivos Interministerial 312 de 28/06/2001, Coleção de Anais da Câmara dos Deputados 09/10/2001, Diário do Congresso Nacional, 09/10/2001, p. 21075).

5. Para administrar o novo sistema de certificação (i.e., validação para fins jurídicos), o art. 12 da MPV 2200/2001 permitiu a criação da autarquia federal, denominada Instituto Nacional de Tecnologia da Informação (ITI), cuja finalidade é ser a Autoridade Certificadora Raiz (AC Raiz) da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), ou seja, o órgão governamental responsável por desenvolver e fiscalizar o processo de certificação referido no art. 10, § 1º, da MPV 2200/2001 (<https://www.gov.br/iti/pt-br/aceso-a-informacao/institucional/o-iti>).

6. O processo de certificação pelo sistema ICP-Brasil, contudo, não excluiu outros meios de validação jurídica de documentos e assinaturas eletrônicos, consoante se verifica no § 2º do art. 10 da MPV 2200/2001 ao referir expressamente "utilização de outro meio de comprovação da autoria e integridade", e a expressão "meio de comprovação" invariavelmente traz contornos sobre a força probatória do que se pretende provar ou comprovar.

7. A distinção sobre a força (ou carga) probatória do "meio de

comprovação da autoria e integridade de documentos em forma eletrônica" foi adequadamente esclarecida pelo primeiro Procurador-Chefe do ITI, segundo o qual:

A MP 2.200-2, fonte normativa de abrangência geral, adotou uma classificação bipartida das assinaturas eletrônicas. Primeiramente, a partir da previsão do art. 10, §1º, que equiparou a assinatura digital denominada ICP-Brasil à assinatura manuscrita, com referência ao art. 219 do atual Código Civil. Isso implica em dizer que apenas esta assinatura digital agregará presunção de autoria e integridade ao documento eletrônico. ...De outro lado, a MP 2.200-2 facultou a utilização de outros mecanismos de comprovação de autoria para o meio eletrônico, que não os do âmbito da ICP-Brasil, de modo que as partes, no exercício de sua autonomia privada, ou aqueles que estabelecem modelos de negócios ou simplesmente optam pela utilização do ambiente digital em suas atividades, possam optar por outras alternativas. Cuida-se, aqui, de um ambiente desregulado e que merecerá o valor probatório a ser aferido a cada caso, pelas próprias partes, ou, em caso de litígio, pelo Poder Judiciário ou pelo Tribunal Arbitral. Esta é a razoável interpretação do disposto no parágrafo segundo do art. 10 da MP 2.200-24, uma vez que vigora no Brasil o princípio da liberdade de forma da declaração de vontade (art. 107 do Código Civil), ao lado da diretriz de que as partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos para provar a verdade dos fatos (art. 369 do Código de Processo Civil). (Menke, Fabiano. A Medida Provisória nº 983 e a classificação das assinaturas eletrônicas: comparação com a Medida Provisória nº 2.200-2 de 2001. Disponível em: <https://cryptoid.com.br/criptografia-identificacao-digital-id-biometria/a-mp-983-e-a-classificacao-das-assinaturas-eletronicas-comparacao-com-a-mp-2-200-2-por-fabiano-menke>, p. 01-02, g.n.)

8. Em outra oportunidade, o referido autor assim se manifestou:

A Medida Provisória n. 2.200-2 não determina a observância compulsória dos requisitos da ICP-Brasil, sob pena de invalidade. A este ponto não chegou o texto legal. Não há que se perder de vista, outrossim, o contido no §2º do art. 10 da Medida Provisória n. 2.200-2...Este dispositivo tem o intuito de flexibilizar a referida regra do § 1º, esclarecendo que as partes têm a liberdade de escolher outros meios de atribuição de autoria que não a assinatura digital ICP-Brasil. A Medida Provisória n. 2.200-2, portanto, não criou uma forma especial obrigatória para o meio eletrônico. E mais, sua disciplina sobre forma e prova dos atos e negócios jurídicos se situa no âmbito do disciplinado no Código Civil, que determina, no...art. 107, que a validade de declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir. Não se verifica, portanto, no texto da Medida Provisória n. 2.200-2, a fixação da forma especial para os procedimentos de atribuição de autoria da ICP-Brasil....O diferencial da assinatura digital da ICP-Brasil, assim, não é atributo de uma pretensa validade exclusiva e absoluta para o meio eletrônico, mas sim de efeitos jurídico-probatórios diferenciados que o documento eletrônico comum não dispõe....A questão se resolve, pois, no plano da eficácia e não da validade. Esses efeitos jurídico-probatórios diferenciados da ICP-Brasil agregam um maior poder de convencimento sobre a autoria e a integridade do documento eletrônico, portanto, uma segurança jurídica muito mais robusta, ao

dificultar sobremaneira (mas não impossibilitar de todo) as alegações de ausência de autoria. (Menke, Fabiano. Apontamentos sobre o comércio eletrônico no direito brasileiro. In: Coelho, Fábio Ulhoa. Questões de direito comercial no Brasil e em Portugal. São Paulo: Saraiva, 2014. p. 369-372, g.n.)

9. Com o advento da Lei 14063/2020, o sistema multifacetado de níveis de segurança (ou confiança) foi positivado de maneira ainda mais clara, e os conceitos tecnológicos foram adequadamente delimitados nos seus arts. 3º e 4º, sendo os mais relevantes para a compreensão do significado dos termos técnicos da área da tecnologia da informação ora em debate:

(i) autenticação: método de processamento de dados em meio eletrônico que permite a identificação eletrônica de uma pessoa natural ou jurídica;

(ii) assinatura eletrônica: associação de dados em formato eletrônico utilizados pelo signatário para assinar nos três níveis de segurança, classificados do menor ao mais elevado, da seguinte forma:

(a) assinatura eletrônica *simples*: permite identificação do signatário por simples associação de dados;

(b) assinatura eletrônica *avançada*: a que utiliza certificados não emitidos pela ICP-Brasil, ou que utiliza um método alternativo de comprovação de autoria e integridade de documentos em forma eletrônica, desde que:

(1) seja admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento,

(2) seja inequivocamente associada ao signatário,

(3) utilize dados que permitam ao signatário operar sob o seu controle exclusivo e com elevado nível de confiança e

(4) permita a detecção de qualquer modificação dos dados da assinatura posteriormente à sua execução;

(c) assinatura eletrônica *qualificada*: a que utiliza certificados emitidos pela ICP-Brasil.

10. Na ocasião da elaboração da Lei 14063/2020 (que nasceu da conversão da MPV 983/2020), o legislador - com amparo no entendimento da

Procuradoria do ITI (Parecer 00378/2019/PROFE/PFE-ITI/PGF/AGU) - pontuou que "a única espécie de assinatura eletrônica equiparada à assinatura manuscrita no direito positivo brasileiro é a assinatura digital produzida com o uso do processo de certificação digital da ICP-Brasil", ao passo que o "§2º do art. 10 da MP nº 2.200-2/2001...aplica-se exclusivamente às manifestações de vontade realizadas no âmbito privado", ou seja: "o uso das assinaturas eletrônicas qualificadas pelas pessoas naturais e pessoas jurídicas de direito privado também devem ser tidas como confiáveis para a prática de diversos atos, especialmente para documentos particulares que necessitam ser levados a registros perante entes e Poderes Públicos em todas as esferas, para que tenham efeitos perante terceiros" (Câmara dos Deputados, MPV 983/2020, Parecer Preliminar de Plenário n. 1, de 10/08/2020, p. 06-24).

11. Ou seja, a intenção do legislador foi de criar níveis diferentes de força probatória das assinaturas eletrônicas, conforme o método tecnológico de autenticação utilizado pelas partes, e - ao mesmo tempo - conferir validade jurídica a qualquer tipo de assinatura eletrônica, levando em consideração a autonomia privada e a liberdade das formas de declaração de vontades entre os particulares.

1.2. DA INTENÇÃO DO LEGISLADOR QUANDO DA ELABORAÇÃO DA LEI 11419/2006

12. No âmbito do processo judicial eletrônico, a validade dos documentos produzidos e juntados aos autos eletrônicos é elucidada nas seguintes normas da Lei 11419/2006:

Art. 11. Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.

Art. 1º ...

§ 2º Para o disposto nesta Lei, considera-se:

...

III - assinatura eletrônica as seguintes formas de identificação inequívoca do signatário:

a) assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica;

b) mediante cadastro de usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos.

13. A Lei 11419/2006 adveio do anteprojeto de informatização do processo judicial, proposto pela Associação dos Juízes Federais do Brasil - AJUFE, que, entre as justificativas apresentadas, constava o objetivo de "evoluir na vereda inaugurada pelas leis [do uso do fac-símile e dos juizados especiais], regulando plenamente a informatização dos procedimentos judiciais, afastando dúvidas acerca da validade de atos processuais assim praticados", e, ao mesmo tempo, sem eliminar "a possibilidade de as partes se manifestarem pelos métodos convencionais, a fim de levar em conta as necessidades de profissionais, regiões e/ou segmentos que - por diferentes motivos - não disponham dos equipamentos necessários" (Anais da Câmara dos Deputado, SUG 1/2001 CLP: ofício AJUFE nº 174 de 13/08/2001, p. 9-10).

14. Importa notar que no anteprojeto proposto pela AJUFE inexistia qualquer ressalva quanto ao uso de certificação para o envio de peças processuais, mas apenas o credenciamento perante o judiciário por meio de "procedimento no qual esteja assegurada a adequada identificação do interessado" (art. 2º do anteprojeto).

15. Com o acolhimento da sugestão normativa pela Comissão de Legislação Participativa da Câmara, o anteprojeto foi convertido no PL 5828/2001 da Câmara dos Deputados, sendo no âmbito do Senado Federal registrado como Projeto de Lei da Câmara nº 71/2002.

16. Na casa legislativa revisora (Senado), houve debate sobre a adequação do uso de criptografia por meio do emprego de chaves públicas e privadas para permitir "de forma simples a assinatura digital de documentos eletrônicos", de forma a evitar "reinvenções da roda", considerando que "já existem, livremente disponíveis, soluções quiçá mais simples, que bem atenderiam à necessidade de autenticação dos documentos processuais". Assim, o texto original do substitutivo do Senado (constante do Documento Anexado pela Secretaria-Geral da Mesa) enunciava em seu art. 2º que "para ter validade, o

documento eletrônico deve ser assinado digitalmente, por meio de sistema criptográfico de chave pública e chave privada" (Senado Federal, Parecer da Comissão de Constituição e Justiça e Cidadania 1961/2005, Diário do Senado Federal de 19/11/2005, p. 10).

17. Todavia, houve alteração na relatoria do PLC 71/2002, e o texto final do substitutivo que foi aprovado pela CCJC do Senado modificou o precitado art. 2º, deslocando o tópico do método de autenticação para o art. 1º e efetivamente substituindo o requisito mais genérico da proposta original do substitutivo (i.e., de uso de um sistema de chaves criptográficas) pelo texto que consta atualmente no art. 1º, III, "a", da Lei 11419/2006, ou seja, "assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica" (idem, p. 2).

18. Com o retorno do PL 5828/2001 para a Câmara dos Deputados, a exigência de uso de certificado digital emitido por Autoridade Certificadora credenciada" foi mantida com a ressalva da CCJC da Câmara que "a proposta altera o Código de Processo Civil para adaptá-lo ao uso de meios eletrônicos, afastando do ordenamento os obstáculos que possam dar ensejo a questionamentos judiciais sobre o uso de novas tecnologias na prática de atos processuais e na transmissão de informações" (Câmara dos Deputados, Comissão de Constituição e Justiça e Cidadania, Parecer às Emendas e Substitutivos do Senado - EMS 5828/2001 de 29/06/2006, p. 4).

19. Portanto, em que pese ser possível notar que - entre o momento de apresentação do anteprojeto pela AJUFE e o momento de se ultimar a redação final do projeto de lei nas casas legislativas - houve a inserção da exigência de uso de "certificado digital emitido por Autoridade Certificadora credenciada", não se pode igualmente se perder de vista a preocupação do legislador com respeito à validade dos "atos processuais" no ambiente eletrônico, ou seja, a validade jurídica dos atos de peticionamento propriamente.

20. Tanto é assim que o legislador igualmente previu a possibilidade de

"cadastro de usuário no Poder Judiciário" como meio alternativo de certificação para a prática de atos processuais pelas partes - i.e., o enfoque dado pelo legislador ocorre especificamente na relação entre o Estado e o jurisdicionado no âmbito da lide.

2. DA EVOLUÇÃO JURISPRUDENCIAL QUANTO À FORÇA PROBANTE DOS DOCUMENTOS E ASSINATURAS EMITIDAS EM MEIO ELETRÔNICO

21. Nos últimos 10 anos, esta Corte Superior - atenta à evolução tecnológica nas comunicações e na celebração de negócios jurídicos entre os particulares e acompanhando o espírito do legislador em buscar maior segurança jurídica às transações comerciais privadas conduzidas em meio eletrônico - passou a atestar validade jurídica a uma série de documentos que tradicionalmente exigiam formalidades típicas do "mundo físico", a exemplo da assinatura de próprio punho e da presença de testemunhas no ato da assinatura.

22. Mesmo antes da MPV 2200/2001 este STJ relevou o tradicional requisito formal da assinatura de próprio punho, para fins de validade jurídica de títulos de crédito, segundo a legislação cambiária, quando por outros elementos (a exemplo da confissão do emitente) era possível atestar a autenticidade da assinatura - mesmo que tenha sido escaneada ou digitalizada -, em prol da boa-fé objetiva nas relações comerciais (REsp 1.192.678/PR, Terceira Turma, DJe de 26/11/2012).

23. Esta Corte Superior evoluiu - e, de certo modo, antecipou o que viria a ser positivado no novo § 4º do art. 784 do CPC - para o "excepcional reconhecimento da executividade de determinados títulos (contratos eletrônicos) quando atendidos especiais requisitos, em face da nova realidade comercial com o intenso intercâmbio de bens e serviços em sede virtual", relevando a tradicional exigência de assinatura de duas testemunhas, para fins de se conferir executividade a título extrajudicial, fazendo expressa ressalva de que sempre poderá o executado suscitar irregularidade formal do "documento eletrônico, seja

em exceção de pré-executividade, seja em sede de embargos à execução" (REsp 1.495.920/DF, Terceira Turma, DJe de 07/06/2018).

24. Atualmente é possível afirmar que o referido "excepcional reconhecimento da executividade" dos contratos assinados eletronicamente se transformou em regra geral na visão deste STJ, devendo ser reconhecida como tal "diante da nova realidade comercial, em que se verifica elevado grau de relações virtuais" (AgInt no REsp 1.978.859/DF, Terceira Turma, DJe de 25/05/2022), pois "o avanço tecnológico observado na presente 'era digital' tornou necessário conferir a mesma higidez e segurança na identificação de documentos em formato eletrônico, elaborados com o auxílio de computadores" (AgInt no AREsp 1.917.838/RJ, Quarta Turma, DJe de 09/09/2022), sendo a vocação da assinatura digital de contrato eletrônico "certificar...que determinado usuário de certa assinatura a utilizara e, assim, está efetivamente a firmar o documento eletrônico e a garantir serem os mesmos os dados do documento assinado que estão a ser sigilosamente enviados" (AgInt no AREsp 2.001.392/SP, Terceira Turma, DJe de 27/04/2023).

25. A garantia da autenticidade dos dados digitais, todavia, tem encontrado importantes contornos especialmente na seara do direito processual penal, no que se refere à necessidade de preservação da cadeia de custódia da prova digital, tendo este STJ reconhecido que, por um lado, a "volatilidade dos dados telemáticos" e a "maior suscetibilidade a alterações" requer "adoção de mecanismos que assegurem a preservação integral dos vestígios probatórios" de forma a possibilitar a "auditabilidade, a repetibilidade, a reprodutibilidade e a justificabilidade...das evidências digitais" com utilização de técnicas acompanhadas da "utilização de um software confiável, auditável e amplamente certificado, que possibilite o acesso, a interpretação e a extração dos dados do arquivo digital", a exemplo da utilização da técnica de "algoritmo hash" para "garantir a mesmidade dos elementos digitais" (AgRg no HC 828.054/RN, Quinta Turma, DJe de 29/04/2024).

26. Por derradeiro, é pacífico nesta Corte Superior que a exigência de uso do certificado digital no sistema da ICP-Brasil a que se refere o art. 1º, § 2º, III, “a”, da Lei 11419/2006 (ou o credenciamento de forma presencial do usuário da plataforma eletrônica judicial a que se refere a alínea “b” da referida norma) diz respeito à validade dos atos processuais de peticionamento nos autos (EAREsp 452.107/RJ, Terceira Seção, DJe de 14/11/2017; AgInt no AREsp 1.917.838/RJ, Quarta Turma, DJe de 09/09/2022; REsp n. 1.442.887/BA, Terceira Turma, DJe de 14/05/2014) - ou seja: não há de se confundir com a validação de autenticidade e integridade documental “fora dos autos” a que se refere a MPV 2200/2001 de modo mais abrangente em seu art. 10.

27. Portanto, o reconhecimento da validade jurídica e da força probante dos documentos e das assinaturas emitidos em meio eletrônico, quando aliados ao uso de ferramentas tecnológicas que permitem inferir (ou auditar) de forma confiável a autoria e a autenticidade da firma ou do documento, está, na evolução dos precedentes desta Corte Superior, em franca harmonia com o espírito do legislador.

3. DOS ASPECTOS TÉCNICOS DO CONTROLE DE AUTENTICIDADE E DE INTEGRIDADE DAS ASSINATURAS E DOS DOCUMENTOS ELETRÔNICOS

28. O controle de autenticidade das assinaturas ou dos documentos eletrônicos - ou seja, a garantia de que a pessoa quem preencheu o documento ou assinou ele é realmente a mesma pessoa - depende dos métodos de autenticação utilizados no momento da assinatura, incluindo o número e a natureza dos fatores de autenticação.

29. Enquanto a assinatura eletrônica simples geralmente utiliza apenas um fator de autenticação — fornecendo uma informação que, em teoria, somente o signatário saberia (como uma senha ou um código) — a assinatura eletrônica avançada requer múltiplos fatores para assegurar a autenticidade do signatário. Esses podem incluir confirmações enviadas para o e-mail pessoal, códigos via SMS

para o celular, mensagens em aplicativos de mensagens instantâneas ou a utilização de aplicativos autenticadores que geram senhas temporárias (tokens), combinando assim diferentes métodos de verificação.

30. Métodos mais sofisticados de autenticação dizem respeito à biometria, sendo as mais comuns em escala comercial o reconhecimento da geometria facial (com a captura fotográfica de uma "selfie"), a coleta papiloscópica da impressão digital (em um leitor com sensores óticos) e o reconhecimento da voz (pela tonalidade do timbre) - e as menos comercialmente populares (porém, tecnologicamente mais seguras em termos de menor margem de erro ou susceptibilidade a fraudes), consistindo na captura da imagem da íris, da retina, ou da configuração venosa das articulações do corpo humano - i.e., pela análise do padrão das artérias do globo ocular, dos punhos ou das mãos (Tripathi, K. P. A Comparative Study of Biometric Technologies with Reference to Human Interface. International Journal of Computer Applications, vol. 14, n. 5, Jan/2011, p. 10-11).

31. Já o controle de integridade dos documentos eletrônicos ou das assinaturas eletrônicas - ou seja, a garantia de que a assinatura ou o conteúdo do documento não foram modificados no trajeto entre a emissão, validação, envio e recebimento pelo destinatário -, é feito por uma fórmula matemática (algoritmo) que cria uma "impressão digital virtual".

32. A garantia da singularidade dessa "impressão digital virtual" ocorre por meio de criptografia, i.e., o processo de codificar informações de modo que somente aqueles autorizados possam decifrá-las (o termo vem das palavras gregas "kryptós" - escondido, oculto - e "gráphein" - escrita).

33. Uma das funções mais importantes na segurança da informação é a função criptográfica "hash", que gera um resumo único de um documento (ou de uma assinatura) em meio eletrônico com base no conteúdo original. As primeiras funções criptográficas "hash" foram desenvolvidas na década de 1970 nos EUA, mas ganharam destaque na década de 1990 com o desenvolvimento do "Secure Hash Algorithm" (SHA) pela Agência de Segurança Nacional (NSA) em conjunto

com o Instituto Nacional de Padrões e Tecnologia (NIST). O objetivo era padronizar a integridade e a autenticidade na transmissão de dados sensíveis no âmbito do governo federal (Penard Wouter, Tim Van Werkhoven. On the secure hash algorithm family. Cryptography in context, p. 1-18).

34. O resumo criado pela função criptográfica “hash” é geralmente representado em formato hexadecimal, utilizando os dígitos de '0' a '9' e as letras de 'a' a 'f', facilitando a leitura e comparação por humanos (o Instituto Forense do Ministério da Justiça holandês explica razoavelmente bem a função "hash" para leigos em ciência da computação no documento "Technical Supplement – Forensic Use of Hash Values and Associated Hash Algorithms", jan/2018, p. 02 - disponível em

https://www.forensicinstitute.nl/binaries/forensicinstitute/documenten/publications/2018/02-forensic-use-of-hash-values-and-associated-hash-algorithms/Supplement-hashes-v2018_01a_English.pdf).

35. Por exemplo, utilizando um conversor de texto "humano" para o texto básico das máquinas (i.e., o código binário), o termo "Superior Tribunal de Justiça" na linguagem binária da computação é representado pela seguinte sequência de "0" e "1": 01010011 01110101 01110000 01100101 01110010 01101001 01101111 01110010 00100000 01010100 01110010 01101001 01100010 01110101 01101110 01100001 01101100 00100000 01100100 01100101 00100000 01001010 01110101 01110011 01110100 01101001 11000011 10100111 01100001 (disponível em <https://www.rapidtables.com/convert/number/ascii-to-binary.html>).

36. Embora a sequência binária seja tecnicamente legível por máquinas, ela não é prática para verificação de integridade e tampouco está protegida do conhecimento de terceiros – daí a importância de se aplicar a criptografia para lhe tornar ilegível, ou seja, cifrando e decifrando os dados da sequência binária com uso de chaves criptográficas (i.e., a “senha algorítmica” para cifrar ou decifrar).

37. Atualmente, um dos padrões de função criptográfica “hash” mais

utilizados é o SHA-256 ("Secure Hash Algorithm" de 256 bits). Uma das características importantes desse algoritmo é o efeito avalanche, onde uma pequena alteração no conteúdo original resulta em uma mudança significativa no resumo gerado. Isso significa que mesmo uma modificação mínima no documento produzirá um código "hash" completamente diferente, evidenciando qualquer tentativa de adulteração.

38. Por exemplo, utilizando-se um gerador de código "hash" no padrão SHA-256 (<https://passwordsgenerator.net/sha256-hash-generator>), podemos calcular o resumo único em código "hash" das expressões "Superior Tribunal de Justiça" e "Superior Tribunal de Justica" (i.e., alterando a cedilha para o "c" normal na palavra "Justiça/Justica") na seguinte forma:

(i) "Superior Tribunal de Justi**ç**a", cujo código "hash" é "**6a328262c5697f836ac57cbb6e84bfe823e50e1e97d0052bcd709ce058c20c26**"; e

(ii) "Superior Tribunal de Justi**c**a", cujo código "hash" é "**178c4f9c109a303f9e23576aa7770c6a713f25b0605015d6fc1e1b9f8da508ac**".

39. Ou seja, uma sutil mudança em apenas uma letra ("c" ao invés de "ç") - que facilmente passaria despercebida aos olhos humanos - se torna extremamente visível pela notável diferença nos códigos "hash" gerados, ilustrando o "efeito avalanche".

40. No âmbito criminal, esta Corte Superior, já teve a oportunidade de compreender a importância dessa função criptográfica e o impacto dela na questão relativa à cadeia de custódia de provas digitais, esclarecendo que com a "técnica de algoritmo hash, é possível obter uma assinatura única para cada arquivo, que teria um valor diferente caso um único bit de informação fosse alterado", de forma que "comparando as hashes calculadas nos momentos da coleta e da perícia (ou de sua repetição em juízo), é possível detectar se o conteúdo extraído do dispositivo foi modificado" (AgRg no RHC 143.169/RJ, Quinta Turma, DJe de 02/03/2023), ou, em outras palavras, "a prova da cadeia de custódia

não se confunde com a cadeia de custódia da prova" (Reis, Rodrigo Casimiro. A cadeia de custódia dos vestígios digitais como instrumento para se alcançar a verdade possível no Processo Penal. Reflexões sobre a prova no processo penal, São Paulo: Amanuense (2024), p. 65).

41. Isso demonstra como as funções "hash" são sensíveis a mudanças e eficientes na detecção de qualquer modificação de conteúdo original de documentos ou assinaturas em meio eletrônico. Essa propriedade é fundamental para garantir a integridade em assinaturas eletrônicas, tanto na modalidade avançada quanto na modalidade qualificada.

4. DO RECURSO SOB JULGAMENTO

42. O Tribunal de Origem entendeu que "nos termos da Lei n.º 11.419/2006, que dispõe sobre a informatização do processo judicial, é admissível a assinatura digital baseada em certificado digital emitido por autoridade certificadora credenciada, a fim de que seja assegurada a identificação inequívoca do signatário", todavia, "embora o §2º, do artigo 10, da Medida Provisória n.º 2.200-2/2001, reconheça a possibilidade de utilização de outro meio para a comprovação da validade de documento assinado eletronicamente, em especial com certificado não emitido pela ICP-Brasil, essa previsão apenas é cabível para as hipóteses em que a dilação probatória é viável, o que não é o caso destes autos", pois "a execução é amparada em cédula de crédito bancário assinada digitalmente, mais precisamente por plataforma vinculada à exequente", a qual "não está credenciada como autoridade certificadora perante o ITI" (e-STJ fls. 400-402).

43. Instado a se pronunciar sobre a incidência da norma do art. 784, § 4º, do CPC, o Tribunal de Origem assinalou que "o fato de ser...admitida qualquer modalidade de assinatura eletrônica prevista em lei...não dispensa a necessidade de que a validade de documento, em especial para que configure título executivo assinado eletronicamente possa ser confirmada extrajudicial (sic)" (e-STJ fl. 420).

44. Em outras palavras, o Tribunal de Origem entende que apenas assinatura eletrônica qualificada (i.e., aposta com uso de certificado digital do

sistema da ICP-Brasil) possui validade jurídica, seja para fins de autenticação de documentos e assinaturas em meio eletrônico em momento pré-processual, seja no âmbito do processo judicial.

45. O entendimento colide com a intenção manifesta do legislador, endossada por esta Corte Superior nos termos dos citados precedentes, de conferir validade legal às assinaturas eletrônicas em documentos particulares, independentemente do grau de robustez do método de autenticação.

46. Evidentemente que a assinatura eletrônica avançada possui uma presunção menor de veracidade quando comparada com a assinatura eletrônica qualificada que utiliza certificação ICP-Brasil, porém, ainda assim, ela possui uma carga razoável de força probatória e - mais importante - validade jurídica idêntica, conforme endossado pelo próprio ITI, para o qual o "documento com a assinatura digital avançada tem a mesma validade de um documento com assinatura física" apenas dependendo "da aceitação do emitente e do destinatário" (Instituto Nacional de Tecnologia da Informação, Carta de Serviço ao Usuário, 2ª Versão (2023), p. 13 - disponível em: <https://www.gov.br/iti/pt-br/acesso-a-informacao/perguntas-frequentes/certificacao-digital>).

47. As partes acordaram expressamente "que a presente operação de crédito poderá ser contratada através de meios eletrônicos das quais se puder verificar a autoria, mediante aposição de login, senha, assinatura eletrônica e/ou assinatura digital, nos termos da Lei 13.986, de 7 de abril de 2020 e da Medida Provisória nº 2.200-2, de 24 de agosto de 2001" e "ainda, aceita(m) e concorda(m) que a contratação eletrônica da operação terá, para todos os fins e efeitos de direito, a mesma validade de uma ordem escrita equivalente" (cláusulas 2.1 e 2.2, e-STJ fl. 58).

48. Em outras palavras, há presunção de acordo de vontades quanto à utilização do método de assinatura eletrônica (avançada) por meio da plataforma de assinatura desenvolvida e disponibilizada pela credora.

49. Segundo consta do relatório "Gerenciador de Assinaturas Eletrônicas

de Documentos" (e-STJ fl. 70) - i.e., a representação histórica das assinaturas eletrônicas na cártula dos recorridos (devedores e avalistas) - houve a utilização de múltiplos fatores de autenticação (nome, CPF, código "hash" de cada assinatura, data, horário e IP da máquina onde ocorreu a assinatura), o que é suficiente para se presumir a autenticidade e a integridade das assinaturas, apostas no modo avançado, conforme explanado na fundamentação acima.

50. Por um lado, a refutação da veracidade da assinatura eletrônica e dos documentos sobre os quais elas foram eletronicamente apostas - seja no aspecto de sua integridade, seja no aspecto de sua autoria - deve ser feita por aquele a quem a norma do art. 10, § 2º, da MPV 20200/2001 expressamente se dirigiu, que é a "pessoa a quem for oposto o documento"; em outras palavras: a pessoa que admite o documento como válido (i.e., o destinatário). Essa é, aliás, a norma do art. 411, I, do CPC, ao criar a presunção de autenticidade do documento particular quando a parte contra quem ele for produzido deixar de impugná-lo.

51. A pessoa a quem o legislador refere é uma das partes na relação processual (no caso de execução de título de crédito, o emitente e seus avalistas), o que - por definição - exclui a pessoa do juiz, sob pena de se incorrer no tratamento desigualitário, vetado pela norma do art. 139, I, do CPC.

52. Por outro lado e com respeito à carga probatória das assinaturas eletrônicas, é possível se compreender, por analogia, que 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.

53. Ambas são válidas e apenas se distinguem no aspecto da força probatória - ou seja, é muito mais difícil se provar a falsidade de uma assinatura reconhecida por autenticidade do que por semelhança. Não é impossível (até mesmo porque selos notariais podem ser falsificados - v.g. HC 687.660/RS, decisão unipessoal de membro da 5ª Turma, DJe de 10/09/2021), mas no mundo da informática, a prova da falsidade é muito mais direta e objetiva de ser feita do que um complexo exame grafotécnico, considerando que a análise forense digital

envolve fundamentalmente a comparação de resultados de aplicação de fórmulas matemáticas.

54. E como geralmente os números não "mentem", a perícia computacional forense possui um grau de confiança muito maior em termos de precisão da comprovação da falsidade em razão dos seus atributos particulares de "repetibilidade da extração da prova digital", ou seja, pelo fato de o código "hash" ser "calculado a partir da fonte original da informação digital e não a partir de simples cópia" (Reis, op. cit., p. 66).

55. Daí por que quis o legislador emprestar o mesmo grau de validade jurídica para as assinaturas eletrônicas - seja avançada, seja qualificada - pois a forma técnica de se impugnar seus aspectos de validação partem das mesmas premissas de auditoria de integridade de seus dados.

56. Assim, negar validade jurídica a um título de crédito, emitido e assinado de forma eletrônica, simplesmente pelo fato de a autenticação da assinatura e da integridade documental ter sido feita por uma entidade sem credenciamento no sistema ICP-Brasil seria o mesmo que negar validade jurídica a um cheque emitido pelo portador e cuja firma não foi reconhecida em cartório por autenticidade, evidenciando um excessivo formalismo diante da nova realidade do mundo virtual.

57. Por derradeiro, a exigência da Lei 11419/2006 com respeito às assinaturas eletrônicas emitidas na modalidade qualificada (i.e., com uso de certificação no sistema da ICP-Brasil) diz respeito à realização de atos processuais, ou seja, o peticionamento nos autos eletrônicos, o que não se confunde com a produção - em momento pré-processual - de documentos eletrônicos e sua validação entre os particulares a que se refere a MPV 2200/2001, conforme contextualizado no espírito do legislador.

58. A inovação trazida pela Lei 14620/2023, ao inserir o § 4º no art. 784 do CPC, segue exatamente a linha jurisprudencial desta Corte Superior, conforme delineado na fundamentação, sendo o legislador ainda mais preciso ao informar

que se admite "qualquer modalidade de assinatura eletrônica prevista em lei" desde que a integridade da assinatura seja "conferida por provedor de assinatura" - ou seja, inexistência de exclusividade de certificação digital do sistema ICP-Brasil na constituição ou ateste de título executivo extrajudicial no meio eletrônico, tal como ocorre na presente hipótese.

59. Plausível, por conseguinte, a ofensa aos arts. 10, § 2º, da MPV 2200/2001 e 784, § 4º, do CPC, devendo o acórdão impugnado ser reformado, a fim de se determinar o prosseguimento da ação de execução com o curso normal do processo.

60. Despicienda a análise do dissídio, tendo em vista o provimento do recurso especial pela alínea "a" do permissivo constitucional.

5. DISPOSITIVO

Forte nessas razões, **CONHEÇO** do recurso especial e **DOU-LHE PROVIMENTO**, para anular o acórdão recorrido e determinar a devolução dos autos ao juízo de origem a fim de que se processe a ação de execução de título extrajudicial.

Ante o resultado do julgamento, deixo de aplicar o disposto no art. 85, § 11, do CPC.

CERTIDÃO DE JULGAMENTO
TERCEIRA TURMA

Número Registro: 2024/0212892-1

PROCESSO ELETRÔNICO REsp 2.150.278 / PR

Números Origem: 00036804220248160030 00081421320228160030 36804220248160030

PAUTA: 24/09/2024

JULGADO: 24/09/2024

Relatora

Exma. Sra. Ministra **NANCY ANDRIGHI**

Presidente da Sessão

Exmo. Sr. Ministro HUMBERTO MARTINS

Subprocurador-Geral da República

Exmo. Sr. Dr. ONOFRE DE FARIA MARTINS

Secretária

Bela. MARIA AUXILIADORA RAMALHO DA ROCHA

AUTUAÇÃO

RECORRENTE : COOPERATIVA DE CREDITO DE LIVRE ADMISSAO TRES
FRONTEIRAS - SICOOB TRES FRONTEIRAS
ADVOGADOS : MARCELO RICARDO URIZZI DE BRITO ALMEIDA - PR030715
ALESSANDRA CELANT - PR057984
RECORRIDO : RHL LTDA
RECORRIDO : HELOISA CEZARINO MARTINS
RECORRIDO : RODRIGO BIANCO
ADVOGADO : ROMANO CAPPONI JÚNIOR - PR058481

ASSUNTO: DIREITO CIVIL - Obrigações - Espécies de Títulos de Crédito - Cédula de Crédito
Bancário

CERTIDÃO

Certifico que a egrégia TERCEIRA TURMA, ao apreciar o processo em epígrafe na sessão realizada nesta data, proferiu a seguinte decisão:

A TERCEIRA TURMA, por unanimidade, conheceu do recurso especial e lhe deu provimento, com majoração de honorários, nos termos do voto da Sra. Ministra Relatora.

Os Srs. Ministros Humberto Martins (Presidente), Ricardo Villas Bôas Cueva, Marco Aurélio Bellizze e Moura Ribeiro votaram com a Sra. Ministra Relatora.