Organizadores
José Augusto Garcia de Sousa
Rodrigo Baptista Pacheco
Maurilio Casas Maia

ACESSO À **JUSTIÇA** *na era da* **TECNOLOGIA**

Autores(as)

Beatriz Carvalho de Araujo Cunha
Bruno Ricardo Bioni
Cintia Regina Guedes
Daniel Becker
Débora Brandão
Fernanda Tartuce
Frederico Boghossian Torres
Fredie Didier Jr.
Humberto Dalla Bernardina De Pinho
Júlio Camargo de Azevedo
Maria Beatriz Rodrigues
Marina Sayuri Kitayama
Maurilio Casas Maia
Messi Elmer Vasconcelos Castro
Rafael A. F. Zanatta
Rafael Alexandria de Oliveira
Rafael da Silva Menezes
Rodrigo Baptista Pacheco

Prefácio
Cássio Scarpinella Bueno

Posfácio
Alfredo Emanuel Farias de Oliveira

2022

EDITORA *Jus*PODIVM
www.editorajuspodivm.com.br

CAPÍTULO 3

O USO DA TECNOLOGIA BLOCKCHAIN PARA ARQUIVAMENTO DE DOCUMENTOS ELETRÔNICOS E NEGÓCIOS PROBATÓRIOS SEGUNDO A LEI DE LIBERDADE ECONÔMICA[1]

Fredie Didier Jr.[2] *e Rafael Alexandria de Oliveira*[3]

Sumário: 1. Introdução. **2**. A Lei de Liberdade Econômica e a ampliação do uso do documento eletrônico: armazenamento em meio eletrônico de documentos públicos ou privados. **3**. Documento eletrônico: a questão da segurança e da confiabilidade. **4**. A presunção de autenticidade, integridade e confidencialidade do documento eletrônico certificado no padrão da ICP-Brasil. **5**. A previsão de hipótese típica de negócio jurídico sobre prova. **6**. *Blockchain* – **6.1**. O que é *blockchain*; **6.2**. Segurança e imutabilidade; **6.3**. Transparência; **6.4**. *Blockchain* como prova atípica; **6.5**.

---

1. Este artigo é também resultado do grupo de pesquisa "Transformações nas teorias sobre o processo e o Direito processual", vinculado à Universidade Federal da Bahia, cadastrado no Diretório Nacional de Grupos de Pesquisa do CNPq respectivamente nos endereços dgp.cnpq.br/dgp/espelhogrupo/7958378616800053. O grupo é membro fundador da "ProcNet – Rede Internacional de Pesquisa sobre Justiça Civil e Processo contemporâneo" (http://laprocon.ufes.br/rede-de-pesquisa).
2. Mestre em Direito pela UFBA. Doutor em Direito pela PUC/SP. Livre-docente pela USP. Pós-doutorado pela Universidade de Lisboa. Professor associado da Universidade Federal da Bahia, nos cursos de graduação, mestrado e doutorado. Membro da Associação Internacional de Direito Processual, do Instituto Iberoamericano de Direito Processual, do Instituto Brasileiro de Direito Processual e da Associação Norte e Nordeste de Professores de Processo. Advogado e consultor jurídico.
3. Mestre em Direito Público (UFBA). Especialista em Direito Processual Civil (Fac. Jorge Amado/Juspodivm). Professor do Programa de Pós-Graduação *Lato Sensu* da Faculdade Baiana de Direito. Membro da Associação Norte e Nordeste de Professores de Processo (ANNEP). Procurador do Município de Salvador/BA. Advogado.

Blockchain como forma de garantir a autoria, integridade e confidencialidade de documento eletrônico. **7**. Conclusão. **8**. Referências.

1. Introdução

A Lei n. 13.874/2019 (Lei de Liberdade Econômica) ampliou a possibilidade de utilização do documento eletrônico de duas formas: *(i)* ao alterar a redação do art. 2º-A da Lei n. 12.682/2012, passou a autorizar o armazenamento, em meio eletrônico, óptico ou equivalente, de documentos privados e também de documentos públicos; *(ii)* equiparou a digitalização[4] ao próprio documento em suporte de papel, desde que atendidos a técnica e os requisitos estabelecidos em regulamento (art. 3º, X, Lei n. 13.874/2019[5]).

Essas alterações estão em conformidade com o movimento de desburocratização da Administração Pública que vem sendo implementado por sucessivos atos normativos – como, por exemplo, a Lei n. 13.460/2017, a Lei n. 13.726/2018 e a Lei 12.682/2012. Esse movimento abrange também os métodos de documentação, inclusive os métodos de documentação aplicáveis às relações entre particulares.

A consequência disso, no âmbito dos métodos de documentação, é uma crescente utilização dos documentos eletrônicos em substituição a outras formas de armazenamento de dados e de imagens, especialmente em substituição aos documentos em suporte de papel.

4. Conforme art. 1º, par. ún., da Lei n. 12.682/2012, "entende-se por digitalização a conversão da fiel imagem de um documento para código digital".

5. Art. 3º São direitos de toda pessoa, natural ou jurídica, essenciais para o desenvolvimento e o crescimento econômicos do País, observado o disposto no parágrafo único do art. 170 da Constituição Federal: [...] X – arquivar qualquer documento por meio de microfilme ou por meio digital, conforme técnica e requisitos estabelecidos em regulamento, hipótese em que se equiparará a documento físico para todos os efeitos legais e para a comprovação de qualquer ato de direito público.

O propósito deste artigo é tratar da *blockchain* como meio atípico de comprovação da autoria, integridade e confidencialidade de documentos particulares ou públicos, a partir da hipótese típica de negócio jurídico sobre prova previsto no art. 18 da Lei n. 13.874/2019 c/c art. 10, § 2º, da Medida Provisória n. 2.200-2/2001.

2. A Lei de Liberdade Econômica e a ampliação do uso do documento eletrônico: armazenamento em meio eletrônico de documentos públicos ou privados

A Medida Provisória n. 881, de 30 de abril de 2019, que instituiu a Declaração de Direitos de Liberdade Econômica (e foi a antecessora da Lei de Liberdade Econômica), já havia acrescentado o art. 2º-A à Lei n. 12.682/2012. No *caput* desse art. 2º-A, a MP 881 autorizava "o armazenamento, em meio eletrônico, óptico ou equivalente, *de documentos privados*, compostos por dados ou por imagens, observado o disposto nesta Lei, nas das demais legislações específicas e no regulamento" (acrescentamos o itálico).

O art. 10 da Lei de Liberdade Econômica alterou esse art. 2º-A acrescentado pela MP 881 à Lei n. 12.682/2012. Com a mudança, o *caput* passou a autorizar "o armazenamento, em meio eletrônico, óptico ou equivalente, *de documentos públicos ou privados*, compostos por dados ou por imagens, observado o disposto nesta Lei, nas legislações específicas e no regulamento" (acrescentamos o itálico).

A alteração é sensível: acrescentou-se a possibilidade de, para todos os fins, os documentos públicos serem, também eles, armazenados em meio eletrônico, óptico ou equivalente.

A distinção entre documento público e privado parte da análise de quem seja o autor do documento[6]: "será público quando o seu autor *imediato* for agente investido de função pública, e quando a

6. DIDIER JR., Fredie; BRAGA, Paula Sarno; OLIVEIRA, Rafael Alexandria de. *Curso de direito processual civil*: teoria da prova, direito probatório, decisão, precedente, coisa julgada, processo estrutural e tutela provisória. 15ed. Salvador: Ed. Juspodivm, 2020, v. 2, p. 227-228.

formação do documento se der no exercício desta função […]. Será, ao contrário, particular o documento quando sua autoria *imediata* se dê por ação de um particular ou mesmo de um funcionário público (desde que este não se encontre no exercício de suas funções)"[7].

A redação atual do *caput* do art. 2º-A da Lei n. 12.682/2012 harmoniza com o art. 3º, X, da Lei de Liberdade Econômica, que reconhece a toda pessoa, natural ou jurídica, o direito essencial de "arquivar *qualquer documento* por meio de microfilme ou por meio digital, conforme técnica e requisitos estabelecidos em regulamento, hipótese em que se equiparará a documento físico para todos os efeitos legais e para a comprovação de qualquer ato de direito público" (acrescentamos o itálico).

O armazenamento (ou arquivamento) em meio eletrônico de documento público ou privado é técnica que se aplica tanto aos documentos novos, criados já em formato de código digital, quanto aos documentos criados em suporte de papel cuja imagem venha a ser digitalizada e convertida para o formato de código digital (art. 1º, par. ún., Lei n. 12.682/2012).

A digitalização constitui, pois, uma forma de converter o documento em suporte de papel num documento eletrônico, a fim de que ele passe a ser armazenado (ou arquivado) em meio eletrônico.

Conforme visto, nos termos do art. 3º, X, da Lei de Liberdade Econômica, desde que atendidos técnica e requisitos estabelecidos em regulamento, o documento eletrônico produto da digitalização se equipara ao "documento físico para todos os efeitos legais e para a comprovação de qualquer ato de direito público"; isso vale "inclusive para atender ao poder fiscalizatório do Estado" (art. 2º-A, § 2º, Lei n. 12.682/2012).

A eficácia desse art. 3º, X, está condicionada à regulamentação (art. 18, *caput*), mas alguns parâmetros já constam na Lei n. 12.682/2012, na Medida Provisória n. 2.200-2/2001 e também na própria Lei de Liberdade Econômica (art. 18, I e II).

---

7. MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. *Comentários ao Código de Processo Civil*. 2 ed. São Paulo: RT, 2005, v. 5, t. 2, p. 245-246.

O art. 18 da Lei de Liberdade Econômica prevê que: *(i)* se o documento digitalizado for particular, 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; *(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 integralidade, autenticidade e confidencialidade para documentos públicos e privados.

Todos esses parâmetros precisam ser observados pelo regulamento.

Conforme o art. 2º-A, § 1º, da Lei n. 12.682/2012, após a digitalização, constatada a integridade do documento digital nos termos estabelecidos no regulamento, o original poderá ser destruído, ressalvados os documentos de valor histórico, cuja preservação observará o disposto na legislação específica. Quanto aos documentos referentes a operações e transações realizadas no sistema financeiro nacional, a aferição de integridade do documento eletrônico e as hipóteses em que o documento original pode ser destruído devem ser regulamentadas em ato do Conselho Monetário Nacional (art. 2º-A, § 6º, Lei n. 12.682/2012).

O dever de guarda dos documentos armazenados em meio eletrônico, tenham sido eles criados já como código digital ou sejam fruto de digitalização de documento em suporte de papel, termina com o exaurimento dos respectivos prazos de decadência ou de prescrição das situações jurídicas que deles emanam[8], momento em que se faculta sejam eles eliminados (art. 2º-A, § 3º, Lei n. 12.682/2012).

8. Sobre o tema, o STJ já decidiu que "ocorrida a prescrição, não mais sobrevive o dever de guarda de documentos, sendo legítima a recusa fundada no transcurso do prazo prescricional. Pensar diferente seria impor à parte obrigação juridicamente impossível" (STJ, 4ª Turma, REsp 1046497/RJ, rel. Min. João Otávio de Noronha, j. 24/08/2010, DJe 09/11/2010).

3. Documento eletrônico: a questão da segurança e da confiabilidade

A valorização do meio eletrônico para fins de documentação de fatos e declarações de vontade está em conformidade com o avanço tecnológico e com a forma pela qual as relações jurídicas vêm sendo constituídas atualmente. É crescente, por exemplo, o uso de aplicativos em dispositivos móveis para o registro de ideias e de manifestações de vontade (como os aplicativos de mensagem)[9], para a realização de transações financeiras (como os aplicativos de instituições financeiras) – em alguns casos, a senha pessoal é até substituída por recursos de biometria, como o reconhecimento facial – e para a celebração de *smart contracts* (como nos aplicativos de transporte, de aluguel de bicicletas ou patinetes, ou de *delivery* de comidas ou de compras feitas em ambiente *online* etc.).

Há, por isso mesmo, uma preocupação constante quanto ao grau de segurança e de certeza que se pode ter em relação à *autenticidade* dos documentos eletrônicos, que permite identificar a sua autoria, e à sua *integridade*, que permite garantir a inalterabi-

9. Foi amplamente divulgada, em 2015, a notícia do primeiro acordo viabilizado por meio do aplicativo *WhatsApp*. O fato ocorreu num processo que tramitava perante a Justiça do Trabalho da 15ª Região, em Campinas/SP. A juíza e os advogados das partes iniciaram as tratativas por meio do aplicativo de mensagens e compareceram à audiência apenas para reduzi-lo a termo e assinar o documento físico. A despeito da preferência que se tenha dado ao documento de papel, é preciso ver que o diálogo entabulado por meio do *WhatsApp*, eletronicamente documentado, já consistia, por si só, numa exteriorização da vontade dos transatores; a juíza, no caso, optou por homologá-lo em audiência, mas poderia, sem qualquer prejuízo, tê-lo feito ali, no próprio grupo de *WhatsApp*, do qual também ela, juíza, participava, anexando posteriormente o documento eletrônico comprobatório da avença (e da sua homologação) aos autos do processo. A rigor, o documento (eletrônico) surtiria o mesmo efeito que o documento de papel. A notícia reforça a ideia de que essas novas tecnologias estão e estarão cada vez mais acessíveis e a serviço do processo (processo n. 0010025-20.2015.5.15.0094; notícia disponível em <http://www.conjur.com.br/2015-jun-08/justica-trabalho-promove-acordo-entre-partes-via-whatsapp>. Acesso em 27 dez. 2015).

lidade do seu conteúdo. Somente a certeza quanto a esses dados é que pode garantir a eficácia probatória desses documentos.[10]

O problema é que, pelo seu próprio conceito (sequência de *bits* representativa de um fato), já se vê que a maior e melhor característica do documento eletrônico – que é a sua versatilidade, ou flexibilidade, na medida em que, em segundos, ele pode ser formado e utilizado, mediante envio pela Internet, em qualquer lugar do mundo – é também a porta para possíveis adulterações, o que infirma a sua integridade e, pois, a sua eficácia probatória.

Têm sido desenvolvidas técnicas que buscam dar maior segurança e confiabilidade aos documentos eletrônicos. Normalmente essas técnicas vinculam a garantia da autenticidade à integridade do conteúdo do documento, de modo que, alterado o seu conteúdo, desfaz-se a vinculação entre este novo conteúdo (alterado) e o autor do documento originário.

São várias as técnicas, que podem conferir maior ou menor segurança, a depender do tipo.

Tem-se, por exemplo[11]: *(i)* a assinatura digitalizada (que não se confunde com a assinatura digital), que nada mais é que uma imagem da assinatura autógrafa, a qual pode ser lançada no documento para identificar a sua autoria; *(ii)* as firmas biométricas, que permitem reconhecer a autoria de uma declaração a partir das características físicas do seu emitente (o formato do rosto, a íris dos olhos, a impressão digital, o timbre de voz etc.), muito utilizadas por aplicativos instalados em *smartphones* com ferramentas de detecção de impressão digital ou de reconhecimento facial; *(iii)* as senhas pessoais, como o PIN (*Personal Identification Number* ou Número de Identificação Pessoal), a *Password* (palavra de aprovação) e a *Passphrase* (frase de passagem ou aprova-

10. A propósito, o enunciado n. 297 das Jornadas de Direito Civil do Conselho da Justiça Federal: "O documento eletrônico tem valor probante, desde que seja apto a conservar a integridade de seu conteúdo e idôneo a apontar sua autoria, independentemente da tecnologia empregada".

11. Exemplos colhidos em MARQUES, Antônio Terêncio G. L. *A prova documental na internet*. Curitiba: Juruá, 2005, p. 152-155.

ção), comuns nos terminais bancários, nas transações eletrônicas etc.; *(iv)* a esteganografia, que transforma o documento em um código (espécie de criptografia) e lhe agrega um elemento marcante, semelhante a uma marca d'água; dentre outras.

A técnica mais segura de que hoje se tem conhecimento é a *criptografia*. Por essa técnica, a declaração (mensagem) é cifrada e transformada num código ininteligível àquele que não conhece o padrão para a decifração. O padrão utilizado para cifrar ou decifrar as mensagens é denominado de *chave*. Somente quem a conhece é que pode ter acesso ao conteúdo da mensagem[12].

Atualmente, a criptografia usa conceitos matemáticos extremamente complexos (os *algoritmos*) como chave para cifrar as mensagens. Essas chaves, no entanto, não codificam letras ou números, mas os próprios *bits* que compõem a sequência do documento eletrônico[13].

Há duas formas de criptografia: a criptografia *simétrica* e a *assimétrica*.

Como ensina Antônio Lago Jr., "o uso da *criptografia simétrica*, também chamada de criptografia de chave privada, requer que o destinatário da mensagem conheça o algoritmo usado para cifrar o seu conteúdo, caso contrário, ficará impossibilitado de decifrar a mensagem, ou seja, o destinatário da mensagem deve ter acesso à chave utilizada pelo remetente"[14]. Esse método é frágil em termos de segurança, na medida em que a chave utiliza-

12. Júlio César, imperador romano, criou um eficiente sistema de envio de mensagens criptografadas para os seus centuriões no campo de batalha. Por meio dela, mandava substituir as letras do texto original sempre pela terceira letra que lhe sucedesse no alfabeto. Essa era, portanto, a *chave* para cifrar a mensagem. Quem a recebesse, precisaria valer-se desta mesma *chave* para decifrá-la, aplicando-a inversamente: as letras da mensagem recebida deveriam ser substituídas pela terceira letra que lhe antecedesse no alfabeto.

13. Cf. MARQUES, Antônio Terêncio G. L. *A prova documental na internet*, ob. cit., p. 156-159; LAGO Jr., Antônio. *Responsabilidade civil por atos ilícitos na internet*. São Paulo: LTr, 2001, p. 35.

14. LAGO JR., Antônio. *Responsabilidade civil por atos ilícitos na internet*, ob. cit., p. 35-36. Acrescentamos o itálico.

da para decifrar a mensagem é a mesma utilizada para cifrá-la. Assim, sendo ela conhecida pelo receptor, não se pode garantir que ele não venha utilizá-la para cifrar novas mensagens, fazendo-se passar pelo autor da mensagem originária. Isso infirmaria, como se pode ver, talvez não a autenticidade da mensagem recebida, mas de tantas outras que, a partir da chave conhecida, pudessem vir a ser formadas.

Já a *criptografia assimétrica* é uma das técnicas capazes de conferir maior segurança quanto à autenticidade e integridade do conteúdo do documento eletrônico. Como explica Augusto Marcacini:

> A criptografia assimétrica, ao contrário da convencional (que pede a mesma chave tanto para cifrar como para decifrar a mensagem), utiliza *duas* chaves, geradas pelo computador. Uma das chaves dizemos ser a *chave privada*, a ser mantida em sigilo pelo usuário, em seu exclusivo poder, e a outra, a *chave pública*, que, como sugere o nome, pode e deve ser livremente distribuída. Estas duas chaves são dois números que se relacionam de tal modo que uma desfaz o que a outra faz. Encriptando a mensagem com a chave pública, geramos uma mensagem cifrada *que não pode ser decifrada com a própria chave pública que a gerou*. Só com o uso da chave privada poderemos decifrar a mensagem que foi codificada com a chave pública. E o contrário também é verdadeiro: o que for encriptado com o uso da chave privada, só poderá ser decriptado com a chave pública.[15]

A chave privada, utilizada por aquele que formou o documento eletrônico, gera uma assinatura digital, que permite a identificação do seu autor. Essa assinatura digital pode ser conferida a partir do uso da chave pública. Não se trata, contudo, de um sinal visível, como o é a assinatura manuscrita, mas de uma sequência numérica a que o programa de computador chega a par-

15. MARCACINI, Augusto Tavares Rosa. *O documento eletrônico como meio de prova*. Obtido em: <http://www.advogado.com/internet/zip/tavares.htm>. Acesso em: 21 dez 2006.

tir de fórmulas matemáticas. A assinatura digital será diferente para cada documento gerado por uma determinada chave privada, mas sempre estará vinculado a ela, o que garante a prova da autenticidade do documento.

Além de essa chave privada poder atestar a autenticidade do documento, ela ficará vinculada ao seu conteúdo, de modo que qualquer alteração superveniente tornará, automaticamente, ineficaz a assinatura digital outrora lançada. Com isso, embora seja possível a alteração do conteúdo do documento guardado pela criptografia assimétrica, essa alteração não mais vinculará o seu autor originário[16]. Em outras palavras: a integridade do documento é garantida em relação ao seu autor; não sendo possível identificá-lo, tem-se aí um indício de que o documento foi alterado.

Como se viu, somente a chave pública distribuída por uma determinada pessoa pode ser utilizada para decifrar a mensagem codificada pelo titular da respectiva chave privada. Mas aí surge um novo problema: "qualquer um poderia gerar um par de chaves e atribuir-lhe o nome de qualquer pessoa, existente ou imaginária. A autenticidade do documento eletrônico é conferida sem dificuldade por qualquer usuário de computador, com o uso do programa de criptografia e de posse da chave pública do seu subscritor. Mas, e se a própria chave pública não for autêntica? Esta conferência o programa não tem como realizar. O que fazer, então, para contornar o problema?"[17]. Nesse caso, a assinatura digital apontaria, como autor do documento, uma determinada pessoa, distinta da que efetivamente formara o documento.

16. Cf. MARCACINI, Augusto Tavares Rosa. *O documento eletrônico como meio de prova*. Obtido em: <http://www.advogado.com/internet/zip/tavares.htm>. Acesso em: 21 dez 2006. O autor explica: "Se uma mínima modificação for feita ao abrir-se o arquivo, e for ele gravado em disco, o documento eletrônico ficará inutilizado, pois perderá o vínculo com a assinatura".

17. MARCACINI, Augusto Tavares Rosa. *O documento eletrônico como meio de prova*. Obtido em: <http://www.advogado.com/internet/zip/tavares.htm>. Acesso em: 22 dez 2006.

"Para evitar, então, essa fraude, instituiu-se a *certificação digital*, onde a identidade do proprietário das chaves é previamente verificada por uma terceira entidade de confiança dos interlocutores, que terá a incumbência de certificar a ligação entre a chave pública e a pessoa que a emitiu, como também a sua validade"[18]. Essa terceira entidade a que alude Antônio Terêncio, responsável pela certificação digital da identidade do proprietário das chaves e pela divulgação ao público das chaves públicas válidas, é a chamada *autoridade certificadora*[19].

4. A presunção de autenticidade, integridade e confidencialidade do documento eletrônico certificado no padrão da ICP-Brasil

No intuito, dentre outras coisas, de garantir a autenticidade, a integridade e a validade jurídica dos documentos eletrônicos, a Medida Provisória n. 2.200-2/2001 instituiu a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil (art. 1º), composta por uma autoridade vinculada ao Comitê Gestor por ela criado e pela cadeia de autoridades certificadoras (art. 2º).

A regulamentação legal veio para viabilizar meios de tornar ainda mais segura a utilização dos documentos eletrônicos protegidos por criptografia assimétrica. A sua eficácia probatória, quando produzido com a utilização de processo de certificação disponibilizado pela ICP-Brasil, é a mesma dos documentos públicos e particulares, presumindo-se verdadeiros em relação aos signatários (art. 10, *caput* e § 1º, MP n. 2.200-2/2001).

Quando se trata de digitalização de documentos em papel, o art. 3º da Lei n. 12.682/2012 prescreve que o processo de digitalização deve ser realizado de forma a manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento

18. MARQUES, Antônio Terêncio G. L. *A prova documental na internet*, ob. cit., p. 174.

19. É uma espécie de "cibernotário", como sugere Marcacini (MARCACINI, Augusto Tavares Rosa. *O documento eletrônico como meio de prova*. Obtido em: <http://www.advogado.com/internet/zip/tavares.htm>. Acesso em: 21 dez 2006).

digital, com o emprego de certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Nesses mesmos termos, a Lei de Liberdade Econômica (Lei n. 13.874/2019) estabelece a presunção de que o processo de digitalização do documento de papel, público ou particular, que empregar o uso da certificação no padrão da ICP-Brasil terá garantia de integralidade, autenticidade e confidencialidade (art. 18, II).

5. A previsão de hipótese típica de negócio jurídico sobre prova

A certificação no padrão da ICP-Brasil pode ser substituída por outro método de certificação escolhido em comum acordo pelas partes ou aceito pela pessoa a quem for oposto o documento. Em linha de princípio, isso é expresso apenas em relação aos documentos particulares, conforme se vê no art. 18, I, da Lei de Liberdade Econômica: "*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" (acrescentamos o itálico).

O art. 2º-A, § 8º, da Lei n. 12.682/2012, acrescentado pela Lei n. 13.874/2019, prescreve que "para a garantia de preservação da integridade, da autenticidade e da confidencialidade de *documentos públicos* será usada certificação digital no padrão da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)".

Uma leitura apressada desse art. 2º-A, § 8º, da Lei n. 12.682/2012 e do art. 18, I, da Lei n. 13.874/2019 poderia dar a entender que a certificação dos documentos públicos somente é possível se utilizado o padrão da ICP-Brasil.

Sucede que o art. 10, § 2º, da MP n. 2.200-2/2001, responsável por instituir a ICP-Brasil, prescreve que, para todos os fins legais, os documentos eletrônicos tratados na Medida Provisória se consideram públicos ou particulares (art. 10, *caput*), a de-

pender da sua autoria. Já o § 2º estabelece que "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".

Fica muito claro, portanto, que o sistema normativo não estabelece a certificação digital no padrão da ICP-Brasil como *método exclusivo* para garantir a preservação da integridade, da autenticidade e da confidencialidade dos documentos eletrônicos. Apenas há, como já visto no item anterior, uma *presunção* de que o uso da certificação no padrão da ICP-Brasil implica esse tipo de garantia para documentos públicos e privados (art. 18, II, Lei n. 13.874/2019), bem como que, *a princípio*, quanto aos documentos públicos, essa garantia decorre da certificação digital no padrão da ICP-Brasil (art. 2º-A, § 8º, da Lei n. 12.682/2012).

É possível, porém, que outros meios de comprovação de autoria, de integridade e de confidencialidade de documentos eletrônicos sejam utilizados para essa finalidade, desde que isso seja "admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento". O § 2º do art. 10 da MP n. 2.200-2/2001 não diferencia entre documentos públicos e particulares; o *caput* do art. 10 prescreve, inclusive, e como visto, que os documentos eletrônicos tanto podem ser públicos como particulares.

Conjugando-se, pois, o art. 18, I, da Lei n. 13.874/2019 com o art. 10, § 2º, da MP n. 2.200-2/2001, temos que o sistema normativo contém hipótese típica de negócio jurídico sobre prova, consistente no acordo quanto ao método de certificação da autoria, integridade e confidencialidade do documento eletrônico, seja ele público ou particular.

Nesse cenário, nada impede que se convencione, por exemplo, o uso da *blockchain* como método de certificação da autoria, integridade e confidencialidade do documento eletrônico.

6. *Blockchain*

6.1. O que é blockchain?

Blockchain é palavra em língua inglesa que significa *cadeia de blocos*.

Esse é o nome usado, ao mesmo tempo, para *(i)* designar uma *base de dados distribuída* e também para *(ii)* designar a *tecnologia que mantém as múltiplas cópias dessa base de dados operando em sincronia umas com as outras*, de modo que estejam sempre atualizadas[20]. Vejamos.

Blockchain é uma base de dados distribuída.

Quando pretendemos obter informação sobre determinado imóvel, nós buscamos essa informação no Registro de Imóveis da cidade – o Registro de Imóveis centraliza as informações sobre imóveis existentes em determinada região. Quando pretendemos obter informação sobre antecedentes criminais de determinado sujeito, nós buscamos essa informação no Setor de Distribuição das Justiças Estadual e Federal – o Setor de Distribuição centraliza as informações sobre processos pendentes. Quando pretendemos obter informação sobre o nosso saldo na conta bancária, nós acessamos o sistema eletrônico do banco – o nosso banco centraliza as informações sobre a nossa conta bancária. Por fim, quando pretendemos obter informação sobre um determinado assunto que seja do nosso interesse, é comum procurarmos essa informação no *site* do *Google* – o *Google* é uma ferramenta que centraliza muitas informações sobre assuntos variados cujo acesso está disponível na *internet*.

Todos esses são exemplos de bases de dados concentradas, não distribuídas, que dependem sempre de um servidor ou de um intermediário para que possam ser acessadas. Se houver um incêndio na sede do Registro de Imóveis, perdem-se os registros

20. ALEIXO, Gabriel. Aula 1: Blockchain e Direito. *Blockchain e seus aspectos jurídicos*. Curso online do ITS Rio, 1h06m35s, acesso em 23 de dezembro de 2018.