

Belo Horizonte, 25 de junho de 2024.



NOTA TÉCNICA - ASSINATURAS ELETRÔNICAS, MANDATO JUDICIAL E OUTROS DOCUMENTOS ASSINADOS ELETRONICAMENTE, DESTINADOS À COMPROVAÇÃO DE FATOS E ATOS JURÍDICOS MATERIAIS, E TRATAMENTO ADEQUADO DE INDÍCIOS DE ANOMALIAS

INTRODUÇÃO

Durante considerável período, em esforço de estreitamento de sua atuação em rede, preconizada por normas como a Resolução CNJ nº 349/2020 e em cumprimento das Diretrizes números 7/2023 e 6/2024 da Corregedoria Nacional de Justiça, o Centro de Inteligência da Justiça de Minas Gerais (CIJMG), o Centro de Inteligência do Núcleo de Gerenciamento de Precedentes do Poder Judiciário do Estado do Tocantins (CINUGEP) e o Núcleo de Monitoramento de Perfil de Demandas do Tribunal de Justiça do Distrito Federal (NUMOPEDE – TJDFT) identificaram possível relação entre focos anômalos de litigiosidade (ou litigância) e utilização massiva de modos pouco seguros de assinatura de documentos, notadamente documentação destinada à comprovação do preenchimento de condições da ação e de pressupostos processuais.

Dados jurimétricos colhidos diuturnamente, não apenas pelos referidos órgãos judiciários, mas também por Centros de Inteligência e NUMOPEDEs de outros Tribunais brasileiros têm indicado uso muito intensivo de assinaturas eletrônicas, especialmente em modalidades sem uso de certificado digital e que resultam na

inserção, em documentos como procurações e contratos, de desenhos de nomes ou nomes em padrão de editores de texto. As evidências colhidas apontam também uso crescente, por um número reduzido de profissionais e escritórios, com frequente atuação fora do estado de inscrição originária no órgão profissional, muitas vezes sem inscrição suplementar, e com patrocínio de milhares de ações em diversos Estados da federação, em regra propostas às centenas em curto espaço de tempo, de instrumentos de mandato com essa espécie de assinatura, o que evidenciou a necessidade de avaliação dos focos de litigiosidade pelos órgãos de inteligência judiciária.

Importa pontuar que apenas se identificaram tais focos em relação a determinados assuntos processuais – repetidos em diversos Estados da federação e, em regra, envolvendo direito à saúde e relações contratuais – e a ações iniciadas por petições iniciais genéricas, com alegações vagas e muito semelhantes entre si, frequentemente hipotéticas e relacionadas a pedidos sucessivos baseados nessas hipóteses, além de valores da causa em regra muito semelhantes entre si, embora relativas a lides essencialmente fáticas. Não se identificou o mesmo fenômeno em relação a outras espécies de litígios repetitivos.

O resultado da análise profunda da questão, com distinção do tratamento relativamente a documentos destinados à comprovação da presença dos pressupostos processuais e das condições da ação e dos destinados a demonstrar a ocorrência de fatos e atos materialmente relevantes, é o objeto desta nota técnica.

1) ASSINATURA ELETRÔNICA E DISTINÇÕES NECESSÁRIAS

Uma definição de fácil apreensão de assinatura eletrônica é apresentada por Leite (2023):

De acordo com as definições constantes da legislação brasileira (Lei 14.063/2020 (LGL\2020\12790), art. 3º, inc. II) e de diplomas internacionais, a assinatura eletrônica pode ser conceituada como conjunto de dados em formato eletrônico, relacionado de algum modo a determinada pessoa, que se liga ou logicamente se associa a outro conjunto de dados em formato eletrônico, evidenciando a intenção do signatário de se vincular por seu conteúdo.

Trata-se de técnicas voltadas a desempenhar, no “mundo online”, as mesmas funções da assinatura manuscrita: identificar a pessoa e vinculá-la a determinado ato.

Sobre as possibilidades de assinatura eletrônica admissíveis em relação a atos processuais eletrônicos, dispõe o inciso III do artigo 1º da Lei n. 11.419/2006:

Art. 1º O uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais será admitido nos termos desta Lei.

(...)

§ 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.

A respeito de tal dispositivo, comenta Andrade (2018):

A assinatura eletrônica carrega os atributos da autenticidade, privacidade e integridade. O documento será autêntico, pois uma vez lançada a assinatura eletrônica, identificado estará o seu titular, tornando formalmente autêntico o documento no tocante à sua materialidade. A integridade é atributo que impede a alteração material no documento, que, uma vez assinado eletronicamente, não pode ser alterado material ou formalmente. Por fim, a privacidade é outorgada ao documento pela possibilidade de encriptação, método pelo qual o documento é codificado e somente poderá ser aberto e ter seu conteúdo conhecido pelo titular da assinatura eletrônica, uma vez que o remetente do documento poderá utilizar a chave pública para codificar o documento, que somente poderá ser decodificado – decriptação – pelo destinatário, ou seja, pelo titular da assinatura eletrônica.

Todavia, o art. 1º, § 2º, inc. III, da Lei 11.419/2006 (LGL\2006\2382), criou uma nova espécie de assinatura eletrônica, mas somente para o processo eletrônico, pois também considera assinatura eletrônica, o cadastro prévio junto ao Poder Judiciário. Evidente que o referido cadastro não é assinatura eletrônica nos moldes que é conhecida e utilizada nos sistemas jurídicos de vários países, mas, sem dúvida, tal como ocorre nos sistemas informáticos de bancos, sites de lojas virtuais e várias empresas que atuam na Internet, é um sistema de identificação do usuário que dá este acesso aos serviços do Poder Judiciário e a oportunidade de praticar atos processuais por meio eletrônico.

Já o art. 11 estabelece:

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.

§ 1º Os extratos digitais e os documentos digitalizados e juntados aos autos pelos órgãos da Justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pelas procuradorias, pelas autoridades policiais, pelas repartições públicas em geral e por advogados públicos e privados têm a mesma força probante dos originais, ressalvada a alegação motivada e fundamentada de adulteração antes ou durante o processo de digitalização.

§ 2º A argüição de falsidade do documento original será processada eletronicamente na forma da lei processual em vigor.

§ 3º Os originais dos documentos digitalizados, mencionados no § 2º deste artigo, deverão ser preservados pelo seu detentor até o trânsito em julgado da sentença ou, quando admitida, até o final do prazo para interposição de ação rescisória.

§ 4º (VETADO)

§ 5º Os documentos cuja digitalização seja tecnicamente inviável devido ao grande volume ou por motivo de ilegibilidade deverão ser apresentados ao cartório ou secretaria ou encaminhados por meio de protocolo integrado judicial nacional no prazo de 10 (dez) dias contado do envio de petição eletrônica comunicando o fato, os quais serão devolvidos à parte após o trânsito em julgado. (Redação dada pela

Lei nº 14.318, de 2022) Vigência

§ 6º Os documentos digitalizados juntados em processo eletrônico estarão disponíveis para acesso por meio da rede externa pelas respectivas partes processuais, pelos advogados, independentemente de procuração nos autos, pelos membros do Ministério Público e pelos magistrados, sem prejuízo da possibilidade de visualização nas

secretarias dos órgãos julgadores, à exceção daqueles que tramitarem em segredo de justiça. (Incluído pela Lei nº 13.793, de 2019)

§ 7º Os sistemas de informações pertinentes a processos eletrônicos devem possibilitar que advogados, procuradores e membros do Ministério Público cadastrados, mas não vinculados a processo previamente identificado, acessem automaticamente todos os atos e documentos processuais armazenados em meio eletrônico, desde que demonstrado interesse para fins apenas de registro, salvo nos casos de processos em segredo de justiça. (Incluído pela Lei nº 13.793, de 2019)

Embora as expressões “assinatura eletrônica” e “assinatura digital” sejam frequentemente utilizadas como sinônimas, Menke (2018) esclarece que não coincidem:

Enquanto o termo “assinatura eletrônica” abrange o leque de métodos de comprovação de autoria mencionados, e até mesmo outros que possam vir a ser criados, a palavra “assinatura digital” refere-se exclusivamente ao procedimento de autenticação baseado na criptografia assimétrica. Essa modalidade de assinatura eletrônica, qual seja a assinatura digital baseada em criptografia assimétrica, foi a opção adotada pela Medida Provisória 2.200-2 de 2001.

Embora haja autores que, como Leite (2023), defendam que todos os documentos relativos a atos travados entre particulares, aí incluído o instrumento de mandato, poderiam ser submetidos a qualquer espécie de assinatura eletrônica, não lhes sendo aplicáveis as exigências da Lei 11.419/2006 (o que leva a autora a criticar a jurisprudência, inclusive do Superior Tribunal de Justiça), tal entendimento não se revela correto.

Uma distinção necessária precisa ser feita: o tratamento jurídico da assinatura dos atos processuais propriamente ditos não pode destoar do aplicável aos documentos destinados a produzir efeitos estritamente processuais, isto é, dos documentos destinados a comprovar o preenchimento dos pressupostos processuais e das condições da ação, notadamente o mandato judicial. Como se trata de documentos essenciais para evidenciar o cumprimento de verdadeiras condições de procedibilidade, é imprescindível garantir, com segurança, sua autenticidade e a integridade de seu conteúdo.

Assim, diversamente do que se pode admitir em relação aos contratos destinados a produzir efeitos *inter partes* – como uma prestação de serviços comum, e mesmo uma consultoria advocatícia não judicial – quando se trata de um documento a ser apresentado para evidenciar o cumprimento de pressuposto processual, a aplicabilidade da Lei 11.419/2006 é clara, como inclusive evidencia a jurisprudência do Superior Tribunal de Justiça (STJ) e se demonstrará adiante.

2) INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA (ICP-BRASIL)

A Medida Provisória nº 2.200-2/2001 instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), em seu art. 1º, e, no art. 2º, estabeleceu sua composição:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de

autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Explica Teixeira (2024, p. 337) a relevância da Infraestrutura de Chaves Públicas Brasileira, inclusive como instrumento garantidor da segurança da documentação de atos e negócios jurídicos:

(...) a MP n. 2.200-2/2001, ao criar a Infraestrutura de Chaves Públicas Brasileira – ICP-BRASIL –, instituiu o Comitê Gestor e uma rede de autoridades certificadoras subordinadas a ela, que mantêm os registros dos usuários e atestam a ligação entre as chaves privadas utilizadas nas assinaturas dos documentos e as pessoas que nelas apontam como emitentes das mensagens, garantindo a inalterabilidade dos seus conteúdos.

Assim, por meio deste mecanismo de segurança, permite-se às pessoas realizarem negociações no meio eletrônico com a confiabilidade de que as informações transmitidas estão seguras. Estes instrumentos eletrônicos possibilitam que se assinem contratos, obtenham-se informações sensíveis do Estado ou do setor privado, pratiquem-se atos processuais eletrônicos autorizados pela Lei n. 11.419/2006, entre outros.

A Autoridade Certificadora Raiz, primeira autoridade da cadeia de certificação, executora das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, é o Instituto Nacional de Tecnologia da Informação (ITI), autarquia federal, ao qual compete

(...) emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subsequente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê (...) (art. 5º)

O art. 6º da Medida Provisória estabeleceu as atribuições das entidades credenciadas em relação aos certificados digitais, a fim de viabilizar a segurança do sistema de certificação digital, por meio da vinculação idônea de cada par de chave pública-chave privada, ao passo que o art. 8º ditou quais entidades são passíveis de cadastramento como autoridades certificadoras e como autoridades de registro:

Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 8º Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Conforme se extrai do Portal do Governo Federal em relação à Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), trata-se de “cadeia hierárquica de confiança

que viabiliza a emissão de certificados digitais para identificação virtual do cidadão” (< <https://www.gov.br/iti/pt-br/assuntos/icp-brasil> >. Acesso em 24 mai. 2024). O portal esclarece que “o modelo adotado pelo Brasil foi o de certificação com raiz única” e que cabe ao Instituto Nacional de Tecnologia da Informação (ITI) “desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), (...) credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos”.

As informações disponíveis no portal evidenciam que há controle das entidades cadastradas e dotadas de capacidade técnica para realizar a identificação biométrica dos titulares de certificado digital (meio material de gravação da chave privada, que, em combinação com a chave pública, permite garantir a autenticidade de assinatura eletrônica qualificada), como se verifica no endereço eletrônico < <https://www.gov.br/iti/pt-br/assuntos/icp-brasil/lista-de-prestadores-de-servico-biometrico-psbio> >.

Tendo em consideração o objeto desta nota técnica, mostra-se essencial o disposto no art. 10, segundo o qual há presunção de veracidade das declarações constantes de documentos em forma eletrônica, em relação aos signatários, desde que produzidos com utilização de processo de certificação disponibilizado pela ICP-Brasil, isto é, por meio de assinatura mediante utilização de certificado digital:

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.

Como evidencia o § 2º, a utilização de modalidades de assinatura virtual não lançadas por meio de certificação digital assegurada pela ICP-Brasil ou o uso de outros meios de comprovação da autoria e integridade de documentos de forma eletrônica podem produzir efeitos *inter partes*, ou ser aceitos por particulares a quem for oposto o documento. Essas formas de prática de atos jurídicos, porém, não propiciam nível de certeza e segurança jurídica, de autenticidade suficiente para sua utilização com finalidades de interesse público, como a assinatura de documentos processuais, a assinatura de mandato judicial, ou a celebração de contratos que exijam formalidades especiais como requisito de validade.

Sobre os elementos envolvidos no processo de certificação digital, leciona Teixeira (2024, p. 338):

Cabe ponderar que o processo de certificação digital prescinde de três elementos para a consecução do seu fim (não constam nessa lista os softwares, drivers e hardwares necessários, por tratarem de requisitos pelos quais a mesma se viabiliza), a saber: certificado digital; assinatura digital; e uma normatização técnica positivada que regulamente o sistema de chaves digitais e os órgãos estatais fiscalizadores do sistema eletrônico.

Esses elementos respeitam a algumas necessidades, como: para que o documento eletrônico seja considerado juridicamente válido, é imprescindível que se possam identificar o autor, a localização e a data da sua autoria; que haja segurança quanto à integridade dos dados criados, de forma que inviabilize alteração; e que esse sistema seja regulamentado pelo Estado.

Por isso, ainda que talvez tardiamente, é importante conceituarmos assinatura digital e certificado eletrônico. Por certificado eletrônico entende-se o arquivo eletrônico gerado por uma Autoridade Certificadora, cuja função será a de identificar com segurança pessoas (físicas ou jurídicas) que emitiram determinado documento eletrônico mediante um par de chaves criptográficas. Estes certificados contêm dados do seu titular, como nome, números de documentos identificadores, entre outros, conforme regulamento da respectiva Política de Segurança da sua Autoridade Certificadora.

3) CLASSIFICAÇÃO DA ASSINATURA ELETRÔNICA

A Lei 14.063/2020 dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de *softwares* desenvolvidos por entes públicos.

Embora o inciso I do parágrafo único do art. 2º preveja expressamente que as disposições do capítulo II (Da assinatura eletrônica em interações com entes públicos) não se aplicam aos processos judiciais, inexistente óbice a que se apliquem a qualquer situação jurídica, pública ou privada, inclusive processual, os conceitos jurídicos constantes de tal capítulo; apenas não se podem fazer incidir às relações jurídicas processuais as regras de conduta nele previstas.

As principais definições estão contidas no art. 3º:

Art. 3º Para os fins desta Lei, considera-se:

I - autenticação: o processo eletrônico que permite a identificação eletrônica de uma pessoa natural ou jurídica;

II - assinatura eletrônica: os dados em formato eletrônico que se ligam ou estão logicamente associados a outros dados em formato eletrônico e que são utilizados pelo signatário para assinar, observados os níveis de assinaturas apropriados para os atos previstos nesta Lei;

III - certificado digital: atestado eletrônico que associa os dados de validação da assinatura eletrônica a uma pessoa natural ou jurídica;

IV - certificado digital ICP-Brasil: certificado digital emitido por uma Autoridade Certificadora (AC) credenciada na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), na forma da legislação vigente.

Em complementação, o art. 4º estabelece a classificação da assinatura eletrônica, conforme o grau de complexidade da estrutura viabilizadora e da segurança associada a cada tipo listado em tal dispositivo normativo:

Art. 4º Para efeitos desta Lei, as assinaturas eletrônicas são classificadas em:

I - assinatura eletrônica simples:

- a) a que permite identificar o seu signatário;
- b) a que anexa ou associa dados a outros dados em formato eletrônico do signatário;

II - assinatura eletrônica avançada: a que utiliza certificados não emitidos pela ICP-Brasil ou outro meio de comprovação da autoria e da integridade de documentos em forma eletrônica, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento, com as seguintes características:

- a) está associada ao signatário de maneira unívoca;

b) utiliza dados para a criação de assinatura eletrônica cujo signatário pode, com elevado nível de confiança, operar sob o seu controle exclusivo;

c) está relacionada aos dados a ela associados de tal modo que qualquer modificação posterior é detectável;

III - **assinatura eletrônica qualificada**: a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

§ 1º Os 3 (três) tipos de assinatura referidos nos incisos I, II e III do caput deste artigo caracterizam o nível de confiança sobre a identidade e a manifestação de vontade de seu titular, e a assinatura eletrônica qualificada é a que possui nível mais elevado de confiabilidade a partir de suas normas, de seus padrões e de seus procedimentos específicos.

§ 2º Devem ser asseguradas formas de revogação ou de cancelamento definitivo do meio utilizado para as assinaturas previstas nesta Lei, sobretudo em casos de comprometimento de sua segurança ou de vazamento de dados.

Leite (2023) explicita que “as assinaturas eletrônicas mais seguras valem-se de técnicas de vinculação que impedem a modificação do documento assinado, assegurando certeza não apenas quanto à identidade do signatário mas também quanto à integridade do documento”.

Segundo o Instituto Nacional de Tecnologia da Informação, a assinatura eletrônica avançada é a

provida por meio do portal Gov.br, a partir da Lei n. 14.063/20, que regula o tipo de assinatura a ser utilizado nas relações entre o cidadão e os serviços públicos. Todo cidadão tem acesso a essa modalidade de

assinatura desde que se qualifique ao modelo de autenticação existente no portal, de modo que quando a qualificação é prata ou ouro, pode-se ter acesso ao Portal de Assinatura Eletrônica. Esse é um serviço provido pelo ITI à Plataforma Gov.br gerida pela Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos (MGI). (<https://www.gov.br/iti/pt-br/assuntos/assinatura-eletronica-avancada> Acesso em 24 mai. 2024)

As informações disponíveis no portal eletrônico no ITI evidenciam que, por meio da assinatura eletrônica avançada, é possível assinar “um documento em meio digital a partir da sua conta GOV.BR, no Portal de Assinatura Eletrônica, ou em aplicações públicas integradas à Plataforma Gov.br, via API de integração provida pelo ITI”, que tais documentos extraem validade jurídica da Lei 14.063/2020, regulamentada pelo Decreto 10.543/2020, e que o serviço pode ser utilizado pelos detentores de contas “Gov.br” de níveis de segurança prata ou ouro (< <https://www.gov.br/iti/pt-br/assuntos/assinatura-eletronica-avancada> > Acesso em 24 mai. 2024).

Sobre o nível de resguardo de autenticidade de documento assinado por meio de certificação digital emitida por autoridade certificadora devidamente credenciada segundo o padrão ICP-Brasil (assinatura eletrônica qualificada), afirmam Arruda Alvim e Cunha (2023):

Para se saber se quem realizou o ato eletrônico foi mesmo a pessoa, o critério utilizado é o emprego de pontos ou fatores de autenticação, pontos estes que têm o objetivo essencial de demonstração deste liame com o signatário e que são exigidos no momento da assinatura do documento. Consistem em elementos que, em alguma medida, permitam a vinculação à pessoa, podendo ser decorrente de algo que a pessoa tenha em seu poder (por exemplo, um token), uma informação que apenas ela tem conhecimento (uma senha pessoal) ou, ainda, uma característica única pessoal (como a biometria), ou o acesso a algo que

somente a pessoa poderia ter (e-mail ou SMS com um token). Diversos são os métodos que podem ser empregados, de forma isolada ou conjunta (token + senha pessoal ou token + biometria, entre outros), de modo a se permitir a vinculação subjetiva àquele que é assinante do documento. Atualmente, tem sido comum, em diversas espécies de transações eletrônicas, ao menos, a utilização de dois pontos ou fatores de autenticação.

Essa possibilidade apenas é possível em razão da utilização de tecnologia que permita não só análise relacionada à autenticidade do documento, como, ainda, da sua integridade. A criptografia, tecnologia amplamente empregada nesta esteira, consiste no ato de encriptar o conteúdo do documento eletrônico, e é baseada no uso de chaves, que conferem efetiva segurança aos documentos eletrônicos. Entretanto, especificamente, estamos nos referindo à criptografia assimétrica, que trabalha com duas chaves distintas, uma que tem a função de cifrar e outra que decifra. Essa usualmente é a tecnologia utilizada com grande proveito e segurança nas assinaturas eletrônicas, mas não a única.

Quando se fala em criptografia assimétrica, há de se ter por presente a existência das duas chaves já referidas, isto é, as chaves privada e pública. A primeira é aquela que está no poder de determinada pessoa, sendo a ela vinculada, que permite com que ela realize a assinatura do documento, isto é, nesta situação específica, aquele que vai assinar o documento possui uma chave privada e, com esta, irá cifrar o documento. O decifrar deste documento, para conferência da sua autenticidade (considerando os já referidos pontos de autenticação) e integridade, é viável por meio da utilização de uma chave pública.

Quando se fala em assinatura eletrônica, se tem, essencialmente, um conjunto de dados, no formato eletrônico, que em razão da evoluída tecnologia empregada, por meio de diversos dispositivos ou sistemas (cujos contornos podem variar a depender da tecnologia envolvida), permitem o reconhecimento com substancial segurança da autenticidade e integridade. O sistema e a tecnologia empregados, além de terem

mecanismos para a averiguação da autenticidade ou segurança do documento, em igual medida, não de ter instrumentos aptos a assegurar a integridade do documento ou, melhor dizendo, a vinculação em relação ao signatário, para se manter, depende da inalterabilidade do documento, na medida em que o documento eletrônico, isto é, o conjunto de dados permanece não só vinculado ao signatário, mas com os mesmos contornos existentes no momento em que a assinatura eletrônica foi realizada, ou seja, permanece íntegro.

Exatamente nesta esteira, a MP 2.200-2/2001 é expressa ao tratar da possibilidade de que se reconheça os mesmos efeitos da assinatura física aos documentos em forma eletrônica. (...)

Teixeira (2024, p. 336-337) complementa:

A criptografia é um método matemático que cifra uma mensagem em código, ou seja, transforma-a em caracteres indecifráveis. Cabe esclarecer que a criptografia pode ser simétrica ou assimétrica.

Em razão da segurança, a que mais se utiliza é a criptografia assimétrica. Ela cria um código e uma senha para decifrá-lo, isto é, concebem-se duas chaves: uma chave privada, que codifica a mensagem, e outra chave pública, que decodifica a mensagem. Entretanto, o inverso também pode ocorrer, ou seja, a pública serve para codificar e a privada para decodificar. O emissor da mensagem fica com a chave privada, e os destinatários de suas mensagens ficam com a chave pública. Esse sistema dá segurança aos negócios efetuados na internet, devendo ser controlado por uma terceira entidade, que é a autoridade certificadora, conhecida, de igual modo, como tabelião virtual, que irá conferir a autenticação digital das assinaturas e dos documentos. Por sua vez, a criptografia simétrica cria uma mesma chave para criptografar e decifrar.

Na prática, para possibilitar a assinatura digital, a certificadora fornece ao usuário, em regra, mediante pagamento, um *kit* que contempla: um *smart card*, uma leitora a ser acoplada a um computador e o cadastramento de uma senha (o *smart card* e a leitora podem ser substituídos por um *token*, semelhante a um *pen drive* que é utilizado pelo acoplamento no computador e senha previamente cadastrada).

4) CONSIDERAÇÕES SOBRE O MANDATO JUDICIAL

Em relação aos contratos de mandato em geral, dispõe o art. 657 do Código Civil: “A outorga do mandato está sujeita à forma exigida por lei para o ato a ser praticado. Não se admite mandato verbal quando o ato deva ser celebrado por escrito”.

Como regra, não se pode invocar, a não ser supletivamente, nem essa norma - que frequentemente resulta em reduzidas exigências em termos de requisitos formais para outorga de mandato - nem as demais normas que regem essa espécie contratual, em virtude da clara previsão do art. 692, também do Código Civil: “O mandato judicial fica subordinado às normas que lhe dizem respeito, constantes da legislação processual, e, supletivamente, às estabelecidas neste Código”.

Pelas mesmas razões, diversamente do que se verifica em relação aos contratos em geral, não se aplica ao mandato judicial, em regra, a norma do art. 107 do CCB: “A validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir”.

A específica norma aplicável ao mandato judicial é o art. 105 do Código de Processo Civil (CPC):

Art. 105. A procuração geral para o foro, outorgada por instrumento público ou particular **assinado pela parte**, habilita o advogado a praticar

todos os atos do processo, exceto receber citação, confessar, reconhecer a procedência do pedido, transigir, desistir, renunciar ao direito sobre o qual se funda a ação, receber, dar quitação, firmar compromisso e assinar declaração de hipossuficiência econômica, que devem constar de cláusula específica.

§ 1º A procuração **pode ser assinada digitalmente, na forma da lei.**

(...)

Diante da imprescindibilidade de outorga do mandato judicial na forma escrita, por instrumento público (que tem sido considerado obrigatório no caso do analfabeto) ou particular, com assinatura da parte, que pode ser digital, “na forma da lei”, é necessário perquirir a legislação aplicável.

Como já apontado, a norma legal processual que dispõe a respeito, em relação ao processo eletrônico (único modelo processual de que cabe tratar, diante da determinação do Conselho Nacional de Justiça de eliminação dos processos físicos, com evidentes vantagens em termos de eficiência judiciária), é o art. 1º, III, da Lei n. 11.419/2006, o qual admite duas modalidades de assinatura eletrônica: a lançada mediante certificado digital emitido por Autoridade Certificadora credenciada, na forma da legislação aplicável, ou a aposta mediante informação de usuário e senha, após regular cadastro de usuário no órgão do Poder Judiciário, conforme disciplinado pelos tribunais e pelo Conselho Nacional de Justiça.

No caso do mandato judicial, somente a primeira hipótese prevista no referido diploma legislativo é aplicável, uma vez que o cadastro de usuários apenas se aplica a advogados e auxiliares da justiça, como peritos e leiloeiros, e não aos mandantes (autores, réus, intervenientes diversos).

Relevante também atentar para o disposto nos art. 195, 411, 439, 440 e 441 do CPC:

Art. 195. O registro de ato processual eletrônico deverá ser feito em padrões abertos, que atenderão aos requisitos de autenticidade, integridade, temporalidade, não repúdio, conservação e, nos casos que tramitem em segredo de justiça, confidencialidade, **observada a infraestrutura de chaves públicas unificada nacionalmente, nos termos da lei.**

Art. 411. Considera-se autêntico o documento quando:

I - o tabelião reconhecer a firma do signatário;

II - a autoria estiver identificada por qualquer outro meio legal de certificação, **inclusive eletrônico, nos termos da lei;**

III - não houver impugnação da parte contra quem foi produzido o documento.

Art. 439. A utilização de documentos eletrônicos no processo convencional dependerá de sua conversão à forma impressa e da verificação de sua autenticidade, na forma da lei.

Art. 440. O juiz apreciará o valor probante do documento eletrônico não convertido, assegurado às partes o acesso ao seu teor.

Art. 441. Serão admitidos documentos eletrônicos produzidos e conservados com a observância da legislação específica.

Mostra-se igualmente admissível, claro, a possibilidade de comprovação da outorga de mandato por meio de apresentação de cópia digitalizada¹ de procuração regularmente outorgada nos termos do *caput* do art. 105 do CPC.

Resta avaliar a possibilidade de se admitir a comprovação da outorga de mandato judicial por meio de outras espécies de assinatura eletrônica, diversas da qualificada (assinatura digital lançada por meio de certificado do padrão ICP-Brasil).

Nos diversos casos de aparentes focos de litigiosidade anômala que levaram ao estudo registrado nesta nota técnica, caracterizados pela atuação massiva de profissionais que informaram inscrição originária e endereço em Estados da federação muito distantes do domicílio dos contratantes, pareceu haver indício de ausência de contato pessoal com o mandante, o que suscitou dúvidas em relação à real observância do caráter *intuitu personae* de que o mandato, notadamente o judicial, deve se revestir (STJ, REsp n. 1.346.171/PR, relator Ministro Luis Felipe Salomão, Quarta Turma, julgado em 11/10/2016, DJe de 7/11/2016), e talvez explique o fato de que, embora as ações ajuizadas às centenas ou milhares em curto espaço de tempo – muitas vezes em diversos Estados da federação – refiram-se a conflitos de natureza eminentemente fática, não apresentam, na causa de pedir, qualquer dos detalhes factuais que seria de razoavelmente se esperar.

O caráter personalíssimo é, de fato, característico do contrato de mandato, “por estar assentado na confiança depositada reciprocamente”, como lecionam Farias e Rosenvald (2023, p. 1.202). Desse modo, a identidade do mandante e do mandatário, suas características pessoais e, no caso do mandato celebrado para prestação de serviços profissionais, as habilidades e competências do mandatário, são fundamentais para sua escolha, a fim de atuar no interesse do mandante, e para o aperfeiçoamento da contratação.

¹ A definição legal de digitalização está contida no art. 1º da Lei nº 12.682/2012:
Art. 1º A digitalização, o armazenamento em meio eletrônico, óptico ou equivalente e a reprodução de documentos públicos e privados serão regulados pelo disposto nesta Lei.
Parágrafo único. Entende-se por digitalização a conversão da fiel imagem de um documento para código digital.

No mesmo sentido a lição de Gagliano e Pamplona Filho (2020, p. 547):

(...) o mandato é um contrato *individual e personalíssimo*, ou seja, celebrado *intuitu personae*, em que a figura do contratante tem influência decisiva para a celebração do negócio, sendo razoável afirmar, inclusive, que a pessoa do contratante se torna um elemento causal do negócio.

Essa lição doutrinária, em relação ao mandato conferido ao advogado, encontra integral respaldo nos artigos 10, 11, 2º, VII, 5º e 7º do Código de Ética e Disciplina da OAB:

Art. 10. As relações entre advogado e cliente baseiam-se na confiança recíproca. Sentindo o advogado que essa confiança lhe falta, é recomendável que externar ao cliente sua impressão e, não se dissipando as dúvidas existentes, promova, em seguida, o substabelecimento do mandato ou a ele renuncie.

Art. 11. O advogado, no exercício do mandato, atua como patrono da parte, cumprindo-lhe, por isso, imprimir à causa orientação que lhe pareça mais adequada, sem se subordinar a intenções contrárias do cliente, mas, antes, procurando esclarecê-lo quanto à estratégia traçada.

Art. 2º O advogado, indispensável à administração da Justiça, é defensor do Estado Democrático de Direito, dos direitos humanos e garantias fundamentais, da cidadania, da moralidade, da Justiça e da paz social, cumprindo-lhe exercer o seu ministério em consonância com a sua elevada função pública e com os valores que lhe são inerentes.

Parágrafo único. São deveres do advogado:
(...)

VII – desaconselhar lides temerárias, a partir de um juízo preliminar de viabilidade jurídica;

(...)

Art. 5º O exercício da advocacia é incompatível com qualquer procedimento de mercantilização.

Art. 7º É vedado o oferecimento de serviços profissionais que implique, direta ou indiretamente, angariar ou captar clientela.

5) POSICIONAMENTO DO SUPERIOR TRIBUNAL DE JUSTIÇA EM RELAÇÃO À ASSINATURA ELETRÔNICA

O Superior Tribunal de Justiça, intérprete máximo da legislação infraconstitucional, vem deixando claro que formas de “assinatura” de documento que resultem em aposição de assinatura “escaneada”, desenhada ou estilizada de qualquer forma não se confundem com a assinatura lançada por meio de certificação digital e com ela não podem ser equiparadas, por não garantirem o mesmo nível de autenticidade e segurança jurídica, inclusive em relação à representação processual:

PROCESSO PENAL. AGRAVO REGIMENTAL NO AGRAVO EM RECURSO ESPECIAL. 1) AGRAVO EM RECURSO ESPECIAL NÃO CONHECIDO. APLICAÇÃO DO ART. 21-E, V, DO REGIMENTO INTERNO DO SUPERIOR TRIBUNAL DE JUSTIÇA - RISTJ.

INSTRUMENTO DE MANDATO SUBSTABELECIMENTO COM ASSINATURA DIGITALIZADA OU ESCANEADA. AUSÊNCIA DE VALIDADE. REGULARIZAÇÃO DO VÍCIO NÃO REALIZADA PELA DEFESA. 2) HABEAS CORPUS DE OFÍCIO PARA ANÁLISE DAS TESES DEDUZIDAS NO RECURSO ESPECIAL. NÃO CABIMENTO. DESPROVIDO.

1.Descabido o conhecimento do agravo em recurso especial monocraticamente quando a parte deixa de regularizar a representação processual (art. 932, III e parágrafo único, do Código de Processo Civil - CPC).

1.1. No caso em tela, **a assinatura constante do substabelecimento foi digitalizada ou escaneada, o que não se admite, pois a "assinatura digitalizada ou escaneada, por se tratar de mera inserção de imagem em documento, não se confunde com a assinatura digital baseada em certificado digital emitido por autoridade certificadora credenciada, prevista no art. 1º, § 2º, III, "a", da Lei n. 11.419/2006"** (AgInt no AREsp 1173960/RJ, Rel. Ministro Antonio Carlos Ferreira, Quarta Turma, DJe de 15/3/2018)

1.2. Ademais, **"a reprodução de uma assinatura, por meio do escaneamento, sem qualquer regulamentação, é arriscada na medida em que pode ser feita por qualquer pessoa que tenha acesso ao documento original e inserida em outros documentos. Não há garantia alguma de autenticidade, portanto. A aplicação do princípio da instrumentalidade das formas, invocado pelas recorrentes, deve encontrar limites exatamente no princípio da segurança jurídica. Não se trata de privilegiar a forma pela forma, mas de conferir aos jurisdicionados, usuários das modernas ferramentas eletrônicas, o mínimo de critérios para garantir a autenticidade e integridade de sua identificação no momento da interposição de um recurso ou de apresentação de outra peça processual"** (REsp n. 1.442.887/BA, Terceira Turma, relatora Ministra Nancy Andrichi, DJe de 14/5/2014).

(...)

3. Agravo regimental desprovido. (STJ, AgRg no AREsp n. 1.404.523/SP, relator Ministro Joel Ilan Paciornik, Quinta Turma, julgado em 17/10/2019, DJe de 25/10/2019; grifos nossos)

São diversos os julgados a respeito, no mesmo sentido, o que evidencia tratar-se de jurisprudência consolidada no STJ:

AGRAVO REGIMENTAL NO AGRAVO (ARTIGO 544 DO CPC) - AÇÃO DE CUMPRIMENTO DE OBRIGAÇÃO DE NÃO FAZER C/C REPARAÇÃO DE DANOS - DECISÃO MONOCRÁTICA NEGANDO SEGUIMENTO AO APELO EXTREMO - INSURGÊNCIA RECURSAL DA AUTORA.

1. A certificação digital é ato pessoal e intransferível, portanto a assinatura digital constante da petição do recurso deve corresponder a advogado com procuração nos autos, sob pena de incidência do enunciado n. 115 da Súmula do STJ.

2. Hipótese em que o advogado titular do certificado digital, utilizado para assinar a transmissão eletrônica do agravo regimental, não possui instrumento de procuração nos autos. Recurso inexistente. Incidência da Súmula 115 do STJ. Vício não sanável por juntada posterior de mandato ou substabelecimento, uma vez inaplicável o disposto no artigo 13 do CPC na instância extraordinária. Precedentes.

3. Agravo regimental não conhecido. (STJ, AgRg no AREsp n. 286.636/SP, relator Ministro Marco Buzzi, Quarta Turma, julgado em 13/10/2015, DJe de 21/10/2015.)

PROCESSUAL CIVIL. AGRAVO REGIMENTAL NO RECURSO ESPECIAL. SERVIDOR PÚBLICO FEDERAL. AUSÊNCIA DE

INSTRUMENTO DE PROCURAÇÃO OU SUBSTABELECIMENTO OUTORGADO AO ADVOGADO SUBSCRITOR DO RECURSO ESPECIAL. RECURSO ASSINADO ELETRONICAMENTE. IRREGULARIDADE DE REPRESENTAÇÃO. INCIDÊNCIA DA SÚMULA 115/STJ. PRECEDENTES. AGRAVO REGIMENTAL NÃO PROVIDO.

(...)

2. **"A jurisprudência do STJ passou a considerar que a identificação de quem peticiona nos autos é a proveniente do certificado digital,** independentemente da assinatura que aparece na visualização do arquivo eletrônico. 2. Ocorre que, in casu, o signatário da petição eletrônica não possui instrumento de procuração nos autos, o que obsta o conhecimento do recurso, ante a incidência da Súmula 115/STJ" (AgRg no AREsp 398.520/RN, Rel. Ministro Herman Benjamin, Segunda Turma, julgado em 21/11/2013, DJe 06/12/2013).

3. "Compete à parte zelar pela correta representação processual no ato da interposição do recurso, sob pena de não conhecimento da irresignação, sendo descabida a alegação de que, a despeito da ausência de instrumento de procuração/substabelecimento, o signatário do recurso estaria cadastrado no sistema processual do Tribunal e que seu nome constaria das intimações realizadas anteriormente, circunstâncias estas que não tem o condão de comprovar a regular representação processual, caso em que se mostra indispensável a apresentação do instrumento de procuração ou substabelecimento" (AgRg no REsp 1450269/RJ, Rel. Ministro Mauro Campbell Marques, Segunda Turma, julgado em 25/11/2014, DJe 02/12/2014).

4. Agravo regimental não provido. (STJ, AgRg no REsp n. 1.525.128/SE, relator Ministro Mauro Campbell Marques, Segunda Turma, julgado em 20/8/2015, DJe de 31/8/2015, grifos nossos)

AGRAVO REGIMENTAL NO AGRAVO (ARTIGO 544 DO CPC) - AÇÃO RENOVATÓRIA DE LOCAÇÃO - DECISÃO MONOCRÁTICA NEGANDO PROVIMENTO AO RECLAMO, MANTIDA A INADMISSÃO DO RECURSO ESPECIAL CONSIDERADO INEXISTENTE.

1. **Hipótese em que consta a assinatura digitalizada, a qual não se confunde com a firma digital ou eletrônica, por consubstanciar mera cópia do documento original.** Recurso inexistente. Vício não sanável por juntada posterior de mandato ou substabelecimento, uma vez inaplicável o disposto no artigo 13 do CPC na instância extraordinária. Precedente da Corte Especial.

2. Agravo regimental desprovido. (STJ, AgRg no AREsp n. 626.680/SP, relator Ministro Marco Buzzi, Quarta Turma, julgado em 2/6/2015, DJe de 11/6/2015, grifos nossos)

AGRAVO INTERNO. RECURSO ESPECIAL. REPRESENTAÇÃO PROCESSUAL. CADEIA COMPLETA. AUSÊNCIA. INTIMAÇÃO. ARTS. 76 E 932, PARÁGRAFO ÚNICO, DO CPC. DESATENDIMENTO. SUBSCRITOR DO RECURSO. ASSINATURA ELETRÔNICA. RESP NÃO CONHECIDO. INCIDÊNCIA DA SÚMULA N. 115/STJ. PRECEDENTES.

(...)

2. **"O STJ possui orientação de que, por se tratar de mera inserção de imagem em documento, a assinatura digitalizada ou escaneada não se confunde com a assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, e, por isso, não tem valor"** (AgInt nos EAREsp n. 1.555.548/RJ, relator Ministro Herman Benjamin, Corte Especial, julgado em 2/8/2021, DJe de 16/8/2021).

3. Deixando a parte transcorrer o prazo sem que a representação processual seja regularizada, é inexistente o recurso dirigido a esta Casa, nos termos do enunciado n. 115 da Súmula.

4. Agravo interno a que se nega provimento. (STJ, AgInt no REsp n. 2.033.696/SP, relatora Ministra Maria Isabel Gallotti, Quarta Turma, julgado em 27/11/2023, DJe de 30/11/2023, grifos nossos)

PROCESSUAL CIVIL. EMBARGOS DE DIVERGÊNCIA. PROCESSO INFORMATIZADO. LEI 11.419/2006 E RESOLUÇÃO STJ 1/2010. TITULAR DO CERTIFICADO DIGITAL COM PROCURAÇÃO NOS AUTOS. IRRELEVÂNCIA DA AUSÊNCIA DE MENÇÃO DO NOME DO SIGNATÁRIO DIGITAL NA PETIÇÃO REMETIDA ELETRONICAMENTE.

1. Controverte-se acerca da interpretação do art. 1º, § 2º, III, da Lei 11.419/2006, quando, no processamento de petição eletrônica, o nome do advogado titular do certificado digital não se identifica com o do subscritor da peça processual, embora aquele possua poderes para representar a parte.

2. De acordo com o entendimento da Corte Especial do STJ, "A prática eletrônica de ato judicial, na forma da Lei n. 11.419/2006, reclama que o titular do certificado digital utilizado possua procuração nos autos, sendo irrelevante que na petição esteja ou não grafado o seu nome" (AgRg no REsp 1.347.278/RS, Rel. Ministro Luis Felipe Salomão, DJe 1º.8.2013).

3. É a assinatura eletrônica que legitima a prática do ato processual e que confere sua autoria. Continuar identificando o autor da petição pelo nome que aparece subscrito na peça é concepção que não se coaduna com o espírito da Lei 11.419/2006.

(...) (STJ, EREsp n. 1.326.823/AM, relator Ministro Herman Benjamin, Corte Especial, julgado em 3/6/2015, DJe de 20/11/2015, grifos nossos)

AGRAVO REGIMENTAL. AÇÃO PENAL ORIGINÁRIA. PROTOCOLO E ASSINATURA DO RECURSO POR MEIO ELETRÔNICO. ADVOGADO TITULAR DO CERTIFICADO DIGITAL QUE NÃO POSSUI PROCURAÇÃO NOS AUTOS. RECURSO INEXISTENTE. SUM. 115/STJ.

1. A utilização do meio eletrônico de peticionamento exige a observância das regras próprias previstas na Lei 11.419/2006, em especial, para a hipótese sob análise, o disposto no art. 2º, inc. III, alínea "a", segundo o qual, **a assinatura eletrônica, baseada em certificado digital emitido por Autoridade Certificadora credenciada, considera-se "forma de identificação inequívoca do signatário"**.

2. A opção pela utilização do meio eletrônico de peticionamento implica na vinculação do advogado titular do certificado digital ao documento chancelado, considerando-se-o, para todos os efeitos, o subscritor da peça. Precedentes.

3. **Não tem valor eventual assinatura digitalizada**, de outro advogado, que venha constar da peça encaminhada e assinada eletronicamente, mesmo que este possua procuração, dada a impossibilidade de aferição de sua autenticidade e também porque essa modalidade de assinatura - de fácil reprodução por qualquer pessoa no âmbito digital - não possui qualquer regulamentação legal.

4. Na hipótese, considerando que o advogado que assinou eletronicamente os agravos regimentais não possui procuração nos autos, tem-se por inexistente ambos os recursos, ex vi do enunciado nº 115 da Súmula/STJ.

5. Agravos regimentais não conhecidos. (STJ, AgRg na APn n. 675/GO, relatora Ministra Nancy Andrighi, Corte Especial, julgado em 3/12/2014, DJe de 12/12/2014, grifos nossos)

PROCESSO CIVIL. AGRAVO INTERNO NO AGRAVO EM RECURSO ESPECIAL. AÇÃO COMINATÓRIA CUMULADA COM COMPENSAÇÃO POR DANO MORAL. PLANO DE SAÚDE. RECURSO SUBSCRITO POR ADVOGADO SEM PROCURAÇÃO NOS AUTOS. REPRESENTAÇÃO PROCESSUAL. ASSINATURA DIGITALIZADA. IMPOSSIBILIDADE. INCIDÊNCIA DA SÚMULA 115/STJ.

(...)

4. É firme o entendimento de que, por se tratar de mera inserção de imagem em documento, a assinatura digitalizada ou escaneada não se confunde com a assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada.

5. Agravo interno não provido. (STJ, AgInt no AREsp n. 1.691.485/PE, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 19/10/2020, DJe de 21/10/2020.)

Importa ressaltar que, embora em alguns dos julgados acima mencionados a discussão estivesse mais relacionada à assinatura lançada por advogado, a *ratio decidendi* adotada pelo Superior Tribunal de Justiça evidencia que, no processo eletrônico, a única forma de assinatura eletrônica apta a cumprir os requisitos exigidos pela Lei nº 11.419/2006, notadamente no art. 1º, § 2º, III, “a”, é a lançada mediante certificado digital emitido por autoridade certificadora cadastrada em conformidade com a ICP-Brasil.

Ademais, vale repetir ser firme o posicionamento do STJ no sentido de que não é juridicamente admissível qualquer forma de aposição de assinatura, especialmente em instrumento de mandato, mediante escaneamento, montagem ou desenho por meio de ferramenta virtual, por não viabilizar garantia de autenticidade.

6) MODALIDADES DE ASSINATURA ADMISSÍVEIS NO INSTRUMENTO DE MANDATO JUDICIAL

A conclusão a que todos esses fundamentos conduzem – de que o mandato judicial pode apresentar assinatura lançada manualmente (e ser integralmente digitalizado para inserção no sistema de processo eletrônico, o que é totalmente diverso de digitalização apenas da assinatura, para posterior montagem no documento) ou assinatura eletrônica qualificada (lançada mediante certificado digital do padrão ICP-Brasil) – realmente não poderia ser diversa, pois essas duas espécies de assinatura têm peculiaridades e meios de resguardo de integridade documental e conferência de autenticidade muito semelhantes.

A assinatura lançada manualmente é caracterizada por individualização, propiciada por meio de traços, inclinação, formato de letras, força com que é aposta, e, diante de questionamento, sua autenticidade pode ser averiguada mediante perícia grafotécnica. Por outro lado, a autenticidade de assinatura eletrônica qualificada pode ser verificada por meio de um par de chaves (pública-privada) vinculado a certificação digital emitida por entidade certificadora credenciada pela ICP-Brasil, como previsto na legislação vigente.

As similaridades referidas são também destacadas por Teixeira (2024, p.339-340):

(...) assinatura digital é um código anexado ou logicamente associado a um arquivo eletrônico que confere de forma única e exclusiva a comprovação da autenticidade e confiabilidade quanto à integridade do conjunto de dados do referido documento conforme o original.

Poder-se-ia até dizer que, guardadas as devidas peculiaridades distintas, a assinatura digital equipara-se à assinatura manuscrita, uma vez que possibilita a comprovação de que tal documento eletrônico foi

criado pelo autor; ou manifesta uma vontade identificada por ele, na forma da lei. A propósito, a legislação aplicável que confirma a aceitação e a validade jurídica da assinatura digital é a Lei n. 11.419/2006, art. 2º, bem como o CPC de 2015, arts. 193, caput, 205, § 2º, e 943 [CPC de 1973, arts. 154, § 2º, e 164, parágrafo único].

O autor, assim como firmemente apontado pelo Superior Tribunal de Justiça, destaca a fragilidade da assinatura digitalizada, mera reprodução ou “colagem” de imagem, desprovida de aptidão para conferir autenticidade a documento:

Muitas vezes utilizada como “alternativa”, existe a conhecida assinatura digitalizada, que é um arquivo de imagem por excelência, formado por escaneamento ou captura.³⁶⁸ Ocorre que a assinatura digitalizada é elemento frágil, na medida em que pode ser replicado indistintamente via um simples comando de “copiar” e “colar” ou em um “*print screen*”, de modo que não gera a presunção suficiente sobre a autenticidade do documento. (Op. cit., p. 341)

Outras formas de “assinatura virtual”, como, por exemplo, as que utilizam “certificados” emitidos por entidades não credenciadas pelo ITI (e que, portanto, não gozam da garantia de autenticidade e integridade conferida pelo padrão ICP-Brasil), as que se valem do envio de fotografia e dados de geolocalização, e-mail, usuário e senha, dados de equipamentos eletrônicos etc., não garantem nível de segurança jurídica que permita sua utilização para finalidades de interesse público, prática de atos processuais e comprovação da presença das condições da ação e dos pressupostos processuais. É o caso, repita-se, do mandato judicial, que não se destina a produzir efeito apenas diante dos contratantes, mas deve valer diante do próprio Estado (Poder Judiciário), para resguardar a validade da representação processual.

Não se podem perder de vista a notória facilidade com que tais dados, informações e documentos de identificação (nome, e-mail, senha, número de documentos, fotografias) podem ser obtidos, inclusive na própria rede mundial de computadores, e a igual facilidade com que documentos não devidamente protegidos podem ser corrompidos.

Ao se aplicar a classificação estabelecida no art. 4º da Lei nº 14.063/2020, todas essas modalidades de serviços (não resguardados pelo padrão ICP-Brasil, nem pela modalidade de assinatura avançada do Portal Gov.br) resultam em assinatura eletrônica simples, que apresenta reduzido nível de segurança, em termos de autenticidade:

A assinatura eletrônica simples permite a identificação do signatário, bem como anexa dados a outros dados em formato eletrônico do signatário (art. 4º, inc. I).

Embora seja utilizado o termo “simples”, na realidade tal tipo de assinatura exige certos níveis de segurança, podendo-se utilizar de informações como a coleta do endereço de IP (endereço de protocolo de internet)³⁷⁰, geolocalização, o preenchimento de um formulário ou até mesmo a marcação de uma caixa de seleção a fim de confirmar que o signatário externou sua vontade.

Tratando-se da validade da assinatura eletrônica simples, faz-se necessário lembrar o teor do art. 107 do Código Civil, ao prever que “a validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir”.

Evidente que, a vinculação entre a assinatura e seu signatário na assinatura eletrônica simples se trata do seu maior problema, pois um estranho pode se passar com relativa facilidade pelo signatário em razão da simplicidade dos meios empregados em tal modalidade de assinatura.

Contudo, embora tenha uma conexão um tanto quanto frágil com seu signatário, a assinatura eletrônica simples pode ser utilizada como declaração de vontade, salvo quando a lei expressamente exige forma especial. (TEIXEIRA, 2024, p. 342-343)

Sobre a necessidade de se resguardar a segurança jurídica, especialmente diante da prática de atos e produção de documentos em meio eletrônico, importante destacar também as lições de Menke (2018):

A necessidade de incrementar a segurança técnica e jurídica advém da realidade de que existem vulnerabilidades que são intensificadas no meio eletrônico, especialmente no que diz respeito: à identificação, em sentido amplo; à autoria de declarações de vontade, bem como à integridade dos documentos eletrônicos, ou seja, quanto ao fato de que não foram alterados em seu percurso virtual.

Veja-se que o Guia para a incorporação ao direito interno da lei modelo de assinaturas eletrônicas da Uncitral alerta que no ambiente eletrônico o original de uma mensagem é indistinguível da cópia, não comporta uma assinatura manuscrita e não é veiculado em papel. Além disso, o potencial para a ocorrência de fraudes é considerável, devido às facilidades de interceptação e de alteração, sem detecção, da informação sob a forma eletrônica e à velocidade de processamento de múltiplas transações.

7) AMOSTRAGEM COLHIDA PELA EQUIPE DE SUPORTE ESTRATÉGICO E COOPERAÇÃO DA DIREÇÃO DO FORO DA COMARCA DE BELO HORIZONTE

No período de 07/10/2023 a 23/02/2024, o setor de Suporte Estratégico e Cooperação da Direção do Foro da comarca de Belo Horizonte, sob a supervisão do Juiz Sérgio Henrique Cordeiro Caldas Fernandes, Juiz Auxiliar da Corregedoria e Diretor do Fórum da Capital, e do Magistrado Guilherme Lima Nogueira da Silva, Juiz de Direito Auxiliar da comarca de Belo Horizonte, empreendeu análise jurimétrica quantitativa e qualitativa dos feitos distribuídos nas Varas Cíveis (1ª a 36ª Varas Cíveis), a fim de detectar quais continham documentos – notadamente procuração e declaração de pobreza – assinados eletronicamente, e quais os fornecedores de serviços de assinatura eletrônica utilizados em cada feito.

Foram encontrados 247 processos contendo documentos assinados eletronicamente (excluídas, claro, as assinaturas lançadas por meio do próprio sistema PJe). Efetuada a análise detalhada, identificou-se que 19 diferentes fornecedoras do serviço de assinatura eletrônica foram utilizadas; em 95 processos, foi utilizada geolocalização do “signatário”; em 90, captação de fotografia; em 149 feitos, utilizou-se e-mail; constatou-se utilização de QR-Code em 148 processos.

A avaliação evidenciou a ausência de padronização em relação aos diversos serviços de “assinadores digitais” disponibilizados no mercado e contratados para assinatura de documentos, inclusive e especialmente no que diz respeito a procurações e declarações de pobreza.

Na amostragem encontrada, identificou-se que, em 120 processos, utilizou-se a fornecedora de serviços Zapsign by Truora, a mais usada, seguida da Adobe Acrobat (utilizada em 28 processos) e do uso da assinatura da plataforma Gov.br (identificada em 26 processos).

O gráfico a seguir ilustra todas as prestadoras de serviços identificadas nos processos analisados:



Cumpra-se observar que o fato de as prestadoras de serviços terem sido identificadas no gráfico como “certificadoras” não significa que constituam Autoridades Certificadoras credenciadas pela ICP-Brasil, como exigido pela Medida Provisória nº 2.200-2/2001; muitas delas nem sequer estão autorizadas pelo ITI a emitir certificado digital para viabilizar o lançamento de assinatura eletrônica qualificada.

Também é fundamental registrar que mesmo entidades credenciadas pela ICP-Brasil como Autoridades Certificadoras – e, portanto, aptas à emissão de certificação digital – costumam fornecer, no mercado, outras espécies menos seguras (e, em regra, mais baratas) de serviços de assinatura eletrônica, como os que envolvem uso de geolocalização, uso de e-mail e lançamento de assinaturas escaneadas ou desenhadas. É o caso, por exemplo, da Certisign, que, embora seja a Autoridade Certificadora de 1º Nível na estrutura do ITI (como se pode conferir em <https://estrutura.iti.gov.br/>), também fornece uma grande variedade de serviços diversos da certificação digital, como se vê em seu portal na internet. Essa gama de serviços recebeu o nome de “Izsign”, e envolve diferentes níveis de segurança de assinatura eletrônica e digital, mediante uso de “SMS Token”, “Biometria facial” e “E-mail registrado com emissão de certificado” (Disponível em: < <https://izisign.com.br/Home/Planos> >. Acesso em 24 mai. 2024).

Desse modo, ao se avaliar se determinada assinatura eletrônica é ou não qualificada (ou, de qualquer modo, deve ser reputada válida, autêntica ou suficiente para imprimir força probatória ao documento, conforme o caso), é necessário que se verifique não apenas se o fornecedor de serviço de assinatura eletrônica é credenciado como Autoridade Certificadora pelo Instituto Nacional de Tecnologia da Informação, mas também se, no caso concreto que se avalia, a forma de assinatura efetivamente utilizada é adequada a oferecer o nível de autenticidade exigido pela espécie de fato ou ato jurídico em questão.

8) ASSINATURA ELETRÔNICA DE DOCUMENTOS DESTINADOS A COMPROVAR FATOS JURÍDICOS MATERIAIS

Em relação à assinatura eletrônica de documentos apresentados para comprovar fatos ou atos jurídicos materiais, deverão ser consideradas as normas jurídicas aplicáveis aos negócios jurídicos em geral e a cada fato ou ato específico, entre elas os artigos 107 e 219 do Código Civil:

Art. 107. A validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir.

Art. 219. As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários.

Parágrafo único. Não tendo relação direta, porém, com as disposições principais ou com a legitimidade das partes, as declarações enunciativas não eximem os interessados em sua veracidade do ônus de prová-las.

Assim, por exemplo, se, com o objetivo de demonstrar a celebração de um contrato de compra e venda de bem móvel, ou de um contrato de crédito, for apresentado instrumento negocial que apresente assinatura “desenhada”, acompanhada de dados de geolocalização e/ou fotografia de uma das partes (ou de ambas, a depender do caso), caberá ao Magistrado, em cada caso, avaliar a suficiência da prova da contratação, a partir das exigências formais de validade, em relação à espécie de contrato em questão, à aceitação ou não, pelas partes, da forma de contratação, e inclusive à configuração ou não, nos autos, de controvérsia acerca da negociação, após a juntada do instrumento negocial.

A necessidade de avaliar, em cada caso específico, a validade de eventual documento destinado a provar fato ou ato material assinado de modo eletrônico – embora não com certificado digital – decorre inclusive do disposto no § 2º do art. 10 da MP nº 2.200-2/2001, já anteriormente mencionado:

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

(...)

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

Não se pode deixar de atentar também para o disposto no art. 18 da Lei nº 13.874/2019, a chamada Lei da Liberdade Econômica:

Art. 18. A eficácia do disposto no inciso X do caput do art. 3º desta Lei fica condicionada à regulamentação em ato do Poder Executivo federal, observado que:

I - para documentos particulares, qualquer meio de comprovação da autoria, integridade e, se necessário, confidencialidade de documentos em forma eletrônica é válido, desde que escolhido de comum acordo pelas partes ou aceito pela pessoa a quem for oposto o documento; e

II - independentemente de aceitação, o processo de digitalização que empregar o uso da certificação no padrão da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) terá garantia de integridade, autenticidade e confidencialidade para documentos públicos e privados.

Tal dispositivo normativo evidencia que, em relação aos documentos puramente particulares, a regra é a liberdade de forma, desde que a forma adotada seja aceita por ambas as partes do negócio jurídico e não haja impugnação por parte daquele a quem for oposto o documento. Por outro lado, como se extrai do inciso II, somente mediante uso de certificado emitido por autoridade certificadora credenciada pela ICP-Brasil se obtém assinatura oponível a todos (e, portanto, passível de utilização para todos os fins públicos e privados, inclusive em processos judiciais), com garantia plena de autenticidade.

Vale lembrar igualmente o disposto nos artigos 440 e 441 do CPC:

Art. 440. O juiz apreciará o valor probante do documento eletrônico não convertido, assegurado às partes o acesso ao seu teor.

Art. 441. Serão admitidos documentos eletrônicos produzidos e conservados com a observância da legislação específica.

Mais uma vez se ressalta a necessidade de verificar se, em relação ao específico tipo de fato, ato ou negócio jurídico em questão, há exigência jurídica de forma especial, como requisito de validade ou eficácia.

CONCLUSÃO

Em vista de todos os fundamentos expostos, o Centro de Inteligência da Justiça de Minas Gerais recomenda que:

a) em relação à assinatura dos documentos destinados a demonstrar o preenchimento das condições da ação e dos pressupostos processuais, como o instrumento de mandato judicial, verifique-se se está presente assinatura manual em procuração digitalizada em sua integralidade (sem montagem ou colagem) ou assinatura eletrônica qualificada, lançada mediante uso de certificado digital de padrão ICP-Brasil;

b) relativamente a documentos juntados a autos processuais para fazer prova de fatos ou atos jurídicos materiais, efetue-se a análise, em cada caso, acerca da suficiência da prova em questão, à luz inclusive do art. 10 da MP n. 2.200-2/2001, dos artigos 107 e 219 do Código Civil e do art. 18 da Lei nº 13.874/2019, devendo-se verificar se existe, em relação ao fato ou ato jurídico em questão, exigência de especial requisito formal de validade, e ainda avaliar as controvérsias delineadas pelas alegações das partes e o disposto nos artigos 428, I e 429, II, no CPC, assim como o Tema 1.061 do STJ.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Ronaldo Alves. Justiça digital. *Revista brasileira da advocacia*, vol. 9, abr.-jun. 2018, p. 243-259. Revista dos Tribunais Online, Edições Thomson Reuters.

ARRUDA ALVIM, José Manoel de; CUNHA, Ígor Martins da. As assinaturas eletrônicas no ordenamento jurídico brasileiro e a relevância da autonomia privada: uma breve análise dos documentos eletrônicos à luz da MP 2.200-2/2001 e da Lei 14.063/2020. *Revista de Processo*, vol. 227, mar. 2023. Revista dos Tribunais Online, Edições Thomson Reuters.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. *Curso de Direito Civil*. 13 ed. São Paulo: Editora Juspodivm, 2023. V. 4 – Contratos.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. *Novo curso de Direito Civil*. Contratos. 3 ed. São Paulo: Saraiva Educação, 2020.

LEITE, Clarisse Frechiani Lara. Assinatura eletrônica. *Revista de Processo*, vol. 354, no. 2023, p. 79-121. Revista dos Tribunais Online, Edições Thomson Reuters.

MENKE, Fabiano. A criptografia e a infraestrutura de chaves públicas brasileira (ICP-Brasil). *Revista de Processo*, vol. 1/2018 (Caderno Especial – A regulação da Criptografia no Direito Brasileiro), dez. 2018, p. 83-97. Revista dos Tribunais Online, Edições Thomson Reuters.

TEIXEIRA, Tarcísio. *Direito digital e processo eletrônico*. 8 ed. São Paulo: Saraivajur, 2024. Edição do Kindle.