# Poder Judiciário: fragilidade da comunicação entre órgãos jurisdicionais

Alexandre Bueno Cateb*
Ana Amelia Menna Barreto de Castro Ferreira**



---

## 1. Introdução

Recentemente a sociedade brasileira e a comunidade jurídica tomaram conhecimento de ilícito praticado com base na distorção de informação proveniente do Superior Tribunal de Justiça. Tratava-se de fraude com a comunicação de decisão proferida no *habeas corpus* nº. 74.674-MG-2007/0008749-3.

O crime foi descoberto pelo presidente em exercício, Ministro Francisco Peçanha Martins, ao apreciar requerimento de extensão de liminar a outros co-réus que estavam presos por decisão judicial. No pedido formulado no *habeas corpus*, os impetrantes não apenas informavam que a decisão exarada pelo presidente da Corte, Ministro Barros Monteiro, foi reconsiderada e deferida a outros pacientes, como juntaram cópia da decisão, apontando inclusive o número das respectivas folhas.

Foi constatado pelo Min. Peçanha Martins que a única decisão existente nos autos - da lavra do Ministro Barros Monteiro - indeferia a liminar pretendida. Através de contato telefônico mantido com o Tribunal de Justiça de Minas Gerais e com o Juízo da 2ª Vara Criminal da Comarca de Sete Lagoas, apurou-se que, em virtude do recebimento de comunicação via

fax proveniente do STJ - através da qual foi encaminhada a falsa decisão - foram expedidos alvarás de soltura em favor dos pacientes.

O fato ocorrido expõe a fragilidade da comunicação dos atos entre Tribunais, possibilitando a ocorrência de transmissão de decisão falsa fixada no papel timbrado do STJ, constando uma assinatura falsa de Ministro da Corte.

---

## 2. A legislação aplicável

Analisando os dispositivos constantes do Código de Processo Civil, verifica-se que, em relação à forma dos atos decisórios, despachos, decisões, sentenças e acórdãos devem ser redigidos, datados e assinados pelos juízes (art. 164).

Nas disposições gerais relativas à comunicação dos atos, o diploma indica entre os requisitos essenciais da carta de ordem, precatória e rogatória, a existência da assinatura do juiz (art. 202). Em caso de urgência, prevê que estas poderão ser transmitidas por telegrama, radiograma ou telefone (art. 205). Nessa última hipótese, além dos requisitos previstos no art. 202, impõe-se ainda uma declaração da agência expedidora de estar reconhecida a assinatura do juiz (art. 206).

Nas cartas transmitidas por comunicação telefônica (art. 207) seu conteúdo deve ser verificado, na forma do § 1º do mesmo artigo.

O Código de Processo Penal - nos casos em que o paciente estiver preso em lugar que não seja o da sede do tribunal que conceder a ordem - aplica a possibilidade do alvará de soltura ser expedido por via postal ou por telégrafo (art. 660, § 6º). Nesse último caso, a ordem transmitida por telegrama prescinde da necessidade de autenticação da firma do juiz no original levado à agência telegráfica (parágrafo único do art. 289, in fine).

Em processo e julgamento de *habeas corpus* de competência originária do Supremo Tribunal Federal, bem como nos recursos das decisões de última ou única instância, denegatórias de *habeas corpus*, a legislação remete aos mesmos artigos, cabendo ao regimento interno do Tribunal estabelecer as regras complementares (art. 667).

Adjetivamente, o Regimento Interno do Superior Tribunal de Justiça prevê que os atos processuais serão autenticados, conforme o caso, mediante assinatura ou rubrica dos ministros ou dos servidores para tal fim qualificados (art. 84), exigindo-se a assinatura usual nos acórdãos, na correspondência oficial, no fecho da carta de sentença e nas certidões (§ 1º).

A notificação de ordens ou decisões será feita - a critério do Presidente do Tribunal, dos Presidentes das Sessões, da Turma ou do Relator - por servidor credenciado da secretaria, por via postal ou por qualquer outro modo eficaz de telecomunicação, com as cautelas necessárias à autenticação da mensagem e do seu recebimento (art. 87, I e II).

---

## 3. A solução legal para a falha na comunicação

Caso a comunicação dos atos em tela fosse transmitida por meio eletrônico, contaria com a utilização de recursos tecnológicos de segurança, aptos a garantir de forma inquestionável a autenticidade da autoria em atos processuais e aptos a atribuir presunção de validade da autoria do ato praticado.

Fechando o ciclo de atualização legislativa na incorporação dos meios eletrônicos no âmbito do Poder Judiciário, a nova Lei 11.419/06 concedeu validade jurídica à tramitação eletrônica de processos judiciais, a comunicação de atos e transmissão de peças processuais, prevendo que a assinatura de juízes, em todos os graus de jurisdição, pode ser feita eletronicamente (CPC, art. 164, parágrafo único), desde que baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma da lei específica (art. 1º, § 2º, III, a).

### 3.1. Infra-Estrutura de Chaves Públicas Brasileira

A norma legal invocada diz respeito à Medida Provisória 2.200/01, que criou a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil. A referida MP implantou um sistema nacional de certificação digital no país, resultante de um conjunto de técnicas, práticas e procedimentos, com o objetivo de garantir a autenticidade, confidencialidade e integridade das informações contidas em documentos produzidos em forma eletrônica.

A estrutura hierárquica da ICP-Brasil compõe-se de um grupo de autoridades que se submetem às diretrizes estabelecidas pelo Comitê Gestor, em todos os níveis da cadeia de certificação. No topo da estrutura de certificação, figura a Autoridade Certificadora-Raiz - AC-Raiz, exercida pelo Instituto Nacional de Tecnologia da Informação, a quem compete executar as políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.

Em nível imediatamente inferior, as Autoridades Certificadoras - AC - detêm a responsabilidade de expedir, revogar e gerenciar os certificados digitais. São ainda obrigadas a fazer cumprir a Política de Segurança, a Declaração de Práticas de Certificação e a Política de Certificados.

Compete às Autoridades Registradoras - AR, obrigatoriamente vinculadas a uma AC, identificar e cadastrar usuários presencialmente, submetendo a solicitação de certificados à AC à qual se subordinam.

Concede-se o licenciamento para operar como AC ou AR a órgãos e entidades públicas, assim como a pessoas jurídicas de direito privado. As entidades prestadoras de serviço de certificação credenciadas se obrigam ao cumprimento de um conjunto de diretrizes de segurança definidos pela ICP-Br, como instrumentos garantidores de segurança e confiabilidade de todos as operações praticadas pela cadeia de certificação.

### 3.2. Práticas de Certificação

As Autoridades Certificadoras credenciadas pela ICP-Brasil se obrigam a elaborar e divulgar a Política de Segurança, a Declaração de Práticas de Certificação e a Política de Certificados, sujeitando-se a auditoria anual obrigatória.

Tratam-se de documentos que atestam ao público o cumprimento obrigatório das diretrizes emanadas pela ICP-Br no que se refere aos processos e práticas que estabelecem regras para emissão de certificados e exigências de segurança, garantidores da confiabilidade das operações da AC.

### 3.3. Certificação Digital

A assinatura digital disponibilizada pela ICP-Brasil se utiliza de um processo de codificação e decodificação, consistente na aplicação de modelo matemático de algoritmo criptográfico, baseado no conceito de chaves e executado por um programa de computador. Com a inserção da chave criptográfica, o arquivo enviado se torna ilegível, sendo necessário ter conhecimento do algoritmo de decifragem - a chave - para recuperação dos dados originais.

A ICP-Brasil adota o padrão criptográfico assimétrico, cujos algoritmos trabalham com duas chaves geradas simultaneamente - pública e privada - utilizadas, respectivamente, para cifrar e decifrar a informação.

O titular da chave privada disponibiliza sua chave pública para que a informação se torne acessível ao destinatário da mensagem eletrônica. A chave privada é de conhecimento exclusivo do titular da assinatura digital, cabendo-lhe a responsabilidade por mantê-la em sigilo.

Os certificados digitais contendo a assinatura podem ser alocados no próprio equipamento ou em mídia portátil - *smart card* e *token* - que armazenam a chave privada do usuário. As informações contidas nos

certificados digitais são acessíveis através da senha pessoal eleita pelo titular.

O mecanismo concede segurança quanto à autoria e integridade do documento eletrônico, vinculando indissociavelmente a assinatura ao documento. Em caso de tentativa de modificação do documento eletrônico, o certificado digital detectará a violação e não lhe conferirá autenticidade.

O certificado digital, emitido pelo terceiro de confiança credenciado pela ICP-Br, funciona como um documento de identidade eletrônica que armazena os dados pessoais de seu titular, associando essa identificação a uma chave pública.

### 3.4. Validade Jurídica Certificado Qualificado

Como visto, a prestação da atividade de certificação digital pode ser objeto de credenciamento - em caráter voluntário - junto à ICP-Brasil.

Porém, apenas a certificação disponibilizada pela ICP-Br concede a chamada equivalência funcional à assinatura manuscrita, atribuindo uma presunção de veracidade à declaração de vontade por meio digital.

Portanto, as declarações de vontade, expressas em documentos eletrônicos que se utilizam dos certificados qualificados disponibilizados através da ICP-Br, presumem-se verdadeiras em relação aos signatários, gozando da presunção de validade oponível *erga omnes*, nos termos da MP 2.200 (§ 1º do artigo 10).

Apesar de admitido na lei o emprego de outros meios de comprovação de autoria e integridade de documentos em forma eletrônica, os certificados digitais particulares - emitidos por empresas não credenciadas junto à ICP-Br - têm sua eficácia condicionada à admissão pelas partes como válido ou aceito pela pessoa a quem for aposto o documento (§ 2º do art. 10).

Trata-se, nesse caso, de eleição de meio de certificação não corroborado pela legislação brasileira e, por isso, necessário que as partes concordem em atribuir a devida credibilidade e validade ao certificado eletrônico utilizado.

### 3.5. Autoridade Certificadora da Justiça

Após a edição da MP 2200/01 foi criada a Autoridade Certificadora do Sistema Justiça Federal, em janeiro de 2005. Posteriormente, com a adesão do STF, CNJ e Tribunais Superiores, essa autoridade passou a se denominar Autoridade Certificadora da Justiça - AC-JUS.

Primeira autoridade certificadora do mundo criada e mantida pelo Poder Judiciário, é responsável pela implantação da certificação digital do Judiciário em todas as suas esferas, desenvolvendo aplicações específicas para comunicação e troca de documentos, adotando políticas de certificação com validade legal que viabilizam a implantação do processo judicial informatizado.

A estrutura administrativa da AC-Jus compõe-se de um Comitê Gestor - formado por Ministros representantes do Supremo Tribunal Federal, dos Tribunais Superiores e Conselheiros representantes do CNJ e do CJF - e por uma Comissão Técnica que lhe presta assessoria.

Cabe à AC-Jus determinar as regras de certificação e perfis de certificado seguidos pelas ACs-subseqüentes - encarregadas de operacionalizar a emissão de certificados para usuários finais - e fiscalizar a correta execução do processo de certificação.

Sob sua cadeia de certificação, criou-se o certificado denominado Cert-JUS, cuja emissão depende da autorização do órgão e instituição a que se vincula o usuário. Encontra-se disponível em três perfis: Institucional, Equipamento Servidor e Código Seguro.

O certificado "Cert-JUS Institucional" - de uso exclusivo de magistrados, autoridades e servidores públicos - identifica o titular como servidor de determinado órgão ou instituição, contendo seus dados pessoais e informações relativas ao órgão a que se vincula, tais como lotação, cargo e matrícula.

Aplica-se à assinatura de documentos e mensagens eletrônicas, acesso à rede e outras funções, fazendo uso obrigatório do tipo A3. Este tipo de certificado portátil apresenta nível de segurança superior e se armazena em cartão inteligente protegido por senha que permite acesso ao certificado em vários computadores diferentes. Cabe ao titular do certificado a responsabilidade pela segurança do código de acesso à mídia criptográfica - *PIN*.

O certificado "Equipamento Servidor" se destina aos equipamentos dos órgãos que disponibilizem serviços ou informações, aplicando-se o certificado "Código Seguro" para assinatura de código executável que disponibiliza verificadores e programas de peticionamento eletrônico que concedem segurança ao usuário.

O Supremo Tribunal Federal firmou Acordo de Cooperação Técnica com a Caixa Econômica Federal ( nº 06/2006), com a finalidade de estipular formas de ampliação e incremento da prestação de serviços de Certificação Digital da AC-Jus, no âmbito do STF, visando identificar, autenticar,

registrar e emitir certificados do tipo A1, A2 e/ou A3 para magistrados, servidores, prestadores de serviço e/ou estagiários da Justiça.

### 3.6. Responsabilidade pela Transmissão

Deve-se ressaltar a necessidade do Poder Judiciário implementar um protocolo de procedimentos para a transmissão por meio eletrônico, indicando-se os servidores responsáveis pelo envio e destinação do ato, com a finalidade de se assegurar que este seja realmente encaminhado ao órgão competente.

Nesse sentido, o Poder Executivo Federal estabeleceu os procedimentos para transmissão em meio eletrônico, através do Decreto 3.714/2001. A referida norma instituiu uma padronização de procedimentos, determinando a criação de uma caixa postal especifica em cada Ministério para recepção e remessa eletrônica de atos normativos, dotada de sistema de segurança apto a impedir a alteração dos documentos transmitidos. O decreto também cuida, especificamente, da indicação e credenciamento dos servidores encarregados pelo recebimento e destinação dos atos, que devem ser objeto de confirmação mediante aviso de recebimento eletrônico.

---

## 4. Conclusões

Em sentido inverso ao que se poderia imaginar, a fraude ocorrida na comunicação de atos processuais por meio físico, não se materializaria no meio eletrônico.

Isto porque o Magistrado - de posse de seu certificado digital - assina com sua chave privada o documento eletrônico contendo o despacho, gerando um código de autenticidade único a este documento.

A comunicação eletrônica do ato processual seria encaminhada à instância inferior através do sistema tecnológico do Tribunal de origem, gerando um recibo eletrônico de protocolo.

Ao receber o arquivo assinado digitalmente, conferindo a autenticidade da autoria do ato transmitido, o Juízo de primeiro grau daria cumprimento à ordem superior.

Sem dúvida, portanto, que a aplicação de recursos tecnológicos de segurança da informação, superando os questionamentos advindos pela imaterialidade característica do ambiente digital, proporcionará maior segurança jurídica ao procedimento e comunicação judiciais eletrônicos, em comparação com aquela vivenciada nos autos em papel.

**NOTAS:**

[01] Disponível em: <http://www.stj.gov.br/portal_stj/publicacao/download.wsp?tmp.arquivo=84> Acesso em 07 de março de 2007

[2] Disponível em <http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf> Acesso em 07 de março de 2007

[3] Disponível em <www.acjus.gov.br> Acesso em 20.05.2007

[4] Disponível em <http://www.stf.gov.br/processos/autenticacao/> - Necessário digitar o código de documento 01

* advogado, doutor em Direito Comercial, professor da Faculdade de Direito Milton Campos, membro do Instituto dos Advogados de Minas Gerais.
** advogada do Escritório José de Castro Ferreira, Décio Freire & Associados, Rio de Janeiro (RJ).

Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=10424