ADVOCACIA-GERAL DA UNIÃO
PROCURADORIA-GERAL FEDERAL
PROCURADORIA FEDERAL ESPECIALIZADA JUNTO AO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO
PROCURADORIA PFE ITI

PARECER n. 00378/2019/PROFE/PFE-ITI/PGF/AGU

NUP: 00100.006150/2019-17
INTERESSADOS: GABINETE DA PRESIDÊNCIA - ITI
ASSUNTOS: Consulta. Utilização de certificação digital distinta da ICP-Brasil pela Administração Pública Federal. Impossibilidade.

CONSULTA JURÍDICA. CERTIFICAÇÃO DIGITAL. UTILIZAÇÃO DE CERTIFICAÇÃO DIGITAL DISTINTA DA ICP-BRASIL NA ADMINISTRAÇÃO PÚBLICA FEDERAL. IMPOSSIBILIDADE.

1. Consulta oriunda da Receita Federal do Brasil, acerca da viabilidade de utilização, pelo ambiente Gov.br, de certificados digitais emitidos fora da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

2. A Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, instituída pela Medida Provisória n. 2.200-2/2001, possui âmbito de aplicação nacional, requisito este que é necessário para garantir sua interoperabilidade no plano interno.

3. Nos termos do art. 10, §1º, da MP nº 2.200-2/2001, a única espécie de assinatura eletrônica equiparada à assinatura manuscrita no direito positivo brasileiro é a assinatura digital produzida com o uso do processo de certificação digital da ICP-Brasil. Via de consequência, sempre que a lei exija a assinatura como condição de validade ou de eficácia de um ato ou negócio jurídico, tal condição somente restará atendida, no meio eletrônico, mediante a utilização da assinatura com uso de certificação digital da ICP-Brasil.

4. Tendo em vista o princípio da legalidade estrita, que rege a atividade administrativa, a possibilidade da utilização de meios eletrônicos pela Administração Pública está condicionada à prévia previsão legal que a admita, a qual foi albergada pelo art. 10, *caput e* §1°, da MP n° 2.200-2/2001.

5. Com base no art. 10, *caput e* §1°, da MP n° 2.200-2/2001, e tendo em vista os princípios da legalidade, eficiência e razoabilidade, é admissível a utilização de meios eletrônicos por parte da Administração Pública, inclusive para a prática de atos administrativos aptos a produzir efeitos no âmbito administrativo, nos moldes do art. 22, §1º da Lei n. 9.784/99, desde que mediante a utilização de certificação digital proveniente da ICP-Brasil.

6. O §2º do art. 10 da MP n. 2.200/2001 - que admite a utilização de outros meios de comprovação da autoria e integridade de documentos produzidos em forma eletrônica, inclusive a utilização de certificados digitais não emitidos pela ICP-Brasil, desde que assim aceito pelas partes ou pela pessoa a quem for oposto o documento - aplica-se exclusivamente às manifestações de vontade realizadas no âmbito privado, sendo inaplicáveis aos atos do Poder Público, uma vez que estes possuem fé pública, independem de aceitação da parte contrária e tem sua validade condicionada à observância de requisitos formais específicos.

7. Nos termos do Decreto n. 3.996/2001, que permanece válido e em vigor, os serviços de certificação digital no âmbito da Administração Pública Federal devem ser providos, exclusiva e obrigatoriamente, no âmbito da ICP-Brasil, sendo vedada, portanto, a criação de infraestruturas de certificação paralelas por parte de seus órgãos e entidades ou a utilização de outras formas de certificação digital para fins de assinatura de atos e documentos públicos.

8. O art. 6º do Decreto n. 8.539/2015 deve ser interpretado em consonância com o regramento legal e principiológico aplicável à Administração Pública, sendo inaplicável aos serviços de certificação digital como um todo, os quais seguem submetidos ao regime estabelecido pelo Decreto n. 3.996/2001.

9. Assim sendo, sempre que exigida ou necessária a utilização de certificação digital por parte da Administração Pública, esta deverá, obrigatoriamente, ser provida no âmbito da ICP-Brasil, não sendo admitido qualquer outro

método de certificação digital. Da mesma forma, a formalização de atos administrativos (em sentido amplo), nos quais se exija a assinatura da autoridade competente ou do agente público, na forma do art. 22, §1°, da Lei n° 9.784/99, como forma de exteriorização da vontade administrativa (tais como, contratos e acordos administrativos, atos decisórios de qualquer natureza, atos normativos, pareceres técnicos e jurídicos, atos que venham a conferir ou restringir direitos, e, de maneira geral, os atos descritos no art. 50, da Lei n° 9.784/99), deverão, obrigatoriamente, ser firmados mediante o uso de certificação digital provida no âmbito da ICP-Brasil.

10. Por outro lado, admite-se a utilização de outras formas de "assinatura eletrônica" , inclusive do *login e senha,* no máximo, para fins de autenticação em sistemas (como, por exemplo, para acesso ao Sistema Eletrônico de Informações - SEI), ressalvado que apenas serão considerados "assinados", para fins jurídicos, os documentos eletrônicos nos quais tenha sido aposta a assinatura digital com uso de certificado digital da ICP-Brasil, por ter sido essa a única forma de assinatura eletrônica equiparada à assinatura manuscrita no direito brasileiro (art. 10, §1°, da MP n° 2.200-2/2001).

I. RELATÓRIO

1. Trata-se de consulta encaminhada pela Secretaria Especial da Receita Federal do Brasil - RFB a este Instituto Nacional de Tecnologia da Informação (Ofício n° 1.282/2019-COTEC/SUCOR/RFB), acerca da viabilidade de utilização, pelo ambiente Gov.br, de certificados digitais emitidos fora da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

2. Segundo a consulente, o Gov.br, em sua página na Internet, não se utiliza de certificados ICP-Brasil, mas sim de um certificado fora dessa infraestrutura, fato que teria suscitado discussões no âmbito do Acordo de Cooperação Técnica (ACT), celebrado em 18/01/2017 entre a União, representada pela Casa Civil da Presidência da República e pelo Ministério da Economia, e o Serviço Brasileiro de Apoio à Micro e Pequenas Empresas (Sebrae).

3. Dessa forma, visando pacificar os entendimentos sobre o tema, solicita manifestação desta autarquia acerca dos seguintes questionamentos:

a) O Decreto n° 3.996, de 2001, informa em seu art. 2°, §1°, que os serviços de certificação digital na Administração Pública Federal devem ser providos pela ICP-Brasil. Com base nesse dispositivo, é correto o entendimento de que os serviços digitais de governo na internet devem utilizar, exclusivamente, certificados ICP-Brasil?

b) O Decreto n° 8.539, de 2015, informa em seu art. 6°, §1°, que não se obsta a utilização de outro meio de comprovação de autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem identificação por meio de usuário e senha. Com base nesse dispositivo, é correto o entendimento de que os serviços digitais de governo na internet podem utilizar certificados fora da infraestrutura da ICP-Brasil?

c) A MP n° 2.200-2, de 2001, regula em seu art. 10, §2°, que não se obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive o que se utilize de certificados não emitidos pela ICP-Brasil, desde que admitidos pelas partes como válido ou aceito pela pessoa a quem for oposto o documento, com base nesse dispositivo, é correto afirmar que o disposto no art. 6°, §1°, do Decreto n° 8.539, de 2015, depende de prévia manifestação de concordância entre as partes para utilização de certificados fora da ICP-Brasil?

d) Se o Gov.br enviar as credenciais do usuário autenticado, para os serviços digitais de governo que o utilize, mediante assinatura com a ICP-Brasil, a garantia de autenticidade e não repúdio (art. 10, §1°, da MP n° 2.200-2, de 2001) restringe-se à comunicação entre o Gov.br e o serviço digital, ou abrange, inclusive a autenticação do usuário realizada pelo Gov.br, independentemente do certificado utilizado, para comunicação com o cidadão?

e) Se a resposta ao item "d" for de que abrange a autenticação do usuário, é correto o entendimento de que, com base no disposto no art.6°, §1°, do Decreto n° 8.539, de 2015, há comprovação de autoria e integridade para logins realizados por meio de usuário e senha no âmbito do Gov.br?

4. A Diretoria de Infraestrutura de Chaves Públicas - DINFRA se pronunciou acerca dos aspectos técnicos pertinentes às questões levantadas por meio do Parecer Técnico SEI n° 0392647.

5. Em seguida, vieram os autos a esta Procuradoria Federal Especializada, para manifestação quanto aos aspectos jurídicos e legais, consoante o disposto na Portaria PGF n° 526/2013.

6. É o relato do essencial.

II. ANÁLISE JURÍDICA

7. Como se sabe, a competência desta Procuradoria, enquanto órgão de assessoramento jurídico, limita-se, estritamente, às questões jurídicas, não podendo se imiscuir nos aspectos técnicos, financeiros, orçamentários ou econômicos relacionados à consulta realizada.

8. Nessa linha, a orientação jurídica contida no Manual de Boas Práticas Consultivas–BPC n° 07, aprovado pela Portaria Conjunta CGU/CGAU/PGBC/PGFN/PGF/PGU n° 01/2016:

> BOA PRÁTICA CONSULTIVA – BPC No 07.
>
> Enunciado
>
> A manifestação consultiva que adentrar questão jurídica com potencial de significativo reflexo em aspecto técnico deve conter justificativa da necessidade de fazê-lo, evitando-se posicionamentos conclusivos sobre temas não jurídicos, tais como os técnicos, administrativos ou de conveniência ou oportunidade, podendo-se, porém, sobre estes emitir opinião ou formular recomendações, desde que enfatizando o caráter discricionário de seu acatamento.
>
> É oportuno que os Órgãos Consultivos prestigiem os conhecimentos técnicos alheios ao Direito, adotando cautela, por exemplo, ao dissentir da classificação feita por agente público competente acerca do objeto licitatório.
>
> A prevalência do aspecto técnico ou a presença de juízo discricionário determinam a competência e a responsabilidade da autoridade administrativa pela prática do ato.
>
> A responsabilidade na tomada de decisão é sempre da autoridade administrativa. E, pelo conteúdo de seu Parecer o subscritor responde exclusivamente perante as instâncias da Advocacia-Geral da União.

9. *In casu*, contudo, não há como se evitar o exame, em certo grau, de questões técnicas relacionadas à matéria objeto da consulta.

10. Com efeito, conforme ficará evidente no decorrer desta manifestação, a matéria objeto da consulta guarda forte carga técnica e jurídica, de forma que a análise a seguir realizada exige que se adentre em alguns aspectos técnicos, necessários para a correta interpretação jurídica da questão posta, sem a qual o exame restaria prejudicado.

11. Assim é que, conquanto a presente manifestação tenha, por óbvio, o intuito de se examinar a questão jurídica adjacente, não há como se esquivar de algumas considerações de cunho técnico, as quais, contudo, serão baseadas predominantemente nas informações acarreadas aos autos pelas áreas competentes, mais precisamente no Parecer Técnico SEI n° 0392647, elaborado pela Diretoria de Infraestrutura de Chaves Públicas - DINFRA.

12. Feita a ressalva, passa-se ao exame da consulta propriamente dita.

13. Para tanto, tendo em vista a complexidade técnica e jurídica afeta à assinatura e certificação digital, e considerando que os questionamentos levantados encontram-se relacionados entre si, o presente exame jurídico será realizado de forma compartimentada, evitando-se com isso repetições desnecessárias, bem como possibilitando a necessária objetividade quando da elaboração das respostas às questões propostas.

14. Dessa feita, iniciar-se-á a análise pela definição de alguns conceitos basilares, necessários à correta compreensão do tema, mais precisamente assinatura eletrônica, assinatura digital, certificados e certificação digital, qual a sua finalidade e como se dá seu funcionamento, ocasião que serão feitas algumas considerações complementares acerca do modelo de certificação digital adotado pela ICP-Brasil. A seguir, passaremos ao exame da validade jurídica da assinatura eletrônica no Brasil, examinando o regramento legal e regulamentar aplicável à espécie. Em seguida, será examinada a aplicabilidade de tal regramento no âmbito do Direito Administrativo, à luz das regras e princípios que regem a atuação do Estado, bem como a regulamentação administrativa existente sobre o tema. Por fim, os questionamentos formulados serão respondidos objetivamente, fazendo-se referência, naquilo em que necessário, às considerações previamente realizadas.

1) NOÇÕES CONCEITUAIS ACERCA DAS ASSINATURAS ELETRÔNICAS, ASSINATURAS DIGITAIS E O MODELO DE CERTIFICAÇÃO DIGITAL ADOTADO PELA ICP-BRASIL

15. A UNICITRAL (*United Nations Camissions on International Trade Law)*, órgão integrante da Organização das Nações Unidas - ONU, responsável pela uniformização das leis referentes ao comércio internacional, publicou, em 2001, uma lei modelo sobre as assinaturas eletrônicas, definindo-a, logo em seu preâmbulo, como:

> "Electronic signature" means data in eletronic form in, affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message; (...)

16. Tal conceito modelo tem sido, com pequenas variações, repetido nas definições trazidas pelas legislações ao redor do mundo, como se observa dos seguintes exemplos:

> UNIÃO EUROPÉIA (*REGULATION No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*" – eIDAS) *(versão PT)*
>
> Artigo 3º - Definições
>
> Para efeitos do presente regulamento, entende-se por:
>
> (...)
>
> 10) Assinatura eletrónica: os dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar;
>
> CANADÁ (*PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT* – PIPEDA)
>
> *"electronic signature means a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document. (signature électronique)"*
>
> CHILE (LEY 19.799/2014)
>
> *Artículo 2º.- Para los efectos de esta ley se entenderá por:*
>
> *(...)*
>
> *f) Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor;*
>
> ESTADOS UNIDOS (*ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT* – eSING e *UNIFORM ELECTRONIC TRANSACTIONS ACT* - UETA)
>
> *SECTION 2. DEFINITIONS. In this [Act]:*
>
> *(...)*
>
> *(8) "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopt ed by a person with the intent to sign the record.*

17. A área técnica do ITI, no Parecer Técnico SEI n° 0392647, definiu assinatura eletrônica nos seguintes termos:

> Assinatura Eletrônica: uma *string* de *bits* anexada a um ativo digital gerada por um sistema, usada por um usuário signatário cadastrado no momento da assinatura eletrônica.

18. Como se nota das definições acima colacionadas, assinatura eletrônica é um conceito amplíssimo, designando, portanto, qualquer conjunto de dados sob a forma eletrônica, ligados ou logicamente associados a outros dados eletrônicos, que visa identificar determinada pessoa (autenticação) ***[1]***. O conceito técnico de assinatura eletrônica, portanto, compreende toda e qualquer tecnologia eletrônica utilizada para a identificação de um signatário, a exemplo de um simples *login* e senha (acerca do qual teceremos

algumas considerações mais específicas adiante, haja vista ser esse o modelo adotado no e-Gov), criptografia, identificação biométrica, etc. ***[2]***

19. Por outro lado, assinatura digital é um termo que não comporta significado unívoco.

20. Na doutrina, tem-se considerado a assinatura digital como uma espécie de assinatura eletrônica ***[3]***, dotada de determinados requisitos específicos, que permitem verificar, com relativa segurança, a autenticidade e integridade dos documentos eletrônicos nos quais tenham sido apostas.

21. Sobre as diferenças entre **assinatura eletrônica** e **assinatura digital**, cabe transcrever os ensinamentos de André Pinto Garcia ***[4]***:

> Podem ser ressaltadas três principais diferenças entre o gênero e a sua espécie: a) a assinatura eletrônica se contenta com qualquer forma de integridade documental (ou mesmo nenhuma), conquanto na digital exige se a utilização de criptografia assimétrica (operação matemática que utiliza um par de chaves criptográficas e permite que se saibam a origem e a integridade do documento); b) apenas a assinatura digital se exige a identificação presencial do usuário como forma de autenticidade; c) consequência das duas características anteriores, a validade da assinatura digital deriva diretamente da lei.

22. Nos termos do Parecer Técnico SEI n° 0392647, a assinatura digital foi assim definida:

> Assinatura Digital: uma *string* de *bits* calculada por um elemento criptográfico, baseado em procedimentos e algoritmos estudados na matemática e na ciência da computação, que associa, com integridade, os dados de um documento eletrônico a uma manifestação de vontade de uma pessoa ou entidade originária.

23. Em que pese as diversas definições encontradas na doutrina e na literatura técnica especializada, pode-se afirmar que a assinatura digital, invariavelmente, será realizada mediante a aplicação de um elemento criptográfico seguro sobre o próprio documento eletrônico (mais precisamente, sobre a função *hash* desse mesmo documento ***[5]***) que, atrelado a uma determinada pessoa, permite identificar a origem e a integridade desse mesmo documento ***[6]***.

24. Sem adentrar muito profundamente nos aspectos matemáticos - devidamente enfrentados no Parecer Técnico SEI n° 0392647, a assinatura digital vale-se de um sistema criptográfico específico, usualmente a **criptografia assimétrica**, desenvolvido na década de 1970 por matemáticos estadunidenses e britânicos para permitir a troca de mensagens criptografadas entre duas pessoas sem que fosse necessária a troca prévia de uma chave criptográfica comum entre ambas, como ocorre na **criptografia simétrica.**

25. Enquanto na criptografia simétrica ambos os interlocutores usam **a mesma senha (ou chave)** para cifrar as mensagens trocadas entre eles, o que gera a necessidade de compartilhamento prévio dessa senha e, portanto, a possibilidade de sua interceptação, na criptografia assimétrica, para cada participante é gerado um **par de chaves**, sendo uma delas chamada de **chave pública**, que pode ser compartilhada e conhecida por todos, e a outra de **chave privada (ou secreta)**, de controle e conhecimento exclusivos de seu portador ***[7]***.

26. Esse par de chaves utiliza cálculos matemáticos que permitem que uma determinada mensagem cifrada utilizando a **chave pública** somente possa ser decifrada por meio da utilização da **chave privada**. Utilizando-se da **chave pública** de determinado destinatário, qualquer remetente poderá cifrar uma mensagem e encaminhá-la com a certeza de que somente aquele destinatário será capaz de decifrá-la, uma vez que é ele o detentor exclusivo da **chave privada** correspondente. Mesmo que um terceiro intercepte a comunicação e tenha posse da chave pública utilizada para cifrar a mensagem, não conseguirá decifrá-la, eis que somente o detentor da chave privada será capaz de fazê-lo.

27. O mais interessante é que a **criptografia assimétrica**, também **chamada de criptografia de chaves públicas**, é uma via de mão dupla, isto é: as mensagens **cifradas com a chave pública** são **decifradas apenas e exclusivamente com a chave privada correspondente** e as mensagens **cifradas com a chave privada** são decifradas apenas e exclusivamente com a **chave pública correspondente**.

28. Mas qual seria a razão para cifrar uma mensagem com a **chave privada**, já que a **chave pública** correspondente, como seu próprio nome diz, é do conhecimento de todos? Como a criação de um par de chaves criptográficas **vincula a chave pública à chave privada** de forma singular e exclusiva, a cifragem de uma informação com determinada **chave privada** permite a todos os que

tenham acesso à **chave pública** correspondente identificar a autoria da informação, uma vez que tal informação só poderia ter sido cifrada pelo exclusivo detentor da chave privada em questão.

29. É exatamente assim que funciona o processo de assinatura digital. Um documento assinado com determinada **chave privada** pode ter sua assinatura reconhecida por qualquer um que possua a **chave pública** correspondente. E como tal chave é pública, não há nenhum problema em que ela seja amplamente distribuída, sendo até mesmo desejável que isso ocorra. Utilizando recursos criptográficos adicionais (especialmente a chamada "função resumo" ou *"hash function*"), é possível garantir ainda a **integridade** do documento assinado, de tal maneira que qualquer alteração posterior neste documento, por mínima que seja, gere um erro no processo de reconhecimento da assinatura, indicando que a assinatura, o documento, ou ambos, foram corrompidos.

30. Note-se, contudo, que a utilização da criptografia assimétrica como método de assinatura de documentos eletrônicos não garante, por si só, a autoria dessa assinatura. Como bem explica MARCACINI:

> Mas, corretamente conferida a assinatura digital, o que isso precisamente significa? Em termos estritamente científicos, as únicas verdades matemáticas daí decorrentes são: a) quem quer que tenha produzido aquela assinatura utilizou a chave privada correspondente; b) o documento não foi alterado após a a criação dessa assinatura digital.
>
> São essas verdades matemáticas que permitem substituir, no meio eletrônico, as funcionalidades dos documentos em papel. No entanto, isso não resolve todas as possíveis dúvidas que podem pairar em torno desses fatos. A matemática, aí empregada, não permite afirmar *quem* é o signatário da mensagem, ou *quem* é o titular desse par de chaves. Ora, esse par de chaves consiste em dois números, relacionados entre si, mas que foram aleatoriamente gerados por computador, em um determinado momento do passado; tais números não guardam qualquer vínculo com o corpo do seu indicado titular do par de chaves criptográficas. Afirmar que um número gerado aleatoriamente pertence a um dado sujeito é algo que escapa às ciências exatas envolvidas nessas operações, e só pode ser fruto de convenções sociais. ***[8]***

31. E é justamente aqui que entra a atividade de certificação digital, e os certificados digitais, como modo de garantir a **autenticidade** dos documentos eletrônicos.

32. Segundo a definição trazida pelo Parecer Técnico SEI n° 0392647, certificado digital é *"o documento eletrônico assinado digitalmente pela Autoridade Certificadora que o emitiu, contendo a identidade da pessoa, máquina, software ou entidade e a correspondente chave pública calculada"*. Do ponto de vista estritamente jurídico, os certificados digitais nada mais são que documentos eletrônicos, assinados (também digitalmente) por um emissor confiável - a Autoridade Certificadora -, que atesta a vinculação da chave pública ao seu respectivo titular, que tenha sido previamente identificado.

33. Por sua vez, a certificação digital consiste, justamente, na atividade, realizada por uma Autoridade Certificadora, em estabelecer, e posteriormente declarar por meio do certificado digital, uma relação única, exclusiva e intransferível, entre um par de chaves criptográficas e uma pessoa física ou jurídica.

34. Registre-se que o certificado digital é também assinado digitalmente por essa Autoridade Certificadora emissora, a qual, por sua vez, foi também certificado por uma autoridade confiável, e assim por diante, até chegar na Autoridade Certificadora Raiz (que, no caso da ICP-Brasil, como se verá adiante, é o ITI), que se vale de um certificado autoassinado. Tem-se com isso formada uma cadeia de confiança, do tipo hierárquica ***[9]***, denominada "Infraestrutura de Chaves Públicas" (muitas vezes referida simplesmente como PKI, do inglês *Public Key Infrastructure*).

35. Perceba-se que a autenticidade que se atribui a um documento assinado digitalmente somente se faz possível porque essa vinculação entre a chave pública e o seu respectivo titular é feita por parte de um terceiro de confiança - a Autoridade Certificadora -, após prévio e rígido credenciamento, mediante um *procedimento de identificação* do respectivo titular do certificado.

36. Daí porque se dizer que **somente a assinatura digital, por meio do uso da criptografia assimétrica, aliado a um certificado digital emitido por uma Autoridade Certificadora no âmbito de uma Infraestrutura de Chaves Públicas, permite, atualmente, atestar de forma segura a integridade e a autenticidade de um documento eletrônico assinado. Todas as demais modalidades de assinatura eletrônica, conquanto não sejam - como se verá a seguir - juridicamente inválidas, não são capazes, por si só, de assegurar a integridade e a autenticidade de um documento - ainda que, eventualmente, sejam aptas e suficientes para outras finalidades.**

1.1) A Infraestrutura de Chaves Públicas Brasileira

37. Antes de se adentrar os aspectos estritamente jurídicos das assinaturas eletrônicas, importante tecer algumas considerações acerca da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, o que se fará de maneira bastante sucinta, dado não ser este o cerne da questão posta pela RFB.

38. A ICP-Brasil foi instituída pela Medida Provisória nº 2.200-2/01, a fim de *"[...] 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. 1°).

39. Ressalte-se, desde logo, que tal Medida Provisória encontra-se em **vigor**, de acordo com a EC 32/01, art. 2º, *verbis:*

> Art. 2º As medidas provisórias editadas em data anterior à da publicação desta emenda continuam em vigor até que medida provisória ulterior as revogue explicitamente ou até deliberação definitiva do Congresso Nacional.

40. É uma infraestrutura integrada por uma Autoridade Gestora de Políticas (o Comitê Gestor da ICP-Brasil), uma Autoridade Certificadora Raiz (ITI), as Autoridades Certificadoras de nível subsequente ao da Raiz e as Autoridades de Registro, conforme dispõe o art. 2º da MP nº 2.200-2/01 . Além destes, pode-se apontar, ainda, as entidades de apoio (Prestadores de Serviço de Suporte - PSS, Prestadores de Serviços Biométricos - PSBio e Prestadores de Serviços de Confiança - PSC), previstas nas normas regulamentares expedidas pelo Comitê Gestor e, logicamente, os usuários de todo esse sistema; vale dizer, aqueles que se utilizam dos certificados emitidos no âmbito da ICP-Brasil.

41. A competência de cada um dos integrantes da infraestrutura encontra-se delineada na MP n° 2.200-2/01, e especificada nas normas expedidas pelo Comitê Gestor.

42. **Em poucas palavras, pode-se assim resumir o papel desempenhado por cada qual na ICP-Brasil: a) o Comitê Gestor estabelece as normas; b) o ITI, executa-as; c) as Autoridades Certificadoras, conforme o próprio nome diz, emitem os certificados; d) as Autoridades de Registro, que são vinculadas às Autoridades Certificadoras, identificam presencialmente os adquirentes desses certificados. Os PSS, por sua vez prestam serviços de apoio às demais entidades.**

43. Nesse quadro, o Instituto Nacional de Tecnologia da Informação – ITI é a Autoridade Certificadora Raiz da Infraestrutura de Chaves Públicas Brasileira. ***[12]*** É, portanto, a primeira autoridade da cadeia de certificação, responsável pelo **credenciamento, auditoria e fiscalização** das Autoridades Certificadoras de nível subsequente, das Autoridades de Registro e Prestadores de Serviço de Suporte, nos termos do art. 5º da MP nº 2.200-2/01:

> Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, 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 Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

44. Em posição destacada no sistema brasileiro figuram as Autoridades Certificadoras, responsáveis, conforme dito, pela emissão de certificados digitais. A MP 2.200-2/01 é expressa:

> 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.

45. Essas Autoridades Certificadoras, por sua vez, servem-se de Autoridades de Registro – AR para **identificar e cadastrar presencialmente os usuários** e encaminhar às ACs as solicitações de certificado (art. 7° da MP n° 2.200-2/01) ***[13]***. Às Autoridades de Registro, então, não cabe a emissão de certificados digitais, mas tão somente o papel intransferível de verificar a identidade dos usuários para os quais esses certificados serão emitidos.

46. Toda essa infraestrutura, denominada de ICP-Brasil, existe com o fim de assegurar a **integridade** do documento emitido em forma eletrônica (obtida ao se utilizar a criptografia de par de chaves, também chamada de criptografia assimétrica, com visto anteriormente), bem como a sua **autenticidade** (decorrente da atividade de certificação digital levada a cabo por uma Autoridade Certificadora previamente cadastrada, que, por meio de um certificado digital, atesta a vinculação entre uma chave pública e o titular dessa mesma chave pública).

47. Como se nota, o Brasil adotou o modelo de uma **Infraestrutura de Chaves Públicas de âmbito nacional**, com a criação de uma Autoridade Certificadora Raiz única (i.e., o ITI), a quem compete credenciar as entidades responsáveis por emitir certificados aos usuários finais e fiscalizar a sua atuação, assegurando a observância das normas e procedimentos de segurança física e lógica necessários à garantia de **autenticidade** e **integridade** dos documentos assinados com base em certificados digitais integrantes dessa infraestrutura, dentre os quais está a **identificação presencial** do titular da assinatura como requisito do processo de certificação.

48. Os aspectos normativos da Medida Provisória n. 2.200-2/01 serão analisados de forma minuciosa no tópico seguinte, mas, por ora, importa destacar que o art. 10, §1° da referida norma **equiparou as assinaturas digitais produzidas através do processo de certificação disponibilizado pela ICP-Brasil às assinaturas manuscritas,** atribuindo-lhes os mesmos efeitos jurídicos destas, notadamente a **presunção de veracidade em relação aos seus signatários** (i.e., os titulares dos certificados digitais), estabelecendo um verdadeiro **diferencial jurídico** para esta modalidade de assinatura em relação às demais tecnologias de assinatura eletrônica disponíveis.

49. Doravante, para os fins da presente análise, será chamada de **assinatura digital** aquela realizada de acordo com os padrões da ICP-Brasil, e de **assinatura eletrônica** aquela realizada com base em outras tecnologias que não sejam baseados na criptografia assimétrica, aliada ao uso de um certificado digital.

2) A VALIDADE JURÍDICA DA ASSINATURA ELETRÔNICA NO BRASIL

50. Superada as questões conceituais necessárias ao adequado enfrentamento do tema, passamos ao exame dos aspectos propriamente jurídicos - i.e., como a assinatura eletrônica foi internalizada e tratada pelo direito brasileiro.

51. Para tanto, iniciaremos a presente análise pelo regime jurídico-legal relacionado à juridicidade da assinatura eletrônica e digital, e seus efeitos jurídicos, a partir do exame das regras gerais apostas no Código Civil e, em seguida, os aspectos normativos da Medida Provisória relativo ao tema, notadamente o art. 10 e seus respectivos parágrafos. Posteriormente, em capítulo específico, passaremos a examinar, com mais especificidade, a questão relativa ao uso da assinatura eletrônica no âmbito da Administração Pública Federal, ocasião em que será também examinada a regulamentação trazida pelos Decretos n°s 3.996/2001 e 8.539/2015.

52. De plano, vale notar que a expressão "validade jurídica" - da qual se vale o art. 1° da MP n° 2.200-2/2001 - não se mostra a mais adequada. Juridicamente, validade nada mais é que a entrada do fato no mundo jurídico sem defeitos que possam gerar a sua desconstituição ***[13].*** Assim, o que é válido ou inválido não é o documento assinado eletrônica ou digitalmente, e sim o ato ou negócio jurídico nele refletido. A esse respeito, MARCACINI bem aponta a contradição contida no art. 1°, da MP n° 2.200-2/2001:

> Outro equívoco desse texto reside na expressão 'validade jurídica de documentos', que, ao que parece, vem sendo perpetuado por comentadores menos atentos ao seu adequado funcionamento jurídico. Validade não é um atributo de *documentos*, mas do *ato jurídico,* e por certo muitos outros são os requisitos de um ato para que lhe seja atribuída tal qualidade. Um documento é apenas *verdadeiro* ou *falso,* conforme sejam os fatos nele retratados, ou a sua própria existência. (...). ***[14]***

53. Nesse contexto, a assinatura, seja ela manuscrita ou eletrônica, insere-se como uma *forma* específica de exteriorização da vontade, como um requisito, ora de validade, ora de eficácia, do ato ou negócio jurídico ***[15].*** No Brasil, tirante as hipóteses em que a própria lei exige determinada forma específica para efeitos de prova ou da própria validade do ato (casos em que seu não atendimento importará na nulidade do ato respectivo), vigora o que convencionou chamar de **princípio da liberdade das formas,** previsto no art. 107 do Código Civil, nos seguintes termos, *in verbis:*

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

54. Assim, como regra geral, temos que a manifestação de vontade é de forma livre. Pode se dar tanto da forma

manuscrita, por meio da assinatura física, como também de outras formas, a exemplo da oral, ou mesmo mediante um simples "clique" em uma página eletrônica na *internet* (como de fato ocorre na grande maioria dos casos de compras efetuadas online), e até mesmo de forma implícita. E, se assim é, nada impede que tal manifestação de vontade se dê por meio de uma assinatura eletrônica, independentemente da tecnologia empregada, sem que com isso se diga que tal manifestação de vontade seja inválida. Sob a ótica jurídica, isso nada mais significa que a incidência da autonomia privada no mundo digital.

55. Assim, independentemente de qualquer norma específica que trate do assunto, podemos afirmar, sem medo de errar, que **a manifestação de vontade por meio de uma assinatura eletrônica (ainda que fora do padrão ICP-Brasil) não é inválida, sempre que não tenha a lei exigido alguma especial forma para a exteriorização da vontade.**

56. Nesse ponto, uma ressalva se faz necessária: **dizer que a assinatura eletrônica não é inválida, como regra geral, haja vista o princípio da liberdade das formas, não significa, em absoluto, que estejamos afirmando que a assinatura eletrônica seja equivalente à assinatura manuscrita, ou que possa produzir os mesmos efeitos e utilizadas para os mesmos fins jurídicos que aquela *[16].***

57. É da tradição jurídico-cultural brasileira atribuir à assinatura (manuscrita) determinadas presunções e efeitos específicos, não extensíveis a outras formas de manifestação de vontade, das quais, sem dúvida, a *presunção de veracidade* mostra-se como a mais proeminente. Tal presunção encontra previsão, atualmente, no art. 219 do Código Civil (que repete, *ipsis litteris,* o art. 131 do Código Civil anterior), como segue:

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

58. Na mesma linha, o art. 221, 1ª parte, do mesmo diploma, ao dispor que *"o instrumento particular, feito e assinado, ou somente assinado por quem esteja na livre disposição e administração de seus bens, prova as obrigações convencionais de qualquer valor (...)*. Regra análoga é encontrada também na lei processual, mais precisamente no art. 408, *caput,* do Código de Processo Civil, segundo o qual *"as declarações constantes do documento particular escrito e assinado ou somente assinado presumem-se verdadeiras em relação ao signatário"*.

59. Não se pode olvidar, ainda, as diversas disposições legais existentes, que preveem a exigência de documento escrito e assinado, como requisito de forma para a formalização de determinados atos ou negócios jurídicos.

60. Essas presunções e exigências não são aleatórias. Decorrem de uma percepção cultural - albergada pelo direito - de que os documentos escritos e assinados (e aqui estamos tratando da assinatura manuscrita) são **mais seguros** que as demais formas igualmente admitidas.

61. E isso, a partir de uma simples constatação: a assinatura, além de uma *forma* de manifestação de vontade, é também um *meio de prova* dessa mesma manifestação. Assim, um documento escrito e assinado, além de formalizar um determinado ato ou negócio jurídico (mesmo nos casos em que essa exigência não venha a decorrer de lei - hipótese em que a forma específica passará a ser da essência do ato -, mas também quando as partes assim convencionarem fazer), é um meio de prova do ato ou negócio jurídico ali refletido.

62. CARNELUTTI identifica na assinatura física ou manual três propriedades: *"a) indicativa, de quem é o autor do documento; b) declaratória quanto à manifestação da vontade expressa; c) probatória da existência da indicação e declaração apostas no documento". **[17]***

63. Essas três funções atribuídas à assinatura manuscrita decorrem diretamente de alguns pressupostos (que chamaremos aqui de **"pressupostos fáticos"**), extraídos das próprias características inerentes às assinaturas manuscritas: (a) um sinal único, que identifica uma determinada pessoa (i.e., um símbolo específico por ela criado, cuja análise permite identificar ser essa a mesma pessoa que apôs a assinatura); (b) tanto esse símbolo, como também a informação lançada, encontram-se ligados a um determinado documento por meio de um processo químico (a tinta lançada penetra nas fibras do papel de modo indelével); e (c) como o documento físico é, a princípio, inalterável (dependendo, para tanto, de uma atuação externa sobre ele para que a informação, uma vez lançada - e portanto, a ele aderente de forma indelével - possa ser modificada), torna-se possível concluir que a pessoa que ali lançou a sua assinatura está de acordo com os fatos ali constantes.

64. Por fim, uma característica bastante relevante do documento físico - e que é de fundamental importância ao se

examinar os problemas e soluções que surgem ao adentrarmos o mundo digital -, é a sua autonomia (portabilidade). Ora, como todos os elementos que compõem o documento assinado (ou seja, as informações e a assinatura nele aposta) encontram-se indelevelmente atrelados ao suporte físico (em geral, o papel), esse documento sempre manterá tais características ainda que venha a ser transferido, ou armazenado onde quer que seja, sem que haja a separação entre a informação nele contida e o seu suporte.

65. Todas as características acima descritas é que permitem que, no âmbito jurídico, se atribua aos documentos assinados de forma manuscrita, as presunções anteriormente mencionadas, bem como fundamentam as exigências legais quanto à forma a ser adotada em determinados atos ou negócios jurídicos.

66. Tais pressupostos - que parecem óbvios quando tratamos dos documentos físicos e da assinatura manuscrita - ganha especial relevância quando transpomos para o mundo digital. Um documento eletrônico nada mais é que *"uma sequência de* bits *que, traduzida por meio de um determinado programa de computador, seja representativa de um fato"*. ***[18]*** Ou, conforme definiu a área técnica no Parecer Técnico SEI n° 0392647, o *"meio eletrônico em que um dado é registrado ou armazenado por um sistema computacional ou dispositivo similar que pode ser lido e percebido por uma pessoa, sistema computacional ou dispositivo similar"*.

67. Uma das principais características atribuídas ao documento eletrônico é a sua **alterabilidade**. Diferentemente do que ocorre com o documento físico, no qual, a informação nele aposta vincula-se de forma perene por processos físicos, de tal forma que a eventual alteração do seu conteúdo demanda uma atuação externa sobre esse documento (passível de identificação por meio de perícia, exame grafotécnico, etc), os documentos eletrônicos são facilmente modificáveis e copiáveis, sem que se possa, a princípio, identificar a alteração nele realizada. Tratando-se de uma sequência de números, uma imagem ou uma informação que venha a ser aposta em um documento eletrônico não estará a ele atrelada de forma indissociável.

68. Da mesma forma, não possuindo um suporte físico, não há como se assinar um documento da maneira tradicionalmente realizada. Mesmo a aposição de uma imagem da assinatura manuscrita será somente isso: uma simples imagem, que pode até estar agregada ao documento, mas não de forma indissociável, como ocorre com a assinatura manuscrita, sobre o papel. A digitalização dos documentos - e , consequentemente a sua abstração - permitiu, como nunca visto anteriormente, a separação entre a mensagem/informação e o meio.

69. Tais características do documento eletrônico, no mundo jurídico, traz sérias dúvidas quanto à confiabilidade desse documento como prova, tanto dos fatos nele refletidos, quanto da própria manifestação de vontade. Não havendo como assegurar nem que o conteúdo das informações ali constantes não foi alterado (integridade), tampouco a demonstração da vontade manifestada (autenticidade), como admitir tal documento como prova de um fato ou negócio jurídico? Esse dilema levou parte da doutrina jurídica a afirmar se constituir na "grande crise de identidade da prova documental", oriunda da difusão do uso dos documentos eletrônicos ***[19]***.

70. Assim é que, para que se possa pretender atribuir a uma assinatura eletrônica os mesmos efeitos das assinaturas manuscritas, **mostra-se imprescindível que qualquer que seja a tecnologia empregada na assinatura eletrônica, essa seja capaz de exercer, no mínimo, as mesmas funções da assinatura manuscrita, acima listadas, o que somente se mostra possível se essa assinatura eletrônica seja dotada daqueles pressupostos fáticos anteriormente citados**, sob pena de se gerar uma enorme insegurança jurídica nas transações e atos assim realizados, bem como de tornar absolutamente inócua e ineficaz qualquer presunção legal nesse sentido (**e, nesse ponto, reside a principal - embora não a única - crítica ao disposto no art. 6°, §1º, do Decreto 8.539/2005, que pretende atribuir, por ato normativo infralegal (?), autenticidade e integridade mediante o uso de *login* e senha, o que se constitui numa aberração técnica a sem mais poder, e que invariavelmente tornará tal previsão absolutamente inócua, além de representar séria insegurança jurídica, acaso aplicada em sua literalidade, como adiante será detidamente examinado**).

71. E, como visto no capítulo anterior, atualmente a **única** forma de garantir tais atributos a um documento eletrônico é através da assinatura digital, com o uso de criptografia assimétrica, aliada à um procedimento de certificação digital, que permita vincular o par de chaves criadas a uma pessoa física ou jurídica. Todas as demais tecnologias associadas às assinaturas eletrônicas conhecidas não têm o condão de garantir, da mesma forma que a assinatura digital, lastreada na criptografia assimétrica, os pressupostos fáticos acima mencionados.

72. Tal modelo tecnológico e procedimental, além de assegurar todas as funções atribuídas à assinatura escrita, atendendo aos pressupostos fáticos acima descritos, ainda mantém a portabilidade do documento eletrônico, dado a interoperabilidade que lhe é inerente, passando o documento eletrônico, assim assinado, a gozar de todas as características do documento físico em papel assinado de forma manuscrita.

73. Evidentemente, nada impede, que, futuramente, outras tecnologias que permitam "assinar" os documentos eletrônicos com características análogas aquelas anteriormente expostas venham a ser desenvolvidas, até talvez com maior segurança do que a assinatura digital com criptografia assimétrica permite, hipótese em que, igualmente, os pressupostos acima expostos - os quais entendemos imprescindíveis para a admissibilidade de equiparação jurídica às assinaturas manuscritas - restarão também atendidos.

74. Ocorre que **apenas a viabilidade técnica não basta para que a assinatura eletrônica possa ser equiparada à assinatura manuscrita para fins jurídicos.**

75. As presunções e efeitos atribuídos à assinatura manuscrita, embora encontrem fundamento lógico e científico, não deixam de ser **presunções e efeitos legais.** Daí que, para que se possa estender à uma determinada espécie de assinatura eletrônica efeitos idênticos ou similares às assinaturas manuscritas, além do atendimento dos pressupostos fáticos acima descritos, necessário ainda o atendimento de um **pressuposto jurídico**, qual seja, **expressa previsão legal nesse sentido**.

76. Perceba-se que qualquer assinatura eletrônica, inclusive a assinatura digital, possui elementos distintivos basilares que impedem a imediata equiparação entre ambas e, consequentemente, a extensão automática às assinaturas eletrônicas das presunções e efeitos jurídicos garantidos pelo ordenamento jurídico à assinatura manuscrita. Como explica ANDRÉ PINTO GARCIA:

> A assinatura digital não passa de uma série de números, não visíveis a olho nu, nos quais o sistema efetuará a autenticação necessária para verificar se os requisitos técnicos foram cumpridos. É, pois, uma forma totalmente diversa daquela que o ser humano, desde sempre, se encontrou habituado, de representar, graficamente as suas autenticações ***[20]***

77. Assim, **não basta** que a tecnologia possa, eventualmente, cumprir as mesmas funções da assinatura (pressuposto lógico). **Para que uma determinada espécie de assinatura eletrônica produza, juridicamente, os mesmos efeitos das assinaturas manuscritas, ou possam substituí-las no meio eletrônico, é imprescindível que a lei venha a albergar tal possibilidade (pressuposto jurídico).** Sem que a lei trate do tema, o máximo que se pode enquadrar a assinatura eletrônica será como uma forma atípica de manifestação da vontade, provavelmente válida naqueles atos ou negócios jurídicos em que prevaleça a liberdade privada, como visto anteriormente, mas não será, em absoluto, equiparada às assinaturas manuscritas para efeitos legais.

78. MARCACINI, ao discorrer acerca da previsão da criptografia assimétrica em âmbito legislativo, que constava do Projeto de Lei n° 1589/99, traz interessante colocação sobre o tema:

> Nem se pense, por outro lado, que a descoberta de uma "nova tecnologia", num futuro próximo, vá exigir imediata alteração da lei. É que esta "nova tecnologia" só poderia ser considerada segura, do ponto de vista técnico, depois de exaustivamente testada e aprovada, não apenas por quem a vende, mas pela comunidade científica independente. Se o Projeto 1589/99 consagrou o uso de criptografia assimétrica, o fez porque os sistemas que a implementam são públicos, e têm resistido às tentativas de criptoanálise realizadas pela comunidade científica ao longo de duas décadas. Dessa resistência a tais "ataques" é que advém a confiança do legislador na sua segurança, para poder comparar a assinatura digital à assinatura manual. Destaque-se que testar a funcionalidade de sistemas de segurança não é o mesmo que testar outros tipos de produto ou de *software*. Aqui, uma comparação com os automóveis pode ser ilustrativa: o conforto, a potência, ou o prazer de dirigir um automóvel podem bem ser testados pelo próprio consumidor; o cinto de segurança, porém, aparentemente funciona, mas só poderá ter sua eficácia comprovada pelo usuário comum no dia em que se chocar de frente com outro veículo. Ou o alarme anti-furto: o vendedor demonstra que se tocar aqui, forçar ali, ou balançar acolá, o alarme disparará estridentemente como que anunciando uma invasão de seres extraterrenos; aos nossos olhos parece seguro, até o dia em que não encontramos o veículo no local em que estava estacionado...
>
> Se queremos uma lei para atender à necessidade de segurança da sociedade, dos consumidores e empresários, esta lei só deve admitir como prova judicial aquilo que seja reconhecidamente seguro. Estamos lidando com uma questão bastante delicada, ao atribuir força probatória a registros eletrônicos. Imaginem que uma lei "tecnologicamente neutra" seja aprovada, alguém apresente com publicidade eficiente um novo sistema de assinaturas digitais, milhares de contratos sejam assim efetuados, e meses depois algum adolescente peralta demonstre como fraudar o sistema... Exemplos assim existem, em concreto, de rotundos fiascos tecnológicos! E pode ser ainda pior: alguém pode descobrir como fraudar o sistema e não contar aos quatro ventos, preferindo explorar a falha em seu próprio proveito, para fins evidentemente escusos. **Portanto, se e quando uma nova tecnologia de assinaturas digitais for descoberta, deve ser perante o Legislativo, legítimo representante da sociedade, que a discussão sobre sua oportunidade e segurança deve ser debatida.** Afinal, não se trata da venda de videogames; está em jogo a segurança jurídica dos contratos! ***(grifamos) [21]***

79. No Brasil, a assinatura eletrônica e o documento eletrônico encontra especial previsão no art. 10 da MP 2.200-2/2001, o qual dispõe, *in verbis:*

> 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.

80. Analisando o disposto no referido artigo, nota-se desde logo que o *"caput"* desse dispositivo expressamente equiparou os documentos eletrônicos aos documentos públicos e particulares em geral.

81. Tal previsão legal - pouco explorada doutrinariamente - deixa claro que os documentos eletrônicos nada mais são que documentos. Podem ser públicos ou privados, conforme a origem e o regime jurídico incidente, mas encontram-se enquadrados na mesma categoria jurídica dos documentos físicos. Via de consequência, encontram-se, tais quais os documentos físicos, igualmente sujeitos ao regime civil e processual das provas documentais.

82. A nosso entender, andou bem o legislador ao dispor expressamente sobre o tema.

83. Com efeito, o **suporte** em que se encontra o documento (i.e., um meio físico ou eletrônico) é irrelevante sob a ótica da caracterização ou não do documento eletrônico como documento para fins jurídicos, ainda que o documento eletrônico, como mencionamos alhures, possua algumas características próprias (a exemplo da reprodutibilidade e alterabilidade), que demandam cuidado no que tange ao seu valor probatório**.** ***[22]*** O fato do documento eletrônico possuir tais características não parece razão suficiente para que seja considerado uma categoria específica, distinta dos documentos em geral, inclusive no âmbito processual, em que pese a existência de corrente doutrinária em sentido diverso. ***[23]***

84. Tal entendimento, inclusive, foi acolhido no Enunciado n° 298, aprovado na IV Jornada de Direito Civil do Conselho da Justiça Federal, segundo o qual *"os arquivos eletrônicos incluem-se no conceito de 'reproduções eletrônicas de fatos ou de coisas' do art. 225 do Código Civil, aos quais deve ser aplicado o regime jurídico da prova documental"*.

85. Vê-se, assim, que o documento eletrônico nada mais é que uma nova categoria de documentos, a ele se aplicando o regramento jurídico da prova documental, previsto no direito civil e processual.

86. O §1°, por sua vez, estende aos documentos eletrônicos produzidos com o processo de certificação da ICP-Brasil a presunção de veracidade outorgada pela Código Civil aos documentos assinados de forma manuscrita. O art. 131 do anterior Código Civil, citado no dispositivo, foi reproduzido *ipsis litteris* no art. 219 do atual diploma, nos seguintes termos:

> 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.

87. Segundo MENKE e BERTOL, esse dispositivo consagra o que se denomina **equivalência funcional** entre o documento eletrônico assinado digitalmente com certificação da ICP-Brasil, com o documento físico assinado de forma manuscrita:

> "Este dispositivo legal realiza o que se chama de equivalência funcional, reconhecendo a equiparação jurídica entre a assinatura manuscrita e a assinatura digital aposta com os meios técnico organizacionais disponibilizados pela ICP-Brasil". ***[24]***

88. A esse respeito, CLAUDIO FELIPE ALEXANDRE MAGIOLI NÚÑEZ, assim discorre sobre o tema:

> É aqui que surge o conceito de equivalência funcional. Apesar de as assinaturas digital e autógrafa serem distintas de fato, a lei as equipara como se fossem iguais. Assim, pela equivalência funcional, atribuem-se dois efeitos à assinatura digital: a) cumprir os mesmos requisitos formais da assinatura manuscrita; b) torná-la admissível como meio de prova com os mesmos efeitos processuais da assinatura autógrafa (MENKE, 2005,p. 142). No Brasil, também se adotou a equivalência funcional (art. 10, § 1º, da Medida Provisória nº 2.200-2/2001), de maneira que as assinaturas digitais e autógrafas, ainda que distintas de fato, sejam equivalentes para todos os efeitos jurídicos. ***[25]***

89. Como explica MENKE:

> Feito este exame, não se torna muito difícil concluir qual o significado e efeitos jurídicos pretendidos pelo §1º do art. 10 da Medida Provisória 2.200-2. Ao dizer que "as declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizados pela ICP-Brasil presumem-se verdadeiras em relação ao signatário [...]", este texto legal está tratando da autoria de documentos eletrônicos e **determinando que a assinatura digital aposta a partir de chave privada relacionada a chave pública inserida em certificado digital obtido no âmbito da ICP-Brasil será equiparada à assinatura manuscrita, lançada de próprio punho**.
>
> (...)
>
> Em decorrência, no direito brasileiro, via de regra, **só terá os mesmos efeitos da assinatura manuscrita aquela assinatura digital aposta com base em certificado digital emitido por uma das autoridades certificadoras credenciadas pelo Instituto Nacional de Tecnologia da Informação, entidades que têm obrigação de cumprir com todos os requisitos técnicos, administrativos, operacionais e jurídicos elencados nas normas da ICP-Brasil**". ***[26]***

90. Verifica-se, com isso, que **a única espécie de assinatura eletrônica equiparada à assinatura manuscrita no direito positivo brasileiro é a assinatura digital produzida com o uso do processo de certificação digital da ICP-Brasil. Todas as demais formas de assinatura eletrônica, inclusive as assinaturas digitais produzidas fora da ICP-Brasil, não são equiparadas às assinaturas manuscritas.** Essas, eventualmente, podem até ser válidas como uma forma de manifestação de vontade - e provavelmente serão, naqueles atos e negócios em que vigore a autonomia privada, por força do princípio da liberdade das formas, previsto no art. 107 do Código Civil, já tratado anteriormente, e no §2° do art. 10, a seguir examinado -, porém não são equiparadas às assinaturas manuscritas.

91. Dessa equiparação, dada pelo art. 10, §1° à assinatura digital com certificação da ICP-Brasil, decorrem duas importantes consequências jurídicas.

92. Primeiramente, vê-se que a assinatura digital com certificação ICP-Brasil terá os mesmos efeitos jurídicos atribuídos às assinaturas manuscritas, dentre os quais a **presunção de veracidade** com relação ao signatário, previstas no art. 219, do Código Civil, e art. 408, do Código de Processo Civil.

93. Essa presunção atribuída à assinatura manuscrita, e estendida à assinatura digital com certificação ICP-Brasil, é uma presunção relativa *(juris tantum),* admitindo, portanto, prova em sentido contrário. Nada obstante, tal presunção, ainda que relativa, tem o condão de inverter o ônus probatório, por força do art. 374, inc. IV, do CPC, segundo o qual não dependem de prova os fatos *"em cujo favor milita presunção legal de existência ou de veracidade".*

94. Segundo ANDRÉ PINTO GARCIA:

> A presunção oriunda do certificado digital não é absoluta (em termos jurídicos, não se trata de uma presunção *iure et de iure*), mas, justamente por ser relativa (ou seja, *iuris tantum*), possui o condão de inverter o ônus da prova. Se, nas assinaturas eletrônicas a simples negativa imputa ao outro a necessidade de provar os fatos contestados, na digital a negativa da autoria ou da autenticidade do documento apenas possuirá eficácia jurídica se aquele que a nega também provar o porquê da invalidade.
>
> Porém, caso haja a decretação judicial da invalidade da assinatura, ou mesmo da própria emissão do certificado (quando, por exemplo, um estelionatário se faz passar por terceira pessoa), a sua eficácia será retroativa (Código Civil, art. 182), apagando-se do mundo jurídico todos os efeitos do(s) ato(s) impugnado(s). Repise-se: isso apenas é cabível em um processo judicial, justamente porque milita, em relação à assinatura digital, a presunção

> legal de autenticidade e integridade. ***[27]***

95. A segunda consequência jurídica relevante do §1° do art. 10 da MP n° 2.200-2/2001, é a de que, **sempre que a lei exija a assinatura como condição de validade ou de eficácia de um ato ou negócio jurídico, tal condição somente restará atendida, no meio eletrônico, mediante a utilização da assinatura com uso de certificação digital da ICP-Brasil.**

96. Cuida-se de uma decorrência lógica da equiparação funcional trazida pelo referido dispositivo entre a assinatura manuscrita e a assinatura digital com certificação ICP-Brasil.

97. Conforme mencionamos anteriormente, embora, em regra, a manifestação de vontade seja de forma livre, podendo se dar sem maiores formalidades, inclusive mediante o uso das chamadas "assinaturas eletrônicas", existem casos em que a própria lei expressamente condiciona a eficácia ou mesmo a validade de determinados atos jurídicos à determinada forma específica, hipóteses em que a não observância de tal regra importará na invalidade ou na ineficácia do ato assim praticado.

98. Ora, **se no Brasil a única forma de assinatura eletrônica que é equiparada à assinatura manuscrita é a assinatura digital com uso de certificação da ICP-Brasil, a conclusão que se impõe é que, sempre que a lei exigir aquela (assinatura), o ato somente poderá ser efetuado em meio eletrônico mediante o uso da certificação ICP-Brasil. Todas as demais formas de assinatura eletrônica ou digital não serão aptas a atender tal requisito legal, pelo simples fato de não serem essas equiparadas às assinaturas manuscritas.**

99. De outra banda, não impondo a lei a assinatura do documento como um requisito de validade ou eficácia do ato ou negócio jurídico, nada impede a utilização de outra forma de manifestação de vontade, inclusive a assinatura eletrônica, por força da liberdade de formas, consagrada no art. 107 do CC, conforme já analisado acima.

100. A possibilidade de utilização de outros meios de certificação digital, além da ICP-Brasil, encontra fundamento no §2° do mesmo art. 10 da MP n° 2.2000-2/2001, o qual dispõe 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"*.

101. Veja que o referido dispositivo admite expressamente a utilização de outros meios de comprovação da autoria e integridade de documentos produzidos em forma eletrônica, inclusive a utilização de certificados digitais não emitidos pela ICP-Brasil, mas **condiciona a sua validade à aceitação pelas partes ou pela pessoa a quem for oposto o documento.**

102. De início, nota-se que tal disposição se contrapõe aquelas constantes do art. 10, *caput* e §1º, da mesma norma, anteriormente transcritos. Aos documentos eletrônicos assinados com certificação digital pela ICP-Brasil reconhece-se a plena equivalência aos documentos públicos ou particulares, conforme o caso, com a presunção de validade jurídica das declarações nele contidas. Como vimos no capítulo precedente, tal presunção é decorrente da utilização de recursos de criptografia e da aplicação e fiscalização do cumprimento de normas e procedimentos por meio dos quais é possível garantir com elevadíssimo grau de segurança a **autenticidade** e a **integridade** dos documentos eletrônicos assinados com certificação digital pela ICP-Brasil.

103. Situação bastante diversa é aquela do §2º, que nada mais faz do que asseverar que os atos ou contratos eletrônicos com efeitos *inter partes*, desde que aceitos mutuamente pelas partes envolvidas ou pelo destinatário do ato, não possam ser desconsiderados de plano pelo simples fato de não terem sido produzidos em conformidade com as normas da ICP-Brasil.

104. Sob esse enfoque, tal dispositivo consagra, no mundo digital, a autonomia privada e a liberdade das formas, admitindo **desde que acordado pelas partes ou aceito pela pessoa contra quem oposto,** a adoção de outros meios de certificação digital.

105. O que o art. 10, §2º, da MP n. 2.200-2/2001 visa afirmar, portanto, é que a existência da **presunção legal de validade** dos atos eletrônicos assinados com certificação digital da ICP-Brasil **não gera automaticamente a presunção inversa, isto é, a presunção de invalidade dos atos eletrônicos entabulados por outras formas**, assegurando validade também a estes sempre que as partes em comum acordo (no caso dos direitos subjetivos) ou o destinatário do ato (no caso dos direitos potestativos) admitirem tal forma como válida. Quanto ao tema, aduz ANDRÉ PINTO GARCIA:

> A norma é clara: desde que admitido pelas partes, qualquer meio de comprovação de autoria e integridade (leia-se: assinatura eletrônica) é válido. Assim, se é certo que a utilização do certificado ICP Brasil confere validade jurídica à manifestação eletrônica, não menos correto é se chegar à conclusão de que a validade não se encontra

> adstrita à utilização dos certificados digitais. São tais como dois círculos concêntricos, nos quais a validade é o de maior amplitude pois a simples concordância das partes pode alcançá-la. ***[28]***

106. Em interessante colocação, MENKE entende que o referido dispositivo, ao permitir outros meios de certificação, além da ICP-Brasil, estaria também assegurando o **princípio da neutralidade tecnológica:**

> Além da liberdade conferida às partes, o §2° do art. 10 da MP 2.200-2 também pode ser encarado a partir de outra perspectiva: a de abertura de espaço ao princípio da neutralidade tecnológica. A expressão "utilização de outro meio de comprovação de autoria e integridade, inclusive os que utilizem certificados não emitidos pela ICP-Brasil" denota a intenção de não restringir os métodos de comprovação de autoria que podem ser admitidos como meio de prova. Todavia, a desvantagem da utilização de meios como senhas, assinaturas digitalizadas e dados biométricos é que não terão *status jurídico* diferenciados, em que pese possam perfeitamente ser admitidos como meios de prova. ***[29]***

107. Percebe-se que uma das principais finalidades da referida norma, portanto, é garantir que os "*outros meios de comprovação de autoria e integridade*" não sejam sumariamente desconsiderados no âmbito probatório pelo simples fato de não terem utilizado a certificação digital da ICP-Brasil. Assim, muito embora tais meios alternativos não possuam a presunção legal de validade jurídica conferida pela MP n. 2.200-2/2001, poderão também ser utilizados como elementos de prova em relação à existência de determinado ato ou negócio jurídico.

108. Por certo que tal conclusão decorreria naturalmente da aplicação da autonomia da vontade e da liberdade das formas, há muito adotado no direito civil, que imperam nas relações entre agentes privados. Não obstante, houve por bem o legislador tornar expresso tal raciocínio, evitando possíveis interpretações restritivas de direitos que acabariam limitando bastante as possibilidades de utilização de provas produzidas exclusivamente em meio eletrônico fora dos padrões da ICP-Brasil.

109. Nada obstante, não se deve olvidar que a imensa maioria das formas de assinatura eletrônica conhecidas não se preocupam, nem com a integridade, nem tampouco com a autenticidade do documento eletrônico, como bem observa ANDRÉ PINTO GARCIA:

> A assinatura eletrônica admite a ausência de qualquer forma automatizada de identificação do titular ou mesmo da integridade do documento, bastando, para tanto, que haja a expressa aquiescência de todos aqueles que sofrerão os efeitos do referido documento e a lei não exija a forma especial para o ato. ***[30]***

110. Cumpre notar que, conquanto *integridade* e *autenticidade* sejam requisitos de qualquer documento para que tenha valor probatório, tal questão ganha especial relevância no caso dos documentos eletrônicos, dado as características que lhe são inerentes.

111. Nesse sentido, o Enunciado n° 297, aprovado na IV Jornada de Direito Civil do Conselho da Justiça Federal, expressamente consignou que ***"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".***

112. Vê-se, portanto, no caso dos atos e negócios jurídicos para os quais a lei não exija especial forma, que a dificuldade da manifestação de vontade no meio eletrônico, através das assinaturas eletrônicas, não é tanto uma questão de **validade jurídica**, mas sim de **eficácia probatória** dos documentos eletrônicos assim assinados.

113. Assim, **no caso de eventual litígio, se as partes concordam quanto a integridade e autenticidade do documento, nenhuma dúvida haverá quanto ao ponto, e a discussão se limitará a outros aspectos extrínsecos (por exemplo, se houve ou não a entrega do produto, ou o pagamento, no caso de um contrato de compra e venda). Por outro lado, acaso o litígio ocorra sobre a existência ou não do ajuste ou do ato jurídico praticado em meio eletrônico, a parte requerente deverá provar a existência desse ajuste, por força do disposto no art. 373, I, do CPC (que imputa o autor a prova do fato constitutivo do seu direito). E, dependendo da tecnologia que tenha sido empregada, pode se mostrar extremamente difícil, senão impossível.**

114. Nesse contexto, percebe-se claramente a importância da utilização de meios seguros de manifestação de vontade em documentos digitais nos quais a assinatura eletrônica (em sentido amplo) mostra-se como a mais frágil, e a assinatura digital com o uso de criptografia assimétrica e, principalmente, com o uso da certificação digital da ICP-Brasil (com as presunções oriundas do §1° do art. 10 da MP n° 2.200-2/2001), como a mais segura.

115. De qualquer forma, o que fica evidente desde logo (essa questão será retomada a seguir, ao se examinar a assinatura eletrônica na Administração Pública), é que a viabilidade jurídica de uso da assinatura eletrônica, com outros métodos de certificação digital que não a ICP-Brasil, encontra fundamento jurídico na liberdade das formas, razão pela qual **mostra-se admissível apenas no âmbito da autonomia privada**, não se estendendo tal possibilidade no âmbito do direito público.

116. Feitas as digressões acerca da validade e eficácia da assinatura eletrônica e da assinatura digital no direito brasileiro, passa-se ao exame da sua juridicidade na Administração Pública, à luz do regime jurídico-administrativo, e da regulamentação específica aplicável à esfera pública federal.

3) ASSINATURA ELETRÔNICA NA ADMINISTRAÇÃO PÚBLICA

3.1) O princípio da legalidade e a necessidade de prévia previsão legal para prática de atos administrativos em meio eletrônico

117. Não há dúvidas de que a adoção de sistemas eletrônicos no âmbito da Administração Pública é medida salutar, importando em diversos benefícios, tais como maior celeridade, economicidade, racionalidade e eficiência aos procedimentos e processos administrativos. De se ver, aliás, que a eficiência é princípio geral da administração inserto no art. 37 da Constituição Federal pela EC n° 19/98. Por sua vez, o art. 5º, inc. LXXVIII, introduzido pela EC n° 45/04, erigiu o princípio da celeridade ao *status* de direito fundamental, dispondo que *"a todos no âmbito judicial e administrativo, são assegurados a razoável duração do processo e os meios que garantam a celeridade de sua tramitação"*.

118. A automatização dos processos e procedimentos administrativos insere-se, pois, dentro de um novo paradigma de administração denominado de "governo eletrônico" ***[31]***, assim entendido como sendo *"a contínua otimização da prestação de serviços do governo, da participação dos cidadãos e da administração pública pela transformação das relações internas e externas através da tecnologia, da Internet e dos novos meios de comunicação"*. ***[32]***

119. Em que pesem tais considerações, a adoção dos documentos eletrônicos no âmbito administrativo não pode ficar à margem da lei. **A possibilidade técnica não importa na possibilidade jurídica**, ainda que a adoção de tal sistema represente a otimização da atividade administrativa, programaticamente inserta no texto constitucional. Isso porque, no âmbito administrativo, há de se observar, ao lado dos princípios da celeridade e eficiência, o **princípio da legalidade**, que, na esfera administrativa, significa tanto o dever de observância das determinações legais, como na impossibilidade de atuação administrativa, na sua ausência. A esse respeito, JUSTEN FILHO esclarece que:

> O princípio da liberdade, que norteia a vida privada, conduz à afirmação de que tudo o que não estiver disciplinado pelo direito está abrangido na esfera de autonomia. Portanto, a ausência de disciplina jurídica é interpretada como liberação para o exercício das escolhas subjetivas. Isso se traduz no postulado de que tudo o que, em virtude de lei, não for proibido nem obrigatório será reputado como permitido. Portanto, a omissão de disciplina por parte do direito interpreta-se como legitimação da autonomia privada.
>
> Quando se consideram as relações regidas pelo direito público, a situação se altera. Assim se põe porque o exercício de competências estatais e de poderes excepcionais não se funda em alguma qualidade inerente ao Estado ou a algum atributo do governante. Toda organização estatal, a atividade administrativa em sua integralidade, a instituição de funções administrativas são produzidas pelo direito. Logo, a ausência de disciplina jurídica tem de ser interpretada como ausência de liberação para o exercício de algum poder jurídico. Daí afirmar que, nas relações de direito público, tudo o que, em virtude de lei, não for autorizado, será reputado como proibido.
>
> Mais ainda, no âmbito publicístico presume-se que tudo o que, em virtude de lei, for autorizado será reputado como obrigatório. Ou seja, não há cabimento em imaginar que o direito atribuiria poderes para que alguém escolhesse entre fazer ou não fazer – ressalvadas as hipóteses em que essa for a vontade normativa. ***[33]***

120. Nesse mesmo sentido, a doutrina de CELSO ANTONIO BANDEIRA DE MELLO:

> O princípio da legalidade, no Brasil, significa que a Administração nada pode fazer senão o que a lei determina. Ao contrário dos particulares, os quais podem fazer tudo o que a lei não proíbe, a Administração só pode fazer o

> que a lei antecipadamente autorize. Donde, administrar é prover aos interesses públicos assim caracterizados em lei, fazendo-o na conformidade dos *meios e formas* nela estabelecidos e particularizados segundo suas disposições. Segue-se que a atividade administrativa consiste na produção de decisões e comportamentos que, na formação escalonada do Direito, agregam níveis maiores de concreção ao que já se contém abstratamente na lei. ***[34]***

121. Portanto, no caso da Administração Pública, somente poderão ser utilizadas formas de comprovação da autenticidade e integridade de documentos eletrônicos **previamente autorizadas por lei**, como explica CESAR SANTOLIM:

> Reafirma-se que a validade dos atos jurídicos por meio eletrônico (em geral) depende da presença de elementos materiais, decorrentes da tecnologia empregada, que garantam a indelebilidade dos registros e a identificabilidade dos sujeitos implicados. Ademais, tem-se admitido, em matéria de relações de Direito Privado, em atenção ao princípio da equivalência funcional, que qualquer solução encontrada (hardware ou software) para a obtenção destes elementos deve ser considerada, sob a perspectiva jurídica, como adequada (princípio da neutralidade tecnológica). Ainda que fortes argumentos existam para mitigar a importância desta idéia, não se pode desconhecer que boa parte das legislações existentes sobre "documento eletrônico" e "assinatura eletrônica" são tecnologicamente neutras. Mesmo a legislação brasileira que criou a Infra-Estrutura de Chaves Públicas Brasileira (MP nº 2200-2, de 24.08.2001), consagrando aquele que é o mecanismo mais comum de atribuição de validade e eficácia jurídica aos registros eletrônicos (chaves públicas e privadas baseadas em softwares de criptografia assimétrica) deixou aberta a possibilidade do uso de outras soluções (§2º do art. 10), independentemente de expressa previsão legal.
>
> **No caso dos "atos administrativos eletrônicos", todavia, é inviável a adoção de qualquer solução tecnológica que não esteja contemplada em norma expressa, em atenção a idéia de legalidade estrita que se aplica à Administração Pública (ao contrário dos agentes privados, que podem fazer tudo o que a lei não lhes proíbe, os agentes públicos só podem fazer o que a lei lhes permite).**
>
> **A necessidade de prévia autorização normativa para o uso de meios eletrônicos para a prática de atos jurídicos pela Administração Pública decorre, além da circunstância de que estes atos, por regra geral, são sempre formais, também de que devem ser, necessariamente, sindicáveis, o que só é possível diante de normas expressas que digam respeito à sua confecção.** ***[35]***

122. É imprescindível, assim, a verificação quanto à conformação das medidas que pretende ao arcabouço legal existente, o que será feito, primeiramente, a partir do exame da validade jurídica dos atos administrativos, mediante o uso da certificação digital ICP-Brasil, bem como da aplicabilidade ou não do art. 10, §2°, da MP n° 2.200-2/2001 à Administração Pública - que, como visto anteriormente, consagrou o princípio da liberdade de forma, ao admitir a utilização de outros meios de certificação digital, além da ICP-Brasil -, para, a partir daí, se examinar a regulamentação trazida pelos Decretos n° 3996/2001 e 8.539/2015. Por fim, serão tecidas algumas considerações acerca do âmbito de incidência da MP n° 2.200-2/2001 no tocante aos demais entes federativos.

3.2) A obrigatoriedade legal da utilização de certificados ICP-Brasil na Administração Pública Federal

123. A Lei n° 9.784/99, que regula o processo administrativo no âmbito da Administração Pública Federal, não tratou especificamente acerca do chamado processo eletrônico/digital. Dispõe, em seu art. 22, §1º que *"os atos do processo devem ser produzidos por escrito , em vernáculo, com data e local de sua realização e a* ***assinatura da autoridade responsável****"*. Por sua vez, o §4º do mesmo artigo e lei estabelece que *"o processo terá suas páginas numeradas sequencialmente e rubricadas"*.

124. A sistemática disposta na Lei n° 9.784/99 parece, portanto, pressupor que o processo administrativo, bem como os atos administrativos, sejam realizados na forma papelizada, dado tanto a inexistência de qualquer referência à possibilidade de ato ou processo eletrônico/digital, como – e principalmente – na exigência de **assinatura da autoridade administrativa competente**, tradicionalmente aposta de forma manual, como expressão típica de manifestação de vontade.

125. Ocorre que a Lei n° 9.784/99 não pode ser lida de forma isolada, devendo, antes, ser interpretada à luz do sistema jurídico-administrativo no qual encontra-se inserta, de onde se destaca, para os fins da presente análise, a Medida Provisória n° 2.200-2/01. Referida MP estabeleceu as regras aplicáveis à certificação digital e implementou o que se convencionou chamar ordinariamente de "assinatura digital", como já exposto no decorrer dessa análise.

126. A MP n° 2.200-2/01 expressamente reconhece e admite a possibilidade de **documentos públicos produzidos de forma eletrônica**, conforme se observa do *caput* de seu art. 10, *verbis:*

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

127. **Diante disso, não há qualquer dúvida quanto à possibilidade da utilização de documentos públicos para a prática dos atos administrativos.**

128. Assim sendo, o cerne da questão reside não na viabilidade jurídica quanto à realização de atos administrativos por meio eletrônico - expressamente admitida pelo *caput* do art. 10 acima transcrito -, mas na **forma** que tais atos deverão ser formalizados.

129. O art. 22, §1°, da Lei n° 9.784/99, ao dispor que os atos administrativos deverão ser "escritos" e "assinados" pela autoridade competente, estabelece um **requisito formal específico** para a exteriorização da vontade administrativa pelo agente público, a ser observado independentemente do suporte em que o documento se encontre.

130. ODETE MEDUAR destaca a importância da exteriorização da vontade administrativa:

> Em sentido amplo forma significa exteriorização da vontade ou exteriorização da decisão, para o fim de produzir efeitos no âmbito do Direito. Se na formação do ato jurídico de natureza privada a exteriorização da vontade é relevante, no ato administrativo a exteriorização reveste-se de grande importância, tendo em vista o fim de interesse público a que visa, daí decorrendo a necessidade de ser conhecido pelos cidadãos, por outros órgãos da Adminsitração e pelos órgãos de controle. ***[36]***

131. Acerca da forma que se reveste o ato administrativo, destacam-se as lições de MOREIRA NETO:

> O terceiro elemento do ato administrativo é a forma; se no Direito Privado prevalece o princípio da liberdade de forma, no Direito Público a regra é a formalidade. Forma é a exteriorização do ato, absolutamente necessária para assegurar a plena publicidade, sindicabilidade e estabilidade das relações jurídicas. ***[37]***

132. Ora, se a lei (no caso, o art. 22, §1º, da Lei n° 9.784/99) exige que os atos administrativos sejam **escritos e assinado**s pela autoridade competente, é evidente que, quando praticados por meio eletrônico, **tal ato administrativo deverá ser formalizado mediante a utilização de tecnologia que, também por lei, seja equivalente à assinatura manuscrita, sob pena de infração do princípio da legalidade, que rege a atividade administrativa**.

133. E, como visto no capítulo anterior, **a única forma de assinatura eletrônica equiparada, por lei, à assinatura manuscrita no direito brasileiro, se dá mediante o uso do processo de certificação da ICP-Brasil, por força do disposto no art. 10, §1°, da MP n° 2.200-2/2001.**

134. Tal constatação, por si só, já seria mais do que suficiente para concluir que **o ato administrativo, quando praticado por meio eletrônico, deverá, obrigatoriamente (cuida-se de uma imposição legal, e não de uma mera faculdade) ser realizado mediante a utilização do processo de certificação da ICP-Brasil, vedada qualquer outra forma de assinatura ou certificação digital.**

135. Conforme FILGUEIRAS JUNIOR:

> Apenas admitir que o ato eletrônico é também escrito não resolve a contento o problema, isto porque, como bem salienta o Prof. DUNI, por ato escrito entende-se aquele ato que é subscrito, o que não se poderá assim considerá-lo pelo simples fato de ser eletrônico, dado as inegáveis questões que envolvem a assinatura eletrônica. Desse modo, para se considerá-lo escrito e subscrito requer-se a identificação de uma assinatura eletrônica segura e confiável.
>
> **No caso da MP 2.200/01, a certificação digital provinda da ICP-Brasil é atualmente o sistema oficial para atribuir validade à assinatura digital dos documentos eletrônicos. Logo, pode-se afirmar que o ato administrativo eletrônico emitido com base no sistema de certificação eletrônica da ICP-Brasil é considerado um ato escrito e também subscrito. E em sendo o sistema oficial, criado por Lei (Medida Provisória, por enquanto), a ninguém é dado desconhecê-lo ou mesmo argüir em defesa o seu**

> **desconhecimento, tal como enuncia o art. 3° da Lei de Introdução ao Código Civil. Por tudo isso, é o § 1°, do art. 10 da MP, que, em princípio, dá amparo à existência jurídica do ato administrativo eletrônico.** *[38]*

136. Mas, não bastasse isso - que, a nosso entender já derruba por terra qualquer pretensão de utilização de outro modelo de certificação digital na Administração Pública Federal que não a ICP-Brasil -, tal conclusão pode ser alcançada sob outro(s) enfoque(s), qual seja, a inaplicabilidade do disposto no §2° do art. 10 da MP n° 2.200-2/2001 ao Poder Público, bem como os princípios da eficiência e da razoabilidade, todos a ratificar o entendimento aqui exposto, conforme se passará a discorrer nos itens seguintes.

3.3) Da inaplicabilidade do disposto no art. 10, §2º, da MP n. 2.200-2/2001 ao Poder Público

137. Consoante já examinado no capítulo anterior, o art. 10, §2°, da MP n° 2.200-2/2001 admite expressamente a utilização de outros meios de comprovação da autoria e integridade de documentos produzidos em forma eletrônica, inclusive a utilização de certificados digitais não emitidos pela ICP-Brasil, desde que assim aceito pelas partes ou pela pessoa a quem for oposto o documento.

138. Tal dispositivo tem sido invocado pelos diversos entes administrativos, inclusive por alguns órgãos e entidades governamentais, como fundamento legal para a admissibilidade de outras formas de certificação digital na esfera administrativa, da qual é exemplo o próprio e-Gov, e o Decreto n° 8.539/2015.

139. A questão que se coloca, portanto é: o art. 10, §2°, da MP n° 2.200-2/2001 seria aplicável também às relações regidas pelo regime jurídico-administrativo? Ou, melhor dizendo, estaria tal dispositivo admitindo a utilização de outras formas de certificação digital também por parte da Administração Pública, mediante regulamentação específica?

140. Trata-se de questão de especial relevância: se a atividade administrativa encontra-se submetida ao princípio da legalidade, como de fato ocorre, a admissibilidade de qualquer outra forma de certificação digital em âmbito administrativo, somente poderia ser cogitada mediante prévia previsão legal que permitisse tal entendimento. E, como se sabe, o fundamento legal para a utilização de *outras formas de certificação,* além da ICP-Brasil, no direito brasileiro, encontra-se no §2º do art. 10 da MP n° 2.200-2/2001, cujos aspectos gerais foram objeto de análise no capítulo anterior. Mostra-se imprescindível, assim, examinar se tal dispositivo legal seria ou não aplicável na esfera pública.

141. Como exaustivamente demonstrado no decorrer deste parecer, a viabilidade jurídica da adoção de modelos de certificação digital alheios à ICP-Brasil encontra fundamento no princípio da **autonomia privada**, mais precisamente na liberdade das formas, insculpido no art. 107 do CC e, em âmbito digital, no §2° do art. 10 da MP n° 2.200-2/2001.

142. FABIANO MENKE, deixa claro o caráter privativo da norma, ao comentar o dispositivo em testilha:

> **Com isso, resta garantida a autonomia privada e a liberdade que os sujeitos possuem para utilizarem o meio mais adequado e proporcional à importância do negócio ou da comunicação encetada.** Ainda que o ambiente virtual possa apresentar inseguranças, partes que já se conhecem e têm um histórico de realizarem negócios poderão decidir correr eventuais riscos e eleger até mesmo o correio eletrônico para a prática de atos negociais. Há que se ter em mente que a assinatura digital é conceito apropriado às redes abertas, a ser utilizado por indivíduos que não se conhecem e jamais mantiveram contato. Não que esse fator exclua a racionalidade e importância de utilizá-la também em redes fechadas composta por partes já familiarizadas umas com as outras - pois o ideal seria que todos empregassem a técnica mais segura possível - mas **a ponderação do meio de comprovação de autoria e integridade a ser utilizado em negócios estritamente provados é escolha que via de regra deve caber às próprias partes interessadas.** *[39]*

143. A redação dada ao §2º do art. 10 da MP n° 2.200-2/2001, ao admitir a utilização de outros meios de certificação "**desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento",** não deixa qualquer margem de dúvida que **a norma tem nítido caráter privado**, sustentando-se no princípio da **autonomia privada e na liberdade das formas**.

144. Via de consequência, o §2° do art. 10 da MP n° 2.200-2/2001 tem âmbito de aplicação exclusivo nas relações entre particulares, **não se estendendo às atividades administrativas, regidas pelo direito público, nas quais o interesse particular cede espaço ao interesse público, e a prática dos atos administrativos deve observar a forma prescrita em lei.**

145. Com efeito, diferentemente do que se dá no direito privado, onde a autonomia da vontade mostra-se como vetor

fundamental, a atividade administrativa volta-se à consecução do **interesse público,** de onde decorrem os dois princípios basilares do regime jurídico-administrativo: **supremacia do interesse público sobre o privado** e a **indisponibilidade do interesse público.** Conforme expõe LUCAS ROCHA FURTADO, *"o binômio prerrogativas públicas/interesses públicos confere ao regime jurídico administrativo a sua principal característica, e esta pode ser traduzida pela seguinte expressão: o regime jurídico administrativo se caracteriza pela realização do interesse público"* ***[40]***.

146. Segundo o **princípio da supremacia do interesse público sobre o privado**, os atos praticados pelo Poder Público, por estarem voltados à proteção de interesses de toda a coletividade, possuem prevalência sobre os interesses particulares, conforme ensina CELSO ANTÔNIO BANDEIRA DE MELLO:

> Trata-se de verdadeiro axioma reconhecível no moderno Direito Público. Proclama a superioridade do interesse da coletividade, firmando a prevalência dele sobre o do particular, como condição, até mesmo, da sobrevivência deste último.
>
> (...)
>
> A posição de supremacia, extremamente importante, é muitas vezes metaforicamente expressada através da afirmação de que vigora a verticalidade nas relações entre Administração e particulares; ao contrário da horizontalidade, típica das relações entre estes últimos. Significa que o Poder Público se encontra em situação de autoridade, de comando, relativamente aos particulares, como indispensável condição para gerir os interesses públicos postos em confronto. Compreende, em face da sua desigualdade, a possibilidade, em favor da Administração, de constituir os privados em obrigações, por meio de ato unilateral daquela. Implica, outrossim, muitas vezes o direito de modificar, também unilateralmente, relações já estabelecidas. ***[41]***

147. Por sua vez, ainda de acordo com o renomado professor, o **princípio da indisponibilidade do interesse público,** *"significa que, sendo interesses qualificados como próprios da coletividade - internos ao setor público -, não se encontram à livre disposição de quem quer que seja, por inapropriáveis. O próprio órgão administrativo que os representa não tem disponibilidade sobre eles, no sentido de que lhe incumbe apenas curá-los - o que é também um dever - na estrita conformidade do que predispuser a 'intentio legis'".* ***[42]***

148. E, se assim é, **resta clara a inaplicabilidade do disposto no art. 10, §2º, da MP n. 2.200-2/2001 a tais atos, uma vez que tal norma prevê expressamente, como dito, a "*admissão*" ou "*aceitação*" da modalidade escolhida para validação do documento produzido sob forma eletrônica pelas partes ou pela pessoa a quem for oposto.** Ora, o interesse público jamais poderá estar condicionado à vontade individual dos administrados ou mesmo dos agentes públicos.

149. Não é outro, aliás, o entendimento praticamente unânime da doutrina que se debruçou sobre o tema.

150. AIRES J. ROVER e HÉLIO SANTIAGO RAMOS JÚNIOR, examinando especificamente o ato administrativo eletrônico, assim se pronunciaram:

> Por sua vez, a Medida Provisória 2.200-2/01 criou a Infra-Estrutura de Chaves Públicas Brasil - ICP-Brasil e teve como objetivo dar validade aos documentos eletrônicos. **Em seu art. 10, caput, considerou-os como documentos públicos ou particulares para todos os fins legais e, no §1º deste mesmo dispositivo, estabeleceu uma presunção de veracidade para os documentos eletrônicos que fossem assinados digitalmente e que utilizassem os certificados da ICP-Brasil. A partir daí, surge a possibilidade de se admitir a existência do ato administrativo eletrônico apto a produzir efeitos no processo administrativo, nos moldes do art. 22, §1º da Lei n. 9.784/99, desde que respeitado o princípio da publicidade dos atos administrativos para assegurar aos litigantes o direito à ampla defesa e ao contraditório nos processos judiciais ou administrativos, de acordo com o art. 5º, inc. LV da CF/88.**
>
> Conforme estabelece o §2º do art. 10 da MP 2.200-2/01, *"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"*. **A simples leitura dessa norma permite a constatação de que o mencionado §2º do art. 10 desta Medida Provisória não poderá ser aplicável para comprovar a existência de um ato administrativo praticado por meios eletrônicos, isso porque a vontade das partes não pode ser fator determinante da existência de um ato administrativo, por força da supremacia do interesse público sobre o particular. Não poderia ser diferente, pois, caso assim fosse, restaria ameaçada a segurança jurídica bem como estariam comprometidos os princípios da moralidade, da impessoalidade e da legalidade. Enfim, por ser regra de direito privado, não tem aplicação no âmbito**

do direito administrativo.

Por outro lado, **poder-se-á aplicar o disposto no art. 10, caput e §1º da Medida Provisória 2.200-2/01, sendo exatamente este o fundamento legal que dá amparo à existência do ato administrativo eletrônico capaz de produzir efeitos no processo administrativo, pois, conforme ensina Filgueiras Junior, é possível afirmar que *"o ato administrativo eletrônico emitido com base no sistema de certificação eletrônica da ICP-Brasil é considerado um ato escrito e também subscrito"*. *(grifamos)* *[43]***

151. Nesse sentido também é o entendimento de ANDRÉ PINTO GARCIA:

> Diante de suas características, **as assinaturas eletrônicas apenas cuidam de interesses meramente privados (interpartes), e não públicos, como o certificado ICP Brasil o faz. Um documento público, em geral destinado a produzir efeitos em qualquer lugar do Brasil, não poderia, nunca, se valer de outras formas de assinatura que não a digital.**
>
> Tomemos, como exemplo, talvez o mais importante de todos, uma certidão de nascimento. Acaso se adote a sua forma eletrônica, existem duas alternativas para se conferir validade jurídica, nos termos da Medida Provisória 2.200-2/01: a) a assinatura do documento, pelo seu responsável legal (no caso,o registrador civil de pessoas naturais), com certificado ICP Brasil; b) a solicitação de aquiescência de todos aqueles que deverão observância, isto é, toda a população brasileira, além das pessoas jurídicas de direito público interno e externo externo.
>
> Dessa forma, **não há sombra de dúvida acerca do modelo que os documentos públicos devem adotar, até mesmo por imposição constitucional, que veda, em seu art. 19, inc. II, à União, aos Estados, ao Distrito Federal e aos Municípios a recusa de fé aos documentos públicos. Ora, só se pode reconhecer fé naquilo que possua segurança (ao contrário do que ocorre com os documentos privados, nos quais a autonomia da vontade decide o que melhor aprouver aos partícipes da avença).** *(grifamos)* ***[44]***

152. Na mesma linha, porém salientando também a necessidade de utilização de um meio oficial de certificação digital, FILGUEIRAS JUNIOR, em importante obra sobre o tema, é enfático:

> No caso da MP 2.200/01, a certificação digital provinda da ICP-Brasil é atualmente o sistema oficial para atribuir validade à assinatura digital dos documentos eletrônicos. Logo, pode-se afirmar que o ato administrativo eletrônico emitido com base no sistema de certificação eletrônica da ICP-Brasil é considerado um ato escrito e também subscrito. E em sendo o sistema oficial, criado por Lei (Medida Provisória, por enquanto), a ninguém é dado desconhecê-lo ou mesmo argüir em defesa o seu desconhecimento, tal como enuncia o art. 3° da Lei de Introdução ao Código Civil. Por tudo isso, **é o § l°, do art. 10 da MP, que, em princípio, dá amparo à existência jurídica do ato administrativo eletrônico.**
>
> A contrário senso, **o § 2°, do art. 10, da referida MP, é inaplicável aos atos administrativos eletrônicos.** Isso porque o dispositivo admite como válida a certificação digital provinda de outro sistema, bastando ser acordada pelas partes. Ora, **tal disposição tem nítida feição de Direito Privado. Um acordo entre a Administração Pública e o administrado não é o suficiente para legitimar o ato, porque não será um meio oficial, e com base em lei, para a sua emissão.** Note-se que as relações jurídicas de Direito Administrativo formam-se ao influxo de finalidades gerais, previstas no ordenamento jurídico e não de vontades de seus participantes. Como afirmara Ruy Cirne LIMA, o fim - e não a vontade - domina todas as formas de administração.Por consequência, **a vontade das partes não poderá eleger uma condição de existência de um ato administrativo, que a todos interessa e não somente às partes. Noutras palavras, todo cidadão tem o direito de ver os atos administrativos eletrônicos editados por meio do sistema de certificação digital oficial e não por um sistema, que as partes elegeram, diferente do oficial, que é fixado por lei.** ***[45]***

153. Por tudo quanto o exposto, **resta evidente a inaplicabilidade do art. 10, §2°, da MP n° 2.200-2/2001 à Administração Pública na prática dos atos administrativos em geral, os quais, quando praticados em meio eletrônico no qual se exija certificação digital, deverá, obrigatoriamente, adotar a certificação da ICP-Brasil.**

3.4) Princípios da eficiência e da razoabilidade

154. A todos argumentos acima, juntam-se ainda os **princípios da eficiência** (insculpido no art. 37, *caput*, da Constituição Federal) e da razoabilidade (implícito na CF, e expresso no art. 2°, *caput,* da Lei n° 9.784/99).

155. O princípio da eficiência exige não apenas que o ato praticado pela Administração surta os efeitos que dele são

esperados (eficácia), mas também que o faça da melhor forma (eficiência) e com o menor custo possível (economicidade) para os administrados. É o que se extrai das lições de DINORÁ ADELAIDE MUSETTI GROTTI:

> O princípio da eficiência caracteriza-se como um conceito econômico, que introduz, no mundo jurídico, parâmetros relativos de aproveitamento ótimo de recursos escassos disponíveis para a realização máxima de resultados desejados. Não se cuida apenas de exigir que o Estado alcance resultados com os meios que lhe são colocados à disposição pela sociedade (eficácia), mas de que os efetue o melhor possível (eficiência), tendo, assim, uma dimensão qualitativa. [...] A eficiência diz respeito ao cumprimento das finalidades do serviço público, de molde a satisfazer necessidades dos usuários, do modo menos oneroso possível (economicidade), extraindo-se dos recursos empregados a maior qualidade na sua prestação. ***[46]***

156. Por sua vez, o princípio da razoabilidade, nos dizeres de DIRLEY DA CUNHA JUNIOR, *"impõe que as entidades, órgãos e agentes públicos, no desempenho de suas atividades, adotem meios que, para a realização de seus fins, revelem-se adequados, necessários e proporcionais".* ***[47]***

157. Por força de tais princípios, não seria razoável a adoção pela Administração de uma modalidade paralela ou alternativa de certificação digital ou de validação de documentos eletrônicos quando já existe toda uma Infraestrutura de Chaves Públicas nacional lastreada em padrões técnicos instituídos por lei e fiscalizados por uma autarquia federal que garante a observância dos requisitos de segurança física e lógica necessários à comprovação da autenticidade e da integridade de documentos públicos e privados praticados em meio eletrônico.

158. Além de gerar custos adicionais ao erário de forma injustificável, a adoção de outras modalidades de validação de documentos eletrônicos por parte dos órgãos públicos mostra-se desnecessária diante da previsão contida no art. 8º da MP 2.200-2/2001, segundo o qual órgãos e entidades públicas podem credenciar-se diretamente junto ao ITI como Autoridades Certificadoras e de Registro, tornando-se aptas a emitir certificados digitais no padrão ICP-Brasil:

> 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.

159. Assim, mesmo sob uma ótica principiológica, a adoção de qualquer sistema de certificação digital, distinto da ICP-Brasil por parte da Administração Pública, principalmente da Administração Pública Federal, mostra-se desprovido de qualquer fundamento, em absoluta dissonância com os princípios da eficiência e razoabilidade, notadamente quando se considera a existência de um sistema já estabelecido por lei, desde 2001, com plenas condições jurídicas e técnicas de assegurar a integridade e a autenticidade dos atos administrativos eletrônicos.

3.5) MP n° 2.200-2/2001 - Lei nacional ou federal?

160. Antes de se adentrar no exame da regulamentação federal editada (Decretos n°s 3.966/2001 e 8.539/2015), cumpre tecer algumas considerações finais a propósito do âmbito de incidência da MP n° 2.200-2/2001 aos demais entes federativos (Estados, Municípios e Distrito Federal). Ou seja, seria a MP n° 2.200-2/2001 aplicável aos demais entes federativos, ou tal norma estaria limitada ao âmbito federal (União)?

161. O questionamento foi enfrentado por ANDRÉ PINTO GARCIA, o qual é enfático quanto ao tema:

> Cabe assentar que a Medida Provisória 2.200 2/01 **é uma norma nacional, e não apenas federal, com aplicabilidade perante toda a organização político administrativa da República Federativa do Brasil, compreendida nessa a União, os Estados, os Municípios e o Distrito Federal (CF/ art. 18)**.
>
> Significa falar da unicidade territorial de tal modelo, **não facultado a qualquer outro ente político (Estados ou Municípios, p. ex) criar infraestruturas de certificação próprias**, ainda que sigam, por simetria, o modelo adotado na Medida Provisória. Conclui-se, portanto, que **o Brasil só possui uma (numeral e não artigo indefinido) infraestrutura de chaves públicas, instituída e mantida pela União, que possui abrangência perante todos os entes da federação.** ***[48]***

162. Ao se examinar a questão, deve-se ter em mente que a manifestação de vontade, e a própria validade e eficácia dos documentos eletrônicos é um tema afeto ao direito civil e processual, de competência privativa da União (art. 22, I, da CF). Como não bastasse, o mesmo art. 22, em seu inc. IV, dispõe ser igualmente da competência privativa da União legislar sobre informática e

telecomunicações.

163. De tal constatação se extrai duas consequências relevantes no tocante ao tema *sub examinen.* A primeira, a necessidade de lei em sentido estrito a disciplinar a questão (e não de um simples decreto regulamentar, ainda que federal). A segunda, que tal regramento legal deve ser editado pela União, estando vetado aos Estados, Municípios e ao Distrito Federal a edição de lei com o mesmo escopo.

164. Em importante precedente, o Tribunal Regional Federal da 4ª Região já teve oportunidade de se posicionar na linha do quanto aqui exposto. Tratava-se, no caso, do Decreto Municipal n° 4446/06, que instituiu, no âmbito do Município de Florianópolis, o Sistema de Autorização de Documentos Fiscais Eletrônicos - AEDF, operacionalizado por uma Autoridade de Registro (AR), própria da Secretaria Municipal da Receita, que não era integrante da ICP-Brasil. O Tribunal, por meio de decisão do Des. Federal EDGARD ANTÔNIO LIPPMANN JÚNIOR, manteve, por seus próprios fundamentos, sentença proferida pelo juízo *a quo,* que havia deferido Mandado de Segurança interposto contra o referido decreto, sob o seguinte entendimento, *verbis:*

> (...) Nesses termos, tenho que o permissivo em referência veio autorizar o uso da tecnologia em questão nas relações jurídicas entre particulares, nas circunstâncias em que é possível a uma das partes, ou ambas, a aceitação do Sistema ou do documento emitido em forma eletrônica.
>
> A irresignação do impetrante reside no uso de um sistema alheio ao âmbito da ICP-Brasil que se pretende organizar e garantir a emissão de documentos fiscais, ou seja, interferir nas relações de natureza tributária entre o Município de Florianópolis e os seus contribuintes.
>
> Nesse particular, tenho por acolher a argumentação no sentido de que o cumprimento de obrigações tributárias, ainda que acessórias (emissão de documentos fiscais), não pode ser executado na forma eletrônica fora do Sistema hierárquico da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, pela limitação expressa no próprio dispositivo do § 2º do art. 10.
>
> Ademais, o parágrafo primeiro do mesmo artigo dez assegura presunção de veracidade das declarações constantes dos documentos em forma eletrônica, desde que utilizado o processo de certificação disponibilizado pela ICP-Brasil. Em outras palavras, por maior que seja a segurança técnica oferecida pelo Sistema adotado pelo Fisco de Florianópolis (que não se questiona aqui), não pode ostentar a presunção legal de veracidade das declarações em relação aos signatários. Tal circunstância, de ordem legal, é incompatível no âmbito das relações de natureza tributária.
>
> O Decreto Municipal nº 4446/06, questionado nesta ação, introduz intenção de conferir presunção de veracidade aos documentos fiscais gerados e emitidos em forma eletrônica (art. 15). O referido Diploma, na condição de mero regulamento administrativo, não tem força de Lei, não podendo alterar a norma legal expressa acima destacada.
>
> Outra ponderação relevante destacada na inicial é a necessária garantia da interoperabilidade entre os diversos Sistemas, todos integrados, de forma hierárquica, ao Instituto Nacional de Tecnologia da Informação - ITI, o qual figura como Autoridade Certificadora Raiz e constitui uma raiz única. Tal garantia de interoperabilidade permitirá, no futuro, intercâmbio e gerenciamento de informações entre as entidades públicas que venham a operar com a tecnologia em questão, por exemplo: Receita Federal (já integrante), secretarias de fazenda estaduais e municipais.
>
> Nesse quadro, a existência de um sistema fechado, exclusivo de um município e seus contribuintes, tornaria difícil essa interoperabilidade.
>
> No mesmo sentido, aponto o trecho da decisão proferida no Agravo nº 2007.0400009343-4 (fl. 87), ao tratar do Sistema Nacional de Certificação Digital: Tal regramento encontra perfeita sintonia com o disposto no parágrafo único do art. 154, da Lei Adjetiva, ao dar tratamento unificado nacionalmente. Ora, não se diga que a matéria tratada no Decreto Municipal objurgado (n. 4.446/06), seria de índole eminentemente tributária - instituiu o Sistema de Autorização de Documentos Fiscais Eletrônicos - AEDE, criando-se uma autoridade de Registro (AR) própria da Secretaria Municipal da Receita -. Com isso, praticamente, estabeleceu um sistema de Infra-Estrutura de Chaves Públicas Municipal, paralelo, ao sistema nacional antes referido, de sorte que, acaso legitimada tal conduta, importaria em irrogar-se a todos os municípios do Brasil tal possibilidade, cujas consequências seriam desastrosas para o sistema.
>
> A mesma decisão considerou consistente a alegação de que a ICP-BRASIL objetiva constituir uma cadeia de confiança, cujo objetivo fundamental é o de permitir, nacionalmente, a comprovação da autenticidade e da integridade das manifestações de vontade das pessoas físicas e jurídicas. (...) ***[49]***

165. Portanto, não há dúvidas que a MP n° 2.200-2/2001 é uma lei nacional, decorrente do exercício da competência privativa da União, aplicável a todas as esferas da Administração (União, Estados, Municípios e Distrito Federal), de tal modo que

todas as considerações aqui realizadas aplicam-se, em nosso entender, também aos demais entes federados.

166. Posto isso, passemos ao exame jurídico da regulação federal editada, mais precisamente dos Decreto n°s 3.996/2001 e 8.539/2015.

4) DA REGULAMENTAÇÃO FEDERAL: DECRETOS N°S 3.996/2001 E 8.539/2015

167. A certificação digital, no âmbito da Administração Pública Federal, encontra-se regulamentada por dois principais diplomas, quais sejam, o Decreto n° 3.996/2001, e o Decreto n° 8.539/2015.

168. O Decreto n° 3.996/2001 *"dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal"*. Cuida-se da **principal norma regulamentar**, na administração federal, a respeito da certificação digital, que regulamentou a prestação de serviços de certificação a **toda a Administração Federal, direta e indireta** (art. 1°).

169. Registre-se, primeiramente, que, por se tratar de um **decreto presidencial,** tal norma prevalece sobre todas as normas regulamentares editadas pelos demais órgãos e entidades integrantes da Administração Federal. Vale dizer, salvo se a lei (em sentido estrito) dispuser em sentido contrário, qualquer ato regulamentar, oriundo de quaisquer dos órgãos e entidades federais devem, necessária e obrigatoriamente, observar o disposto no referido decreto.

170. O modelo de certificação que deverá ser observado pela Administração Federal encontra-se previsto no art. 2º, §1°, e art. 3°, do mencionado decreto, os quais dispõem, *in verbis:*

> Art. 2°. (...)
>
> § 1º ***Os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.***
>
> (...)
>
> Art. 3º A **tramitação de documentos eletrônicos para os quais seja necessária ou exigida a utilização de certificados digitais somente se fará mediante certificação disponibilizada por AC integrante da ICP-Brasil.**

171. O dispositivo em testilha é de uma objetividade e de uma clareza solar, não deixando qualquer margem para interpretação distinta: **tratando-se de certificação digital, os órgãos e entidades da Administração Pública Federal devem, obrigatória e exclusivamente, se utilizar da certificação digital provida no âmbito da ICP-Brasil.** Em consequência, qualquer outra espécie de certificação digital encontra-se, por força de expressa determinação regulamentar, vedada à Administração Pública Federal.

172. Cumpre consignar que a necessidade de utilização de certificação provida pela ICP-Brasil na administração federal já foi objeto de manifestação, no âmbito da Advocacia Geral da União, pela Procuradoria Geral Federal que, no Parecer n° 20/2014 /DEPCONSU/PGF/AGU, aprovado pelo Diretor do Departamento de Consultoria/PGF n° 37/2014 e também pelo Procurador-Geral Federal, entendeu que ***"sendo constatada a necessidade ou a exigência de utilização de certificados digitais para a tramitação de documentos eletrônicos, somente se fará mediante certificação disponibilizada por AC integrante da ICP-Brasil"***.

173. Por fim, duas últimas observações a respeito do Decreto n° 3.996/2001 merecem registro.

174. Primeiro, é de se salientar que o mencionado decreto permanece válido e em vigor, não tendo sido revogado nem tácita, nem expressamente, pelo Decreto n° 8.539/2015, cujo âmbito de incidência é distinto face ao regulamento em questão. Com efeito, enquanto que o Decreto n° 8.539/2015 trata, especificamente, do processo eletrônico administrativo e, mais precisamente do trâmite procedimental, o Decreto n° 3.996/2001, tem por escopo a certificação digital como um todo, abarcando não apenas os atos produzidos no bojo do processo administrativo eletrônico, mas também outras formas de certificação digital, tais como os certificados SSL, relativos a *sites,* como os chamados *certificados de equipamentos,* utilizados, por exemplo, pela RFB nos equipamentos emissores das notas fiscais.

175. Em segundo lugar, é de se ver que a própria previsão regulamentar nada mais fez que explicitar o que já conta da lei

(em sentido estrito), que, como demonstrado no capítulo anterior, não permitem outra conclusão senão pela obrigatoriedade da utilização da certificação ICP-Brasil na assinatura, pela autoridade competente, de atos administrativos pela Administração Pública e, de maneira geral, quando se fizer necessária a certificação digital, para fins de comprovação de integridade e autenticidade em meio digital (como será adiante esclarecido, outras formas de "assinatura eletrônica" podem, eventualmente, até serem admitidas para outras finalidades específicas, nas quais não se faça necessária ou obrigatória a certificação digital; porém, quanto a forma de certificação digital em si, somente a ICP-Brasil mostra-se como meio adequado e legalmente admitido na Administração, por força de lei, não podendo norma infralegal dispor em sentido diverso, sob pena de patente ilegalidade).

176. Como se nota, portanto, há pouco a se discorrer acerca da previsão regulamentar, dado a clareza dos seus dispositivos, senão que ela **encontra-se em perfeita harmonia com a disposição legal sobre o tema, conforme buscamos demonstrar ao longo de todo esse parecer.**

177. O mesmo, contudo, não pode ser dito acerca do Decreto n° 8.539/2015, que dispõe *"sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional"*. Referido decreto regulamentou o processo administrativo federal na sua forma eletrônica, trazendo disposições diversas acerca do procedimento e aspectos técnicos relacionados à tramitação de documentos.

178. No que importa à presente análise - e, mais precisamente, ao tema afeto à consulta formulada, qual seja a certificação digital - importa destacar o disposto no art. 6°, *caput* e §1°, que estabelecem, *verbis:*

> Art. 6º **A autoria, a autenticidade e a integridade dos documentos e da assinatura, nos processos administrativos eletrônicos, poderão ser obtidas por meio de certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, observados os padrões definidos por essa Infraestrutura.**
>
> **§ 1º O disposto no caput não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem identificação por meio de nome de usuário e senha.**
>
> § 2º O disposto neste artigo não se aplica a situações que permitam identificação simplificada do interessado ou nas hipóteses legais de anonimato.

179. Em uma interpretação literal, o dispositivo *retro* parece dispor que a utilização da ICP-Brasil no processo administrativo eletrônico se constituiria em uma mera faculdade da Administração, a qual poderia se valer de outros meios de comprovação de autoria e integridade *"inclusive os que se utilizem identificação por meio de nome de usuário e senha"*.

180. **Tal interpretação, contudo, não subsiste a uma análise mais detida da disposição regulamentar, tanto sob a ótica técnica, como na ótica jurídica.**

181. De plano, cumpre desde logo destacar que o §1° do art. 6° do Decreto n° 8.539/2015, ao permitir a comprovação da autenticidade e integridade de documentos eletrônicos mediante o uso de *login* e senha, contém uma grave **impropriedade técnica**.

182. A esse respeito, assim se posicionou a DINFRA no Parecer Técnico SEI n° 0392647:

> **O emprego de usuário e senha não garante, em absoluto, nem a presunção de autoria, nem muito menos a integridade de documentos eletrônicos**.
>
> 51. Explica-se.
>
> 52. Usuário e senha, por si só, quando ampliado a realizar processos de assinatura eletrônica, é um sistema falho por natureza. É, usualmente, um segredo compartilhado: a senha, teoricamente sigilosa, é armazenada em um servidor do depositário – dessa forma, não apenas o seu proprietário tem acesso e a manipula. Quando usado para autenticação, via de regra a referida senha trafega abertamente na rede, estando suscetível a violações ou cópias mal-intencionadas de toda espécie. Ora, nada mais frágil sob a ótica da segurança da informação, visto que o elemento que assina é compartilhado, ou seja, com usuário e senha assina-se e verifica-se eletronicamente com o mesmo elemento. É comum notícias de furtos a senhas pelo mundo, utilizando, as vezes, técnicas simples de ataques.

> 53. Ainda que se exija alguma senha mais robusta, tais como a utilização de letras e números, *hashing* passwords, selos, a adoção da tecla *Caps Lock*, entre outros, o *login* não perderá a sua fragilidade.
>
> 54. A consequência de assinar eletronicamente com usuário e senha, em termos mais explícitos, é que basta a negativa (repúdio) de quem a utiliza para carrear o ônus da prova à outra parte.
>
> 55. Adentra-se a obscura tentativa de dar comprovação de integridade ao documento eletrônico por outras vias, como usuário e senha. É impossível nos dias atuais, tecnicamente, garantir, por si só, integridade a um documento eletrônico sem a utilização de um elemento criptográfico, como em uma assinatura digital. Integridade de um documento eletrônico deve ser feita utilizando regras matemáticas/computacionais que incidem diretamente na string de bits que compõem um documento eletrônico (ou no hash desse). É feito um cálculo criptográfico nesses bits, de modo a integralizá-los com a chave de assinatura de controle exclusivo do titular e tornar viável sua conferência por outro elemento distinto criptográfico, preservando fielmente o conteúdo da mensagem. Usuário e senha não possui processos seguros que incidem matematicamente nos bits de um documento eletrônico. São somente anexados a composição do documento, podendo ser facilmente manipulados. Ou seja, não se garante integridade de um documento eletrônico utilizando somente uma técnica de autenticação chamada de usuário e senha.
>
> 56. Admitir-se-ia, no limite, a utilização de usuário e senha apenas para fins de autenticação, isto é, para o (simples) acesso a sistemas informacionais, mas jamais, para se assinar com o reconhecimento de presunção de autoria ou integridade a qualquer documento eletrônico. Entretanto, **até para autenticação, é recomendável que se use outro método conjugado**. Existe uma forte tendência ao desuso do método usuário e senha inclusive para as autenticações.
>
> 57. Assim, **a autenticação por usuário e senha, por si só, não garante nem a autoria (não se tem como saber se aquela pessoa é efetivamente quem afirma o ser), nem tampouco o conteúdo da mensagem (que pode sofrer alterações no caminho entre o emissor e o destinatário). Qualquer disposição legal ou normativa, ao prever a comprovação de tais elementos por meio de usuário e senha, encontra-se completamente incongruente sob a ótica técnica, implicando, inevitavelmente, em insegurança técnica/jurídica.**
>
> 58. **Ademais, um documento eletrônico que possui anexado uma autenticação de usuário e senha não é autocontido. Significa que esse documento eletrônico só pode ser verificado dentro do próprio sistema que criou o usuário e senha.** Sem o sistema, o documento eletrônico não tem "vida", que é totalmente oposto a um documento assinado de forma manuscrita em papel ou assinado digitalmente. Um documento eletrônico precisa ter independência e interoperabilidade de sistemas para que esse possa ser autêntico.
>
> 59. Em um litígio judicial, ou simplesmente o repúdio por parte de alguém, não é possível periciar o documento e aferir prova de autoria e integridade. Isso significa que as partes (oficial e particular) devem ter acesso ao sistema para, talvez, encontrar outros indícios de autoria e integridade. Para sistemas públicos e de segurança isso pode se tornar um incidente muito grave.
>
> 60. Usar esse método simples de autenticação como uma garantia de presunção de autoria e integridade é, do ponto de vista técnico, o anonimato virtual de pessoas e das aplicações, sem rastreabilidade e sem a segurança dos dados. Por óbvio, usuário e senha, entre outros, não são métodos que se utilizam dos padrões, da segurança, da gestão de identidade e de sistemas criptográficos como a ICP-Brasil, conforme explicado. *(grifo nosso)*

183. Embora a questão tenha nítido fundamento técnico, colhe-se o mesmo entendimento na doutrina jurídica que, apontando as mesmas incongruências técnicas descritas pela DINFRA, explicitam a impossibilidade jurídica de se admitir tal modelo de assinatura eletrônica, como método de comprovação de autoria e integridade de documentos eletrônicos.

184. ANDRÉ PINTO GARCIA, ao discorrer acerca do *login* e senha para tal finalidade, bem demonstra a impropriedade jurídica da previsão normativa:

> Diante de todo o exposto, enfim, não seria muito mais simples o ordenamento jurídico brasileiro ter conferido validade jurídica à utilização do *login* e senha, tão difundido entre nós? Não seria muito menos oneroso, tanto

> para o governo brasileiro (que necessita manter uma Autarquia específica para tal finalidade), quanto para os usuários (que necessitam, de tempos em tempos, pagar pelos certificados)?
>
> A resposta é negativa. **Ao tratar de tecnologia, o direito não pode dotar de validade jurídica algo que não possua, intrínseca e tecnologicamente, segurança**. Revela se, assim, a interdisciplinariedade do direito da certificação digital, inserido em um campo mais amplo, o direito da informática.
>
> (...)
>
> Ainda que se exija alguma senha mais rebuscada, tais como a utilização de letras e números (tecnicamente denominada de alfanumérica), a adoção da tecla *Caps Lock* , etc., o *login* não perderá a sua natureza de mera assinatura eletrônica.
>
> Significa dizer, conforme visto nos exemplos acima citados, que **basta a negativa de quem a utiliza para carrear o ônus da prova à outra parte (que será a autora do processo judicial).** Justamente por isso, nos furtos eletrônicos ocorridos em contas bancárias, os bancos pagam desde logo os prejuízos sofridos com a transação fraudulenta, pois sabem que, em um eventual litígio judicial, terão a incumbência de demonstrar que não foi o titular da conta corrente quem a movimentou, fato esse que, de tão difícil ser provado, chega a ser enquadrado juridicamente sob um nome sugestivo: *probatio diabolica*. ***[47]***

185. MARCACINI é ainda mais enfático ao discorrer sobre o tema, deixando claro seu entendimento pela absoluta impossibilidade da utilização do *login* e senha (bem como a biometria, também defendida por alguns como eventual meio de assinatura de documentos) como uma forma de assinatura equiparada à assinatura manuscrita, como segue:

> **Senhas de acesso, por exemplo, não podem ser equiparadas à assinatura autógrafa.** Uma senha é, necessariamente, um segredo compartilhado entre o seu detentor e o sistema informático que se vale desse tipo de identificação para oferecer a ele algum serviço ou informação. A depender do nível de segurança do sistema, essa senha pode estar mais ou menos vulnerável a ataques, mas, ainda que esse risco pudesse ser completamente descartado, **uma senha de acesso não estabelece qualquer vínculo direto e inalterável entre ela própria e os documentos e informações enviados ou recebidos durante a comunicação; portanto, tais documentos, transmitidos durante uma comunicação autorizada pelo uso de senhas, não se tornam portáveis, como ocorre com os documentos em papel.**
>
> O mesmo pode ser dito do controle de acesso por meio de dados biométricos. Neste caso, apenas ocorreu a substituição de uma senha alfanumérica pela digitalização de características do corpo do usuário. Do mesmo modo, trata-se de um segredo compartilhado (pois o sistema em questão deve ter previamente cadastrado esse dado biométrico do usuário) e não é possível estabelecer um vínculo indissociável entre os dados biométricos e as informações transmitidas durante a comunicação. ***[50]***

186. **Como se nota, cuida-se de um fato técnico: usuário e senha jamais comprovará a integridade ou a autenticidade de qualquer documento que se valha, apenas, de tal método de assinatura eletrônica. A tecnologia empregada simplesmente não atende a tal funcionalidade.**

187. Assim, o §1° do art. 6° do Decreto n° 8.539/2015, ao dispor ser possível a comprovação de autenticidade e integridade mediante o uso de *login* e senha, é uma aberração técnica a sem mais poder, e que invariavelmente tornará tal previsão absolutamente inócua, além de representar séria insegurança jurídica, acaso aplicada em sua literalidade.

188. Mas o problema não se encerra por aí.

189. Mesmo que se ignorasse por completo a impossibilidade técnica que a norma busca possibilitar - i.e., a comprovação de autoria e integridade por meio de uma tecnologia inapta para tanto -, o que fazemos aqui *ad argumentandum tantum,* existem outras razões de cunho estritamente jurídico a impedir a aplicabilidade literal do disposto no art. 6°.

190. Como é conhecimento de qualquer pessoa que possua um mínimo de conhecimento jurídico, um ato regulamentar - e o Decreto n° 8.539/2015 é, indubitavelmente, um ato tipicamente regulamentar - **jamais poderá dispor de forma contrária ou distinta do que a lei (em sentido estrito) já tenha disposto.** Cuida-se de decorrência direta do princípio da legalidade que, no âmbito administrativo, ganha especial relevância, dado os princípios regentes da atividade administrativa.

191. E, como julgamos ter demonstrado no capítulo anterior, **por força de lei,** no Brasil, a **única** forma de certificação digital admitida para Administração Pública é a ICP-Brasil, como, corretamente, estabelece o Decreto n° 3.996/2001, não tendo aplicabilidade o disposto no §2° do art. 10 da MP n° 2.200-2/2001, o qual incide exclusivamente em âmbito privado, como

exaustivamente temos repetido ao longo de todo este parecer.

192. Dessa forma, entende-se que **o art. 6° do Decreto n° 8.539/2015 deve ser interpretado em consonância com as disposições legais que regem a matéria.**

193. Assim sendo, **sempre que exigida ou necessária a utilização de certificação digital por parte da Administração Pública, esta deverá, obrigatoriamente, ser provida no âmbito da ICP-Brasil, não sendo admitido qualquer outro método de certificação digital.**

194. Ademais, a formalização de atos administrativos (em sentido amplo), nos quais se exija a **assinatura da autoridade competente ou do agente público, na forma do art. 22, §1°, da Lei n° 9.784/99, como forma de exteriorização da vontade administrativa (tais como, contratos e acordos administrativos, atos decisórios de qualquer natureza, atos normativos, pareceres técnicos e jurídicos, atos que venham a conferir ou restringir direitos, e, de maneira geral, os atos descritos no art. 50, da Lei n° 9.784/99), deverão, obrigatoriamente, ser firmados mediante o uso de certificação digital provida no âmbito da ICP-Brasil.**

195. De outra banda, **admite-se a utilização de outras formas de "assinatura eletrônica" (assim considerado no sentido técnico do termo), inclusive do *login e senha,* no máximo, para fins de autenticação em sistemas (como, por exemplo, para acesso ao Sistema Eletrônico de Informações - SEI), ou documentos nos quais não seja exigida ou necessária a assinatura como forma de exteriorização da vontade (a exemplo de atos de mero expediente em geral).**

196. **Deve-se ter em mente, contudo, que, apenas poderão ser considerados "assinados" (no sentido jurídico do termo), os documentos eletrônicos nos quais tenha sido aposta a assinatura digital com uso de certificado digital da ICP-Brasil, por ser essa, como dito, a única forma de assinatura eletrônica equiparada à assinatura manuscrita no direito brasileiro (art. 10, §1°, da MP n° 2.200-2/2001).**

197. Feitas, pois as considerações pertinentes, passa-se à resposta dos questionamentos formulados pela RFB, o que será feito de forma objetiva, remetendo-se às considerações realizadas, quando pertinentes, evitando-se, com isso, repetições desnecessárias.

5) DOS QUESTIONAMENTOS DA RFB

2.1) O Decreto n° 3.996, de 2001, informa em seu art. 2°, §1°, que os serviços de certificação digital na Administração Pública Federal devem ser providos pela ICP-Brasil. Com base nesse dispositivo, é correto o entendimento de que os serviços digitais de governo na internet devem utilizar, exclusivamente, certificados ICP-Brasil?

198. A resposta é **positiva.**

199. Dispõe o mencionado dispositivo, *in verbis:*

> Art. 2°. (...)
>
> § 1º ***Os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.***

200. Tal previsão é complementada pelo art. 3º do mesmo diploma, segundo o qual ***"A tramitação de documentos eletrônicos para os quais seja necessária ou exigida a utilização de certificados digitais somente se fará mediante certificação disponibilizada por AC integrante da ICP-Brasil".***

201. Conforme discorremos no capítulo 4, a disposição regulamentar em testilha é de uma objetividade e de uma clareza solar, não deixando qualquer margem para interpretação distinta: **tratando-se de certificação digital, os órgãos e entidades da Administração Pública Federal devem, obrigatória e exclusivamente, se utilizar da certificação digital provida no âmbito da ICP-Brasil.** Em consequência, qualquer outra espécie de certificação digital encontra-se, por força de expressa determinação regulamentar, vedada à Administração Pública Federal.

202. Também como já se disse na ocasião, referido decreto nada mais fez que explicitar o que já era possível inferir das disposições legais sobre o tema (conforme se discorreu no capítulo 3 deste parecer). De se destacar, por fim, que o Decreto nº 3.996/2001 permanece válido em vigor, sendo a norma regulamentar regente da certificação digital na Administração Pública Federal.

b) O Decreto n° 8.539, de 2015, informa em seu art. 6°, §1°, que não se obsta a utilização de outro meio de comprovação de autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem identificação por meio de usuário e senha. Com base nesse dispositivo, é correto o entendimento de que os serviços digitais de governo na internet podem utilizar certificados fora da infraestrutura da ICP-Brasil?

203. A resposta é **negativa.**

204. Conforme discorremos no capítulo 4 acima, o §1º do art. 6º do Decreto nº 8.539/2015, ao permitir a comprovação da autenticidade e integridade de documentos eletrônicos mediante o uso de *login* e senha, prevê uma **impossibilidade técnica**, haja vista que tal forma de assinatura simplesmente não permite, tecnicamente, tal funcionalidade, o que invariavelmente tornará tal previsão absolutamente inócua, além de representar séria insegurança jurídica, acaso aplicado em sua literalidade.

205. Dessa forma, o art. 6º do Decreto nº 8.539/2015 deve ser interpretado a partir das disposições legais que regem a matéria. E, conforme se demonstrou no capítulo 3 deste parecer, a **única** forma de certificação digital admitida para Administração Pública no Brasil é a ICP-Brasil, como, corretamente, estabelece o Decreto n° 3.996/2001, não tendo aplicabilidade o disposto no §2° do art. 10 da MP n° 2.200-2/2001, o qual incide exclusivamente em âmbito privado.

206. Por tais motivos, entende-se que os serviços digitais de governo na internet, a exemplo do que deve se dar com todos os demais sistemas eletrônicos na Administração Federal, somente poderão utilizar certificados digitais providos no âmbito da ICP-Brasil, admitido-se o uso do *login* e senha, no máximo, para a autenticação de usuários em sistemas, mas jamais para fins de assinatura de documentos eletrônicos (e, mesmo assim, com a ressalva que tal método não tem o condão de comprovar nem a autenticidade, tampouco a integridade documental).

c) A MP n° 2.200-2, de 2001, regula em seu art. 10, §2°, que não se obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive o que se utilize de certificados não emitidos pela ICP-Brasil, desde que admitidos pelas partes como válido ou aceito pela pessoa a quem for oposto o documento, com base nesse dispositivo, é correto afirmar que o disposto no art. 6°, §1°, do Decreto n° 8.539, de 2015, depende de prévia manifestação de concordância entre as partes para utilização de certificados fora da ICP-Brasil?

207. A resposta é **negativa**.

208. Contudo, necessário esclarecer que o equívoco da afirmação contida no questionamento formulado não consiste na desnecessidade de prévia manifestação de concordância das partes, mas sim na **impossibilidade de utilização de certificados não emitidos pela ICP-Brasil em âmbito administrativo**.

209. Com efeito, como demonstrado no Capítulo 3, mais precisamente no subcapítulo 3.3, **o art. 10, §2º, da MP nº 2.200-2/2001 tem incidência restrita às relações privadas, não se aplicando no âmbito administrativo, pelas razões ali expostas.**

210. Dessa forma, conforme sustentamos no capítulo 4 deste parecer, o art. 6º do Decreto nº 8.539/2015 (e o seu §1º) deve ser interpretado a partir das disposições legais que regem a matéria, de onde decorre que a **única** forma de certificação digital admitida para Administração Pública no Brasil é a ICP-Brasil (pelas razões expostas no capítulo 3), como, aliás, corretamente prevê o Decreto n° 3.996/2001.

d) Se o Gov.br enviar as credenciais do usuário autenticado, para os serviços digitais de governo que o utilize, mediante assinatura com a ICP-Brasil, a garantia de autenticidade e não repúdio (art. 10, §1°, da MP n° 2.200-2, de 2001) restringe-se à comunicação entre o Gov.br e o serviço digital, ou abrange, inclusive a autenticação do usuário realizada pelo Gov.br, independentemente do certificado utilizado, para comunicação com o cidadão?

211. Limita-se unicamente ao **titular do certificado digital emitido no âmbito da ICP-Brasil**, não abrangendo a identificação realizada por meio de outra forma de certificação ou identificação do usuário.

212. Como demonstramos no capítulo 2 (itens 86 a 99), o §1º da MP nº 2.200-2/2001 estendeu aos documentos eletrônicos assinados com o processo de certificação digital da ICP-Brasil a presunção de veracidade outorgada pelo Código Civil aos documentos assinados de forma manuscrita - o que a doutrina especializada chama de equivalência funcional. Da mesma forma que se dá com os documentos assinados de forma manuscrita, a presunção legal em tela limita-se ao signatário, não se estendendo a eventuais terceiros. No caso das assinaturas digitais, o signatário é o titular do certificado, somente a ele incidindo a presunção em questão, não abarcando os eventuais usuários cuja identificação tenha previamente ocorrido pelo sistema de *login* e senha

e) Se a resposta ao item "d" for de que abrange a autenticação do usuário, é correto o entendimento de que, com base no disposto no art. 6°, §1°, do Decreto n° 8.539, de 2015, há comprovação de autoria e integridade para logins realizados por meio de usuário e senha no âmbito do Gov.br?

213. A resposta é **negativa.**

214. Como demonstrado no capítulo 4 acima, é tecnicamente impossível a comprovação de integridade e autenticidade mediante o simples uso de *login* e senha, a despeito da redação do art. 6º, §1º, do Decreto nº 8.539/2015.

215. Assim, a assinatura digital, mediante certificação digital, em um documento eletrônico, irá assegurar a integridade desse documento a partir da **aposição da assinatura digital com certificado ICP-Brasil**, e a autenticidade de tal documento, **com relação exclusivamente ao titular do certificado (e não o usuário previamente identificado por login e senha).**

216. **Repita-se que, nos termos do art. 10, §1º, da MP nº 2.200-2/2001, a presunção de veracidade das declarações contidas nos documentos eletrônicos produzidos com a utilização do processo de certificação disponibilizado pela ICP-Brasil limita-se ao seu signatário (assim considerado o titular do certificado digital, e não o usuário identificado por meio de login e senha).**

III. CONCLUSÃO

217. Face ao exposto, conclui-se que:

a) Nos termos do art. 10, §1º, da MP nº 2.200-2/2001, a **única** espécie de assinatura eletrônica equiparada à assinatura manuscrita no direito positivo brasileiro é a assinatura digital produzida com o uso do processo de certificação digital da ICP-Brasil;

b) Via de consequência, sempre que a lei exija a assinatura como condição de validade ou de eficácia de um ato ou negócio jurídico, tal condição somente restará atendida, no meio eletrônico, mediante a utilização da assinatura com uso de certificação digital da ICP-Brasil;

c) Tendo em vista o princípio da legalidade estrita, que rege a atividade administrativa, a possibilidade da utilização de meios eletrônicos pela Administração Pública está condicionada à prévia previsão legal que a admita, a qual foi albergada pelo art. 10, *caput e* §1°, da MP n° 2.200-2/2001;

d) Com base no art. 10, *caput e* §1°, da MP n° 2.200-2/2001, e tendo em vista os princípios da legalidade, eficiência e razoabilidade, é admissível a utilização de meios eletrônicos por parte da Administração Pública, inclusive para a prática de atos administrativos aptos a produzir efeitos no âmbito administrativo, nos moldes do art. 22, §1º da Lei n. 9.784/99, desde que mediante a utilização de certificação digital proveniente da ICP-Brasil;

e) O §2º do art. 10 da MP n. 2.200/2001 - que admite a utilização de outros meios de comprovação da autoria e integridade de documentos produzidos em forma eletrônica, inclusive a utilização de certificados digitais não emitidos pela ICP-Brasil, desde que assim aceito pelas partes ou pela pessoa a quem for oposto o documento - aplica-se exclusivamente às **manifestações de vontade realizadas no âmbito privado**, sendo inaplicáveis aos atos do Poder Público, uma vez que estes possuem fé pública, independem de aceitação da parte contrária e tem sua validade condicionada à observância de requisitos formais específicos;

f) Nos termos do Decreto n. 3.996/2001, que permanece válido e em vigor, os serviços de **certificação digital** no âmbito da Administração Pública Federal devem ser providos, exclusiva e obrigatoriamente, no âmbito da ICP-Brasil, sendo vedada, portanto, a criação de infraestruturas de certificação paralelas por parte de seus órgãos e entidades ou a utilização de outras formas de certificação digital para fins de assinatura de atos e documentos públicos;

g) O art. 6º do Decreto n. 8.539/2015 deve ser interpretado em consonância com o regramento legal e principiológico aplicável à Administração Pública, sendo inaplicável aos serviços de certificação digital como um todo, os quais seguem submetidos ao regime estabelecido pelo Decreto n. 3.996/2001;

h) Assim sendo, sempre que exigida ou necessária a utilização de certificação digital por parte da Administração Pública, esta deverá, obrigatoriamente, ser provida no âmbito da ICP-Brasil, não sendo admitido qualquer outro método de certificação digital. Da mesma forma, a formalização de atos administrativos (em sentido amplo), nos quais se exija a assinatura da autoridade competente ou do agente público, na forma do art. 22, §1°, da Lei n° 9.784/99, como forma de exteriorização da vontade administrativa (tais como, contratos e acordos administrativos, atos decisórios de qualquer natureza, atos normativos, pareceres técnicos e jurídicos, atos que venham a conferir ou restringir direitos, e, de maneira geral, os atos descritos no art. 50, da Lei n° 9.784/99), deverão, obrigatoriamente, ser firmados mediante o uso de certificação digital provida no âmbito da ICP-Brasil;

i) Por outro lado, admite-se a utilização de outras formas de "assinatura eletrônica" , inclusive do *login e senha,* no máximo, para fins de autenticação em sistemas (como, por exemplo, para acesso ao Sistema Eletrônico de Informações - SEI), ressalvado que apenas serão considerados "assinados", para fins jurídicos, os documentos eletrônicos nos quais tenha sido aposta a assinatura digital com uso de certificado digital da ICP-Brasil, por ter sido essa a única forma de assinatura eletrônica equiparada à assinatura manuscrita no direito brasileiro (art. 10, §1°, da MP n° 2.200-2/2001).

Brasília, 16 de setembro de 2019.

ALEXANDRE MUNIA MACHADO
Procurador-Chefe

VILSON MARCELO MALCHOW VEDANA
Procurador Federal

---

[1] Nessa linha, o DOC ICP 15, item 4.2, aprovado pelo Comitê Gestor da ICP-Brasil, define assinatura eletrônica como *"o conjunto de dados sob a forma eletrônica, ligados ou logicamente associados a outros dados eletrônicos, utilizado como método de comprovação da autoria"*.

[2] "(...) sob a denominação de assinatura eletrônica inclui-se um sem número de métodos de comprovação de autoria empregados em meio virtual. Assinatura digital, desta feita, consiste em espécie do gênero assinatura eletrônica, e representa um dos meios de associação do indivíduo a uma declaração de vontade veiculada eletronicamente dentre os diversos existentes". (MENKE, Fabiano. *Assinatura eletrônica no direito brasileiro.* São Paulo: RT, 2005. p. 42).

[3] A bem da verdade, a própria adoção do termo "assinatura digital" não é uniforme, verificando-se, no direito comparado, a adoção de outras expressões, tais "assinatura eletrônica avançada" (*advanced electronic signatures)* e "assinatura eletrônica qualificada" *(qualified electronic signatures)*, com definição análoga do que se entende, como "assinatura digital" (*digital signatures)*.

[4] GARCIA, André Pinto. *Curso de Direito da Certificação Digital.* Brasília: Ed. do Autor, 2016. p. 110.

[5] No direito comparado, verifica-se que o uso - e a própria eficácia jurídica - das assinaturas eletrônicas varia conforme a legislação no país. De maneira geral, pode-se dividir o reconhecimento legal das assinaturas eletrônicas no mundo em dois grandes grupos: (a) países que não distinguem assinaturas eletrônicas das assinaturas digitais (Estados Unidos e Austrália); (b) países que distinguem as assinaturas eletrônicas e assinaturas digitais (assinaturas eletrônicas avançadas, qualificadas ou seguras), atribuindo efeitos específicos a estas últimas, ou exigindo-as para assinatura de determinados atos e negócios jurídicos (Canadá, União Europeia, Chile, Rússia, Indonésia, Peru, Singapura, África do Sul, Suíça, Turquia, México, Israel, China, Filipinas - como se percebe, a grande maioria das legislações do mundo). No Brasil, a legislação trata expressamente, apenas, da assinatura digital, e, mesmo assim de maneira bastante tímida. Nada obstante, é possível extrair a admissibilidade jurídica das assinaturas eletrônicas das demais normas civilistas e do art. 10, §2º, da Medida Provisória n° 2.200-2/2001, embora tenha sido atribuído *status* especial apenas às assinaturas eletrônicas no padrão ICP-Brasil, conforme se infere do §1° do mesmo art. 10. Essas questões serão detalhadas adiante, em capítulo específico.

[5] O Parecer Técnico SEI n° 0392647 define funções h*ash* como o *"processo matemático e de engenharia computacional unidirecional que converte uma quantidade de bits, em um ativo eletrônico, para uma saída fixa de bits, em que essa saída é exclusiva para um determinado dado de origem, de modo que qualquer alteração no dado original, obrigatoriamente, resulta em uma saída (valor de hash) alterada"*.

[6] "Somente com o uso da criptografia tornou-se possível 'assinar' arquivos digitais de um modo que seja capaz de

reproduzir as funcionalidades de uma assinatura autógrafa escrita sobre o papel. Assim, por assinatura digital deve-se entender tão somente o resultado de funções criptográficas, consistentes em sequências de operações matemáticas, em que o próprio documento é um dos fatores empregados nos complexos cálculos". (MARCACINI, Augusto Tavares Rosa. *Certificação Digital.* In: LIMA, Cíntia Rosa Pereira de; NUNES, Lydia Neves Bastos Telles (Org.). *Estudos Avançados de Direito Digital.* 1ª ed. Rio de Janeiro: Elsevier, 2014. p. 18.

[7] LEVY, Steven. *Crypto*. Penguin Books: New York, 2002, p. 66/89

[8] MARCACINI, Augusto Tavares Rosa. *Certificação ... Ob. cit.* p. 20.

[9] Certo é que existem outros modelos de chaves públicas, a exemplo do modelo de confiança distribuída, adotado nos EUA, no qual cada Autoridade Certificadora constitui uma cadeia independente. Desse modelo, contudo, advém algumas dificuldades, tal como a necessidade de estabelecer diversas certificações cruzadas (*"bridges")* entre as infraestruturas existentes de modo a viabilizar a interoperabilidade, permitindo que os certificados de uma cadeia se comuniquem com as demais cadeias. Diante de tais dificuldades, a imensa maioria dos países do mundo que adotam o modelo PKI tem se valido de uma cadeia hierárquica de confiança, muitas das quais tendo como Autoridade Certificadora Raiz uma entidade que detenha fé pública, como se dá no Brasil (uma vez ser o ITI uma autarquia federal).

[10] Tecnicamente, a expressão "validade jurídica" não se mostre ideal, haja vista que o uso da certificação digital no padrão ICP-Brasil não tem, evidentemente, a capacidade de garantir a validade jurídica do documento assinado (o qual depende de outros requisitos de validade, conforme o ato ou negócio jurídico a ser entabulado), bem como que o documento não se mostrará inválido, a princípio, pelo simples fato de não ter sido assinado com o uso da certificação digital ICP-Brasil (tendo em vista que, no Brasil, prevalece a liberdade das formas, como será examinado no capítulo seguinte).

[11] ″Art. 13. O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira".

[12] "Art. 7°. Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações".

[13] GARCIA, André Pinto. *Curso ... Ob. cit.* p. 110.

[14] MARCACINI, Augusto Tavares Rosa. *Certificação ... Ob. cit.* p. 25.

[15] "Nesse quadro, é importante colocar a vontade como elemento do negócio jurídico. No exame do plano de existência não se cogita de invalidade ou de ineficácia, mas simplesmente da realidade de existência do negócio. Importa examinar a existência da vontade ou, mais que isso, a existência da declaração da vontade. Temos para nós que, contudo, que a vontade, muito antes de ser apenas um elemento do negócio, é um pressuposto dele, mas um pressuposto que ora interferirá na validade, ora na eficácia do negócio, já que pode 'existir' um negócio jurídico com mera aparência de vontade, isto é, circunstância que a vontade não se manifestou e houve apenas mera 'aparência de vontade'". (VENOSA, Silvio de Salvo. *Direito Civil: Parte Geral.* 4ª ed. São Paulo: Atlas, 2004. p. 413).

[16] MARCACINI critica veementemente o emprego, pela literatura técnica, do termo "assinatura", para definir os meios tecnológicos compreendidos no conceito técnico de "assinatura eletrônica" e "assinatura digital": "Adianto que, ao me parece, esse uso que a informática emprestou ao vocábulo, o da locução "assinatura do arquivo" apresentada acima, contaminou indevidamente o significado jurídico que vem sendo dado à expressão "assinatura digital". A língua, sem dúvida, é dinâmica. Chamem o que quiserem de assinatura! Se se tornar usual, esse novo uso da palavra integrará o nosso vocabulário, e no futuro poderá até ser dicionarizada! Mas não queiram que essa coisa qualquer que passaram a chamar de assinatura seja equivalente à assinatura autógrafa tradicional e possa produzir os mesmos fins jurídicos que dela se espera". (MARCACINI, Augusto Tavares Rocha. *Assinatura digital - aspectos jurídicos - Parte I".* disponível em ,https://cryptoid.com.br/identidade-digital-destaques/aspectos-juridicos-que-e-uma-assinatura-digital/.. Acesso em: 09/09/2019)

[17] CARNELUTTI, Francesco. A prova Civil. Título original; *La prova civile.* Trad. Lisa Pary Scarpa. 2ª Ed. Campinas: Bookseller, 2002. *Apud* Bittar, João Paulo Vinha. Assinatura e contratos digitais: uma breve abordagem sobre as novas questões trazidas pelos avanços da informática no campo do direito contratual, mais especificamente sobre a validade das assinaturas digitais. Artigo publicado em 01/11/2011. *In* Revista Âmbito Jurídico - n° 93 – Ano XIV – Outubro/2011. Disponível em http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=10239&revista_caderno=17.

[18] MARCACINI, Augusto Tavares Rocha. *O documento eletrônico como meio de prova.* Disponível em: http://augustomarcacini.net/index.php/DireitoInformatica/DocumentoEletronico#sdfootnote1sym. Acesso em: 07 de setembro de 2019.

[20] GARCIA, André Pinto. *Curso ... Ob. cit.* p. 105.

[21] MARCACINI, Augusto Tavares Rosa. *Criptografia assimétrica, assinaturas digitais e a falácia da "neutralidade tecnológica"*. Disponível em: <http://augustomarcacini.net/index.php/DireitoInformatica/NeutralidadeTecnologica>. Acesso em: 07 de setembro de 2019.

[22] "O parágrafo único do artigo 221 do Código Civil, por sua vez, estatui que 'a prova do instrumento particular pode suprir-se pelas outras de caráter legal', o que seria suficiente à conclusão quanto à viabilidade do documento eletrônico, sendo perfeitamente possível, em tal perspectiva, 'seu uso para a comprovação da declaração negocial' (THEODORO JÚNIOR, 2008, p. 573), desde que preencha os requisitos de "inalterabilidade do teor", "identificabilidade da autoria" e "tempestividade controlável". (TEPEDINO, Gustavo. *A evolução da prova entre o direito civil e o direito processual civil.* In: Revista Pensar, Fortaleza, v. 22, n. 2,

p. 551-566, maio/ago. 2017).

[23] "Entendemos que provas digitais formam uma nova categoria de provas, isto porque, ao analisarmos os conceitos tradicionais de provas e as particularidades que envolvem esse novo meio de prova, percebemos que o fato de serem produzidas, armazenadas ou transmitidas em meio digital, seja num computador, ou qualquer dispositivos eletrônicos lhes conferem características únicas que demandam, em muitos casos, a atuação de profissionais especializados com a tomada de procedimentos específicos para sua identificação (...)". (BARSOTI, Luciane. *As provas digitais e a relevência nas ciências jurídicas da pós modernidade*. In: CAMARGO, Coriolano Almeida; SANTOS, Cleórbete (Org.). *Direito digital: novas teses jurídicas.* 1ª ed. Rio de Janeiro: Lumen Juris, 2018. p. 183).

[24] MENKE, Fabiano; BERTOL, Viviane. *Uso de HSM para guarda de certificados digitais.* Disponível em: <https://cryptoid.com.br/colunistas/viviane-bertol/uso-de-hsm-por-viviane-bertol-e-fabiano-menke/> Acesso em: 07 de setembro de 2019.

[25] NÚÑEZ, Claudio Felipe Alexandre Magioli. Possibilidade jurídica da contestação da assinatura digital. In: Rev. SJRJ, Rio de Janeiro, v. 20, n. 38, p. 13-38, dez. 2013.

[26] MENKE, Fabiano. *Assinatura ... Ob. cit.* p. 139 e 140.

[27] GARCIA, André Pinto. *Curso ... Ob. cit.* p. 133.

[28] GARCIA, André Pinto. *Curso ... Ob. cit.* p. 111.

[29] MENKE, Fabiano. *Assinatura ... Ob. cit.* p. 145.

[30] GARCIA, André Pinto. *Curso ... Ob. cit.* p. 113.

[31] Difere-se doutrinariamente o "governo eletrônico" da "teleadministração", consistindo esta na "Administração Pública Telemática cuja atividade, dotada de valor jurídico, é exercida por meio de terminais de computadores conectados a uma central de dados, que compõe, por sua vez, uma rede nacional de Administração Pública, com várias centrais de dados" (FILGUEIRAS JÚNIOR, Marcus Vinícius. Ato administrativo eletrônico e teleadministração. Perspectivas de investigação. *In:* Revista de Direito Administrativo n. 237. Rio: Renovar/FGV, 2004, p. 243/264).

[32] FERGUSON, Martin. Estratégias de governo eletrônico: o cenário internacional em desenvolvimento. *In :* EISENBERG, José.; CEPIK, Marco (Org.). *Internet e política: Teoria e Prática da Democracia Eletrônica.* Belo Horizonte: UFMG, 2002. p. 104.

[33] JUSTEN FILHO, Marçal. *Curso de Direito Administrativo.* 8ª Ed. Belo Horizonte: Fórum, 2012. p. 192.

[34] MELLO, Celso Antonio Bandeira de. *Curso de Direito Administrativo.* 28ª Ed. São Paulo: Malheiros, 2011. p. 105.

[35] SANTOLIM, César. *Aspectos jurídicos do governo eletrônico: as tecnologias da informação na Administração Pública.* In: R. Dir. Inform. Telecomun. - RDIT, Belo Horizonte, ano 2, n. 2, p. 85-97, jan./jun. 2007

[36] MEDAUAR, Odete. *Direito administrativo moderno.* 6a ed. São Paulo: Revista dos Tribunais, 2002. p. 166.

[37] MOREIRA NETO, Diogo de Figeuiredo. *Globalização, regionalização, reforma do Estado e da Constituição.* Revista de Direito Administrativo, Rio de Janeiro, v. 211,1998. *Apud* SANTOLIM, César. *Aspectos... Ob. cit.*

[38] FILGUEIRAS JUNIOR, Marcus Vinícius. *Ato administrativo eletrônico e teleadministração. Perspectivas de investigação.* In: Revista de Direito Administrativo. n. 237. Rio de Janeiro: Renovar, jul./set.2004. pp. 243-264.

[39] MENKE, Fabiano. *Assinatura ... Ob. cit.* p. 145.

[40] FURTADO, Lucas Rocha. *Curso de Direito Administrativo.* 3ª ed. rev. ampl. e atual. Belo Horizonte: Fórum, 2012. p. 73.

[41] MELLO, Celso Antonio Bandeira de. *Curso... Ob. cit.* p. 58 e 59.

[42] MELLO, Celso Antonio Bandeira de. *Curso... Ob. cit.* p. 62 e 63.

[43] ROVER, A. J.; RAMOS JÚNIOR, H. S. *O ato administrativo eletrônico sob a ótica do princípio da eficiência.* In: *Anais da II Conferência Sul-Americana de Ciência e Tecnologia Aplicada ao Governo Eletrônico - CONEGOV 2005*. Florianópolis: Ijuris, 2005. pp. 33-40.

[44] GARCIA, André Pinto. *Curso ... Ob. cit.* p. 112.

[45] FILGUEIRAS JUNIOR, Marcus Vinícius. *Ato administrativo eletrônico e teleadministração. Perspectivas de investigação.* In: Revista de Direito Administrativo. n. 237. Rio de Janeiro: Renovar, jul./set.2004. pp. 243-264.

[46] GROTTI, Dinorá Adelaide Musetti. *O Serviço público e a constituição brasileira de 1988*. São Paulo: Malheiros, 2003. p. 298-299.

[47] JUNIOR, Dirley da Cunha. *Curso de Direito Constitucional.* 6ª ed. rev ampl. e atual. São Paulo: JusPodivm, 2012. p. 90.

[48] [49] GARCIA, André Pinto. *Curso ... Ob. cit.* p. 25-27.

[48] TRF4, REOMS 2007.72.00.002903-9, QUARTA TURMA, Relator EDGARD ANTÔNIO LIPPMANN JÚNIOR, D.E. 23/11/2007.

[49] GARCIA, André Pinto. *Curso ... Ob. cit.* p. 117.

[50] MARCACINI, Augusto Tavares Rosa. *Certificação ... Ob. cit.* p. 18.

Documento assinado eletronicamente por ALEXANDRE MUNIA MACHADO, de acordo com os normativos legais aplicáveis. A conferência da autenticidade do documento está disponível com o código 306634314 no endereço eletrônico http://sapiens.agu.gov.br. Informações adicionais: Signatário (a): ALEXANDRE MUNIA MACHADO. Data e Hora: 16-09-2019 17:40. Número de Série: 13513104. Emissor: Autoridade Certificadora SERPRORFBv4.

Documento assinado eletronicamente por VILSON MARCELO MALCHOW VEDANA, de acordo com os normativos legais aplicáveis. A conferência da autenticidade do documento está disponível com o código 306634314 no endereço eletrônico http://sapiens.agu.gov.br. Informações adicionais: Signatário (a): VILSON MARCELO MALCHOW VEDANA. Data e Hora: 16-09-2019 17:42. Número de Série: 17355775. Emissor: Autoridade Certificadora SERPRORFBv5.
