

O processo judicial eletrônico e sua segurança

Luiz Carlos Santana Delazzari^{*}

Sumário: 1 Introdução. 2 A informatização do processo judicial. 3 A segurança do processo judicial eletrônico. 3.1 Assinatura digital. 3.2 A criptografia. 3.2.1 Criptografia simétrica ou convencional. 3.2.2 Criptografia assimétrica ou pública. 3.3 Certificação digital. 4 Conclusão. 5. Referências.

Resumo

Cada vez mais real e próximo, o processo judicial eletrônico desperta curiosidades e muitas dúvidas sobre a sua viabilidade e segurança. Por isso, o objetivo do presente estudo é discorrer sobre os instrumentos que podem garantir um mínimo de segurança às informações digitais, como criptografia e assinatura digital. Estudar os mecanismos aptos a garantir a confiabilidade do processo eletrônico revela-se oportuno, principalmente porque o Conselho Nacional de Justiça e os Tribunais Superiores têm incentivado a completa substituição do processo tradicional (em papel) pelo eletrônico (ou digital) em todo o País. Afinal, a via eletrônica tem se apresentado como uma das principais formas capazes de reduzir o tempo gasto com a tramitação processual, fazendo prevalecer o princípio constitucional da duração razoável do processo.

Palavras-chave: Processo. Eletrônico. Segurança.

1 Introdução

Conforme anunciado pelo Ministro Cezar Peluso, Presidente do Conselho Nacional de Justiça, o processo judicial eletrônico já está disponível para os tribunais de todo o país¹. Trata-se de um sistema tecnológico de automação do Poder Judiciário, que eliminará algumas tarefas processuais puramente burocráticas e mecânicas, permitindo, assim, a tramitação eletrônica dos processos judiciais nos tribunais brasileiros.

Ou seja: a tecnologia está alcançando também o Poder Judiciário, de forma surpreendente, trazendo a esperança de que o meio eletrônico pode fornecer instrumentos para agilizar a tramitação dos inúmeros processos que existem em todo o País.

Nesse contexto e atenta às ferramentas disponíveis, a Justiça brasileira tem se rendido às novas tecnologias para buscar formas mais eficientes de desenvolvimento do processo, com o fim de proporcionar maior celeridade à solução dos conflitos, em obediência ao art. 5º, inciso LXXVIII, da Constituição Federal: “a todos, no âmbito judicial e administrativo, são assegurados a razoável duração do processo e os meios que garantam a celeridade de sua tramitação”.

É nesse enfoque que se propõe a utilização do processo eletrônico, atualmente levantado como instrumento capaz de reduzir o tempo gasto com a tramitação processual, mormente porque possibilita a substituição do meio físico (papel) por outro integralmente digital, a partir do uso de computadores, *scanners* e internet.

No entanto, questões atinentes à segurança da informação digital ainda são um desafio da atualidade, tendo em vista o risco de fraudes e de manipulação de dados. Por essa razão, merecem ser estudadas, principalmente porque se trata de informação processual disponibilizada em meio eletrônico.

Diante desse panorama é que se desenvolve o presente trabalho, para abordar o processo eletrônico e a segurança de sua aplicação, a fim de demonstrar até que ponto é possível confiar na tramitação processual integralmente informatizada.

2 A informatização do processo judicial

Destacado como um meio teoricamente eficaz para garantir a celeridade da tramitação processual, esperança de um processo viável, célere e econômico (ALMEIDA FILHO, 2008), o processo eletrônico ganhou destaque a partir na Lei nº 11.419, de 19 de dezembro de 2006, em vigor no País desde 20 de março de 2007, a qual dispõe sobre a informatização do processo judicial.

^{*} Assessor de Juiz na 1ª Vara Cível da Comarca de Ponte Nova-MG.

¹ Notícia acessada no sítio do Conselho Nacional de Justiça. Disponível em: <www.cnj.jus.br/noticias/cnj/14801>. Acesso em: 24 jun. 2011.

Desde então, já se passaram mais de quatro anos e muitas indagações ainda persistem a respeito da viabilidade e, principalmente, da segurança do processo eletrônico. Discussões se travam sobre a perda das informações judiciais e a invasão do sistema de dados por pessoas estranhas ao processo, o que tornaria o Poder Judiciário altamente vulnerável. Ademais, algumas pessoas ainda não têm afinidade com o computador, muito menos com a internet - rede mundial de computadores, o que aumenta a resistência ao uso e aplicação da via eletrônica.

Contudo, o que tem sido considerado para incentivar a aplicação do processo eletrônico é que, atualmente, vive-se no século da Revolução Digital, onde o homem interage com tudo e se conecta com todos os pontos do planeta a partir do uso de computadores e da internet (ALMEIDA FILHO, 2008).

Partindo daí, a informatização do processo tem a pretensão de superar velhas práticas que dificultam a tramitação processual, como numeração e rubrica de autos, cargas aos advogados, autuação com cartolina, carimbos de juntadas, de certidões e de termos, o que tem gerado um amontoado de papéis em torno do processo, pouco ou quase nada contribuindo para a efetiva prestação jurisdicional. Isso sem falar na falta de infraestrutura adequada, pois o número de servidores e magistrados tem-se mostrado, a cada dia mais, insuficiente para atender às demandas judiciais.

Sob esse quadro, o Conselheiro Walter Nunes, do Conselho Nacional de Justiça, destacou que 70% (setenta por cento) do tempo da tramitação dos processos é gasto com atos cartorários, como autuações e juntadas, comunicações processuais, numerações e certificações. Segundo ele, “o problema crônico do Judiciário é a burocracia” e “o processo eletrônico é a grande revolução do modelo de prestação jurisdicional e resolve todos esses problemas relacionados à burocracia”².

Dessa forma, o que essa nova temática propõe é uma quebra de paradigma, para admitir a completa transição do processo em papel para o meio digital.

Entretanto, a informatização do processo ainda enfrenta dúvidas quanto à segurança das informações, o que dificulta a aceitação de um processo judicial que tramite exclusivamente em meio eletrônico.

Diante disso, revela-se importante estudar os instrumentos que se habilitam a garantir a segurança e a confiabilidade das informações processuais eletrônicas.

3 A segurança do processo judicial eletrônico

Muito maior que a resistência de muitas pessoas ao uso das novas tecnologias no Poder Judiciário, a preocupação com a segurança do processo eletrônico é a que mais tem dificultado uma confiança plena nessa nova ferramenta.

E não é sem razão, principalmente porque as informações judiciais não podem ficar vulneráveis a fraudes, manipulações e alterações ou ataques de *hackers*³, o que acarretaria obstáculo ao acesso à Justiça e verdadeira insegurança jurídica.

Enfrentar esse tema deve ser um desafio constante, uma vez que as ameaças dos *hackers* e dos vírus podem tornar um sistema eletrônico altamente vulnerável. Ainda mais quando se trata de processo: o acesso não autorizado pode apagar despachos, sentenças, ou mesmo alterá-los, implicando sérios prejuízos às partes; as fraudes podem permitir que liminares sejam forjadas; pessoas podem se passar pelas partes no processo, provocando uma verdadeira confusão.

Diante disso, o Juiz Federal Edilberto Barbosa Clementino (2009, p. 95) pondera que, da mesma forma como ocorre com o processo tradicional, o processo digital deve possibilitar a mesma certeza quanto à autenticidade e à integridade dos documentos eletronicamente produzidos, bem como garantir a sua proteção contra o acesso indiscriminado.

Certamente, em se tratando de processo digital, todos os documentos que o integram passam a se denominar documento eletrônico. E a validade e a confiabilidade desses documentos, no que se refere à autenticidade e à integridade, é que poderão garantir a segurança de todo o processo eletrônico.

J.E.Carreira Alvim e Silvério Nery Cabral Júnior (2008, p. 43), ao citarem a obra de Augusto Tavares Rosa Marcacini, descrevem que o documento eletrônico é uma sequência de *bits*, que, traduzida por meio de um programa de computador, representa ou comprova um fato. Assim como os

² Disponível no sítio do Conselho Nacional de Justiça. Disponível em: <http://www.cnj.jus.br/index.php?option=com_content&view=article&id=10506>. Acesso em: 6 dez. 2010.

³ *Hacker* - indivíduo que tenta acessar computadores ou sistemas, sem autorização, de forma ilegal e normalmente prejudicial (ALMEIDA FILHO, 2008).

documentos físicos, o eletrônico não se resume em escritos: pode ser um desenho, uma foto digital, sons, vídeos, enfim, tudo o que puder representar um fato e que esteja armazenado em arquivo digital. Sustentam que as peculiaridades técnico-informáticas do documento eletrônico é que o diferenciam dos documentos tradicionais.

A seu modo, o advogado Mário Paiva (2007, p. 31), Assessor da Organização Mundial de Direito e Informática (OMDI), suscita os itens indispensáveis à segurança dos documentos eletrônicos: a) autenticidade: a correspondência entre o autor aparente e o autor real comprovada pela assinatura digital; b) integridade: os documentos eletrônicos não podem ser objeto de alterações que lhes modifiquem o conteúdo; c) confidencialidade: o acesso aos documentos eletrônicos tem de ser controlado com o uso de técnicas de criptografia.

Ainda no que concerne ao documento eletrônico, o autor Augusto Tavares Rosa Marcacini (2002) defende o “princípio da equivalência instrumental ao papel”. O mesmo autor pondera que o principal obstáculo do processo eletrônico se resume à questão da segurança do meio digital em relação ao papel. Conclui que não existe, em nenhum dos dois, segurança em termos absolutos. Assim, propõe que o meio eletrônico pode exercer as mesmas funções do papel, e de modo mais satisfatório, não havendo como rejeitar, portanto, a eficácia do documento eletrônico.

De fato, o cotidiano demonstra que a dúvida quanto à segurança das informações não é privilégio apenas do processo eletrônico, uma vez que o processo tradicional também apresenta algumas deficiências. Como se sabe, o papel é passível de várias formas de destruição: queima, rasgos, dobras, deformação pelo decurso do tempo, rasuras e falsificações. Além do mais, um documento de papel pode sumir, trazendo sérios prejuízos às partes e ao próprio Poder Judiciário.

Talvez, poder-se-ia lembrar dos autos suplementares (art. 159 do Código de Processo Civil⁴), os quais garantiriam, hipoteticamente, a segurança do processo em papel, pois os autos principais seriam integralmente reproduzidos no decorrer de sua tramitação, com cópias fidedignas. Porém, sabe-se que a sua formação é prática de um passado distante, sendo impossível a sua aplicação nos dias atuais, seja por falta de espaço físico, seja por falta de tempo, seja por falta de mão de obra. Não se pode olvidar que, se os autos principais são demorados, são muitos, imagine-se como seria, na prática, a formação de autos suplementares - um verdadeiro caos, pode-se afirmar.

Ademais, não é demais lembrar que uma cópia de segurança do processo eletrônico é muito mais fácil, basta um *backup*.

Prosseguindo, consoante já se afirmou, a segurança do processo digital depende da validade jurídica e da confiabilidade dos documentos eletrônicos. E, mesmo que não haja meio absolutamente seguro, a assinatura digital, a criptografia e a certificação digital são instrumentos capazes de assegurar a integridade e a autenticidade da informação eletrônica.

3.1 A assinatura digital

O inciso III do § 2º do art. 1º da Lei 11.419/2006 disciplina duas formas de assinatura eletrônica: a) a digital, baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma da lei específica; e b) cadastro do usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos.

No entanto, a forma mais segura de garantir a confidencialidade das informações do processo eletrônico é a assinatura digital obtida através da criptografia assimétrica ou de chave pública, o que será explicado adiante.

Expressão relacionada à informática, ela é bem definida pelo autor William Stallings (2008, p. 272):

Uma assinatura digital é um mecanismo de autenticação que permite ao criador de uma mensagem anexar um código que atue como assinatura. A assinatura é formada tomando o *hash* da mensagem e criptografando-a com a chave privada do criador. A assinatura garante a origem e a integridade da mensagem.

Segundo destaca esse autor, a solução mais adequada para situações onde não existe confiança mútua entre emissor e receptor da mensagem é a assinatura digital, que é semelhante à

⁴ “Art. 159. Salvo no Distrito Federal e nas Capitais dos Estados, todas as petições e documentos que instruírem o processo, não constantes de registro público, serão sempre acompanhados de cópia, datada e assinada por quem as oferecer.

§ 1º Depois de conferir a cópia, o escrivão ou chefe de secretaria irá formando autos suplementares, dos quais constará a reprodução de todos os atos e termos do processo original.

§ 2º Os autos suplementares só sairão de cartório para conclusão ao juiz, na falta dos autos originais”.

assinatura manuscrita, com esta não se confundindo. Ela precisa ter as seguintes características: a) deve verificar o autor, a data e hora da assinatura; b) deve autenticar o conteúdo no momento da assinatura; e c) deve ser verificável por terceiros, para resolver disputas. Assim, a função de assinatura digital inclui a função de autenticação.

A partir dessas propriedades, William Stallings formulou os seguintes requisitos para uma assinatura digital: a) ela precisa ter um padrão de *bits* que dependa da mensagem que será assinada; b) precisa usar alguma informação exclusiva do emissor, para impedir tanto a falsificação quanto a retratação; c) deve ser relativamente fácil produzi-la; d) deve ser relativamente fácil reconhecê-la e verificá-la; e) deve ser computacionalmente inviável falsificá-la, seja construindo uma nova mensagem para uma assinatura digital existente, seja construindo uma assinatura digital fraudulenta para determinada mensagem; e f) deve ser prático armazenar uma cópia da assinatura digital.

Para Henrique Nelson Calandra (2009, p. 35):

[...] a assinatura digital conferirá aos documentos o mesmo valor jurídico daqueles em papel, assinados de próprio punho. Esse sistema tem como pilares a autenticidade, a integridade e a confiabilidade, minimizando os riscos em torno da segurança.

Almeida Filho (2008, p. 137) cita em sua obra a definição do Instituto Nacional de Tecnologia da Informação:

A assinatura digital é uma modalidade de assinatura eletrônica, resultado de uma operação matemática que utiliza algoritmos de criptografia assimétrica e permite aferir, com segurança, a origem e a integridade do documento. A assinatura digital fica de tal modo vinculada ao documento eletrônico 'subscrito' que, ante a menor alteração neste, a assinatura se torna inválida. A técnica permite não só verificar a autoria do documento, como estabelece também uma 'imutabilidade lógica' de seu conteúdo, pois qualquer alteração do documento, como, por exemplo, a inserção de mais um espaço entre duas palavras, invalida a assinatura.

A assinatura digital, portanto, é diferente da assinatura manuscrita e da assinatura digitalizada. Esta é obtida pela digitalização de um documento assinado a mão, através de um *scanner* ou aparelho similar, enquanto a assinatura manuscrita é aquela que se apõe de próprio punho em algum documento, vinculando ao mesmo a autoria e a autenticação.

Como a assinatura digital é obtida através da criptografia assimétrica, o estudo desta é essencial para o desenvolvimento deste trabalho.

3.2 A criptografia

Consta do *Dicionário Jurídico Acquaviva* (2006, p. 262) que criptografia é expressão de origem grega (*kriptos* - escondido e *grápho* - grafia), significando escrita oculta, indecifrável, conhecida por poucos, para preservar informações. É uma forma de tornar obscura, incompreensível uma mensagem, com um determinado código, por exemplo. Essa mensagem só será compreensível se o destinatário conhecer a forma de decifrá-la.

Conforme explicado, a assinatura digital é obtida através da criptografia, podendo esta ser denominada como um elemento fundamental daquela, que permite a segurança e a validade dos documentos eletrônicos.

Edilberto Barbosa Clementino (2009, p. 98) explica:

Na era dos Computadores, Criptografia e Intimidade estão ligadas de forma indissociável. Criptografia é um conjunto de técnicas que permite tornar incompreensível uma mensagem ou informação, com observância de normas especiais consignadas numa cifra ou num código. Para deslindar o seu conteúdo, o interessado necessita da chave ou segredo. Essa chave pode ser obtida por ato de vontade daquele que encriptou a mensagem ou informação (confidenciando ao interessado o código de acesso) ou pela utilização de técnicas para descobrir a forma de encriptação utilizada e respectivo código.

Segundo o referido autor, a validade jurídica dos documentos eletrônicos depende da autenticidade, integridade e proteção contra o acesso não autorizado, características diretamente relacionadas à criptografia.

Para William Stallings (2008, p. 15), a criptografia é a ferramenta automatizada mais importante para a segurança das informações de um computador na rede. Ele destaca em sua obra que o crescente uso do computador e dos sistemas de comunicação aumentou o risco de roubo de informações particulares. Por isso, a criptografia tornou-se um dos principais métodos de proteção das informações eletrônicas.

A criptografia divide-se em duas espécies: a convencional, ou simétrica, e a criptografia por chave pública, ou assimétrica. Esta última é a que mais interessa ao presente estudo, pois é a modalidade mais segura e foi a adotada pela Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil (Medida Provisória 2.200-2, de 24 de agosto de 2001). De qualquer modo, ambas serão estudadas.

3.2.1 Criptografia simétrica ou convencional

Nessa espécie, o emissor e o receptor da mensagem cifrada (codificada, oculta) usam a mesma chave (mesmo código) para decifrar a informação. A criptografia simétrica transforma o texto claro em texto cifrado, usando uma chave secreta e um algoritmo de criptografia. Usando dessa mesma chave, o receptor da mensagem decifra o texto - recupera o texto claro a partir do texto codificado (STALLINGS, 2008, p. 17).

O risco da criptografia simétrica é que um mesmo código (a mesma chave) é compartilhado entre emissor e destinatário da mensagem, o que torna a informação vulnerável, pois qualquer pessoa, de posse dessa chave, consegue decodificar a mensagem, podendo alterá-la ou mesmo deletá-la.

3.2.2. Criptografia assimétrica ou pública

A assinatura digital é obtida através da criptografia assimétrica, que cria um vínculo entre a assinatura e o corpo do documento. Nesse modelo, a cifragem (codificação) e a decifragem (ato de tornar inteligível o texto obscuro) são realizadas usando diferentes chaves - uma pública e outra privada.

A criptografia assimétrica transforma o texto claro em texto cifrado usando uma das duas chaves e um algoritmo de criptografia. A partir do uso da outra chave associada e um algoritmo de decriptografia, o texto claro é recuperado. Ela é a forma mais usada para assegurar a confidencialidade e autenticação (STALLINGS, 2008, p. 181).

Conforme descrito por Edilberto Barbosa Clementino (2009, p. 105), a criptografia assimétrica assim funciona:

O interessado em comunicar-se dispõe de duas chaves. Uma, é de apenas seu conhecimento, jamais necessitando revelá-la para quem quer que seja. Uma outra, de conteúdo disponível, podendo até constar de uma espécie de catálogo público. Quem quiser mandar uma mensagem sigilosa para alguém, bastaria buscar a Chave Pública dessa pessoa em um catálogo público. Dessa forma, encriptaria a mensagem que somente poderia ser lida pelo destinatário, o único a conhecer a Chave Privada apta para descriptar a mensagem sigilosa.

O autor Willian Stallings (2008, p. 183) exemplifica, citando quatro etapas essenciais:

1. Cada usuário gera um par de chaves a ser usado para a criptografia e decriptografia das mensagens; 2. Cada usuário coloca uma das chaves em um registro público ou outro arquivo acessível. Essa é a chave pública. A outra chave permanece privada. [...] Cada usuário mantém um conjunto de chaves públicas obtidas de outros usuários; 3. Se Bob deseja enviar uma mensagem confidencial para Alice, Bob criptografa a mensagem usando a chave pública de Alice; 4. Quando Alice recebe a mensagem, ela a decriptografa usando sua chave privada. Nenhum outro destinatário pode decriptar a mensagem, pois somente Alice conhece a sua chave privada.

[...]

Com essa técnica, todos os participantes têm acesso às chaves públicas, as chaves privadas são geradas localmente por cada participante e, portanto, nunca precisam ser distribuídas. Desde que a chave privada de um usuário permaneça protegida e secreta, a comunicação que chega está protegida. A qualquer momento, um sistema pode alterar sua chave privada e publicar a chave pública correspondente para substituir sua antiga chave pública.

Desse modo, a criptografia assimétrica apresenta-se bem mais segura do que a criptografia convencional (simétrica), pois trabalha com chaves diferentes para a cifragem e decifragem da mensagem. Entretanto, não se pode afirmar que seja absolutamente segura, pois o seu sucesso em garantir a integridade, autenticidade e confidencialidade da mensagem depende da guarda sigilosa da chave privada, para evitar que outras pessoas se passem pela detentora dessa chave, praticando atos e negócios jurídicos em seu nome.

De forma expressa, o Brasil se valeu da criptografia assimétrica para garantir o sigilo das comunicações eletrônicas com a adoção da Medida Provisória 2.200-2, de 24 de agosto de 2001.

Essa modalidade, portanto, apresenta-se como método indispensável para imprimir maior confiabilidade ao processo eletrônico, muito embora seja pertinente salientar que dificilmente será alcançada a certeza inequívoca acerca dessa confiança, tanto no processo tradicional (físico ou de papel) quanto no eletrônico.

Mas, enfim, onde são adquiridas as assinaturas digitais e desenvolvidas as chaves pública e privada da criptografia? É o que se verá a seguir.

3.3 Certificação digital

Após tratar da assinatura digital e daquilo que lhe dá segurança, a criptografia assimétrica, é necessário saber acerca da produção dessa espécie de assinatura eletrônica. Para tanto, existe a certificação digital, a tecnologia responsável pela segurança das informações na internet.

Sandro D'amato Nogueira (2009, p.39) traz o conceito de Certificação Digital:

É a atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora.

Pelo visto, a certificação digital é que proporciona a segurança das inúmeras transações eletrônicas que ocorrem no dia a dia, identificando as pessoas através do certificado digital e vinculando os códigos gerados pela criptografia àquele que vai utilizar esse documento na rede mundial de computadores.

Conforme o sítio da autoridade certificadora Serasa Experian Certificados Digitais⁵, “o certificado digital é um documento eletrônico que possibilita comprovar a identidade de uma pessoa, uma empresa ou um *site*, para assegurar as transações *on-line* e a troca eletrônica de documentos, mensagens e dados, com presunção de validade jurídica”.

Na lição de Sandro D'amato Nogueira (2009, p. 43):

O certificado digital é um arquivo eletrônico que identifica uma pessoa física ou jurídica, e funciona como um documento de identidade digital. Seu uso vem trazer maior segurança às transações eletrônicas, garantindo a essas transações a autenticidade, a integridade e o não repúdio. Essas três características são conferidas aos documentos assinados com um certificado digital.

Dessas mencionadas características, o mesmo autor define que o não repúdio “garante que o autor não possa contestar sua validade negando a autoria, após a assinatura”.

A respeito da autoridade certificadora, os autores J.E. Carreira Alvim e Silvério Nery Cabral Júnior (2008, p. 23) ensinam:

[...] A autoridade certificadora é um terceiro alheio ao conteúdo do documento eletrônico, responsável pela autenticidade das chaves públicas utilizadas na criptografia, sendo o seu papel o de criar ou possibilitar a criação de um par de chaves criptográficas para o usuário, além de atestar a real identidade das partes através de informações adicionais, utilizando-se dos métodos convencionais (identidade, CPF, nome ou razão social etc.). Além disso, cabe também a essa autoridade emitir um certificado digital, contendo todas as informações que assegurem a transação eletrônica, inclusive as que vinculem a assinatura e sua respectiva chave a determinado indivíduo, proprietário das chaves.

⁵ Disponível em: <<http://loja.certificadodigital.com.br/Serasa/O-que-e-um-certificado-Digital/D2>>. Acesso em: 24 jun. 2011.

Para Nogueira (2009, p. 39), autoridade certificadora é uma entidade, pública ou privada, que estabelece previamente a identidade digital do portador do certificado digital. Destaca que, para emissão de certificados legalmente reconhecidos, é necessária autorização e registro da Autoridade Certificadora Raiz, o Instituto Nacional de Tecnologia da Informação, responsável por credenciar as demais autoridades certificadoras e garantir o cumprimento de todas as exigências necessárias quanto à segurança da informação.

A certificação digital, portanto, é indispensável para assegurar a integridade, autenticidade e confidencialidade das informações disponíveis na internet, sendo um instrumento de fundamental importância para o processo eletrônico. E, nos termos da Medida Provisória 2.200-2/2001, o sistema oficial de certificação digital no Brasil funciona a partir da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

Não bastasse tudo isso, é possível minimizar os riscos de invasão ou manipulação dos dados digitais do processo eletrônico a partir de políticas de segurança, tais como:

a) *backup* diário - cópia de todo o processo eletrônico. É um método simples, utilizado em todos os sistemas informáticos. Seria, como já destacado, uma espécie de autos suplementares eletrônicos;

b) adoção de programas antivírus sempre atualizados, medida também simples e bastante utilizada, até mesmo em computadores domésticos. O vírus talvez seja o principal incômodo desde o surgimento da internet. Propaga-se através de e-mails e pode apagar arquivos, bem como alterar e roubar informações sigilosas;

c) conscientização e treinamento dos usuários, principais personagens do processo eletrônico; e

d) capacitação da equipe técnica, a fim de que estejam sempre preparados para o controle permanente das informações e a adoção de medidas suficientes para evitar a invasão ao banco de dados do Poder Judiciário.

Em termos de capacitação técnica, essa talvez seja a principal medida a ser tomada quando se está diante da tramitação processual eletrônica. Afinal, a equipe técnica tem de estar preparada para prevenir invasões, coibi-las e identificá-las.

É preciso ter em mente, ademais, que a invasão de um sistema de dados é possível, mas ilude-se quem acha que está escondido atrás de um computador, pois todos os computadores são identificados (número de IP - *Internet Protocol*), ainda mais quando se está interligado pela internet. A fraude ou invasão de um *hacker*, por exemplo, pode ser investigada até se encontrar o computador de onde saiu a ameaça, o programa danoso. Por isso, a pessoa que usa a internet para invadir sistemas ou danificá-los pode ser responsabilizada, tanto na área civil quanto penal.

4 Conclusão

O estudo desenvolvido revela uma mudança de paradigma que já é realidade no Poder Judiciário: a transição do processo em papel para o processo judicial eletrônico, meio moderno e eficiente para alcançar a tão sonhada duração razoável do processo, garantia constitucional (art. 5º, LXXVIII). E a sua implementação em todos os tribunais é questão de pouco tempo, principalmente quando se têm incentivos do Conselho Nacional de Justiça e dos Tribunais Superiores.

No que se refere à segurança da informação em meio digital, demonstrou-se que não há meio absolutamente seguro (nem o papel, nem o eletrônico). Partindo desse ponto, destacou-se a assinatura digital, obtida a partir da criptografia assimétrica e da certificação digital; e a adoção de políticas envolvendo *backups*, programas “antivírus” e capacitação técnica podem contribuir de modo eficiente para a diminuição dos riscos de fraudes, tornando confiável o processo judicial eletrônico.

5 Referências

ACQUAVIVA, Marcus Cláudio. *Dicionário Jurídico Brasileiro Acquaviva*. 13. ed. atual., rev. e ampl. São Paulo: Editora Jurídica Brasileira, 2006, p. 262.

ALMEIDA FILHO, José Carlos de Araújo. *Processo eletrônico e teoria geral do processo eletrônico: a informatização judicial no Brasil*. Rio de Janeiro: Forense, 2008.

ALVIM, J. E. Carreira; CABRAL JÚNIOR, Silvério Nery. *Processo judicial eletrônico (Comentários à Lei 11.419/2006)*. Curitiba: Juruá, 2008.

BRASIL, Constituição (1988). *Constituição Federal da República Federativa do Brasil*, 1988. Brasília, DF: Senado Federal. Atualizada até a emenda constitucional n. 53, de 19 de dezembro de 2006. *Vade Mecum*. Obra coletiva de autoria da Editora Saraiva com a colaboração de Antônio Luiz de Toledo Pinto, Márcia Cristina Vaz dos Santos Windt e Livia Céspedes. 3. ed. São Paulo: Saraiva, 2007.

BRASIL. *Código de Processo Civil*. Lei 5.869, de 11 de janeiro de 1973. *Vade Mecum*. Obra coletiva de autoria da Editora Saraiva com a colaboração de Antônio Luiz de Toledo Pinto, Márcia Cristina Vaz dos Santos Windt e Livia Céspedes. 3. ed. São Paulo: Saraiva, 2007.

BRASIL. *Lei nº 11.419*, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 - *Código de Processo Civil*; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11419.htm>. Acesso em: 24 jun. 2011.

BRASIL. *Medida Provisória 2.200-2*, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm>. Acesso em: 24 jun. 2011.

CALANDRA, Henrique Nelson. O Judiciário e a transição para a era digital. *Revista Jurídica Consulex*, ano XIII, n. 289, de 31 de janeiro de 2009, p. 35.

CLEMENTINO, Edilberto Barbosa. *Processo judicial eletrônico*. Curitiba: Juruá, 2009.

MARCACINI, Augusto Tavares Rosa. Intimações judiciais por via eletrônica: riscos e alternativas. *Jus Navigandi*, Teresina, ano 7, n. 59, 1º out. 2002. Disponível em: <<http://jus.uol.com.br/revista/texto/3229>>. Acesso em: 24 jun. 2011.

NOGUEIRA, Sandro D'amato. *Manual de direito eletrônico*. Belo Horizonte. Leme: BH Editora e Distribuidora, 2009.

PAIVA, Mário. Informática: o futuro da justiça. *Revista Jurídica Consulex*, ano XI, n. 244, p. 28-33, 15 mar. 2007.

REINALDO FILHO, Demócrito. A garantia de identificação das partes nos sistemas para transmissão de peças processuais em meio eletrônico: o modelo da Lei 11.419/2006. *Revista Jurídica Consulex*, ano XI, n. 246, p. 58-63, 15 abr. 2007.

STALLINGS, William. *Criptografia e segurança de redes. Princípios e práticas*. Tradução de Daniel Vieira. Revisão técnica de Graça Bressan, Ákio Barbosa e Marcelo Succi. 4. ed. São Paulo: Pearson Prentice Hall, 2008.