UNIVERSIDADE SALVADOR
DEPARTAMENTO DE CIÊNCIAS SOCIAIS E APLICADAS
PÓS GRADUAÇÃO EM DIREITO PROCESSUAL CIVIL

FABIANI OLIVEIRA BORGES DA SILVA

A IMPUGNAÇÃO DA PROVA DOCUMENTAL NO PROCESSO ELETRÔNICO.

Salvador

2011

FABIANI OLIVEIRA BORGES DA SILVA

A IMPUGNAÇÃO DA PROVA DOCUMENTAL NO PROCESSO ELETRÔNICO.

Monografia apresentada ao Programa de Pós Graduação da Universidade Salvador, como requisito para obtenção do grau de especialista em Direito Processual Civil.

Salvador

2011

FICHA CATALOGRÁFICA

Silva, Fabiani Oliveira Borges da
A impugnação da prova documental no processo eletrônico / Fabiani Oliveira Borges da Silva. - 2011.
176f.

Monografia (Pós Graduação) – Universidade Salvador – UNIFACS – Curso de Direito.

1. Processo eletrônico. 2. Prova (Direito). 3. Direito Processual Civil - Impugnação. I.Universidade Salvador – UNIFACS. II. Título.

CDD:

TERMO DE APROVAÇÃO

FABIANI OLIVEIRA BORGES DA SILVA

A IMPUGNAÇÃO DA PROVA DOCUMENTAL NO PROCESSO ELETRÔNICO.

Monografia aprovada como requisito para obtenção do grau de especialista em Direito Processual Civil, Unifacs, pela seguinte banca examinadora:

Nome: _____

Titulação e instituição: _____

Nome: _____

Titulação e instituição: _____

Nome: _____

Titulação e instituição: _____

Salvador, _____/ _____/ 2011.

Ao meu filho Luís Fernando,
amor imenso e inexplicável, por ter sido
privado do colo de mãe durante os inúmeros
dias e escrita deste trabalho.

Ao meu pai Vlandeslau,
pois perdê-lo no meio do curso deixou-me sem
norte, sinto sua falta, Seu Costa.

AGRADECIMENTOS

O medo de ser injusta com pessoas que tanto amo, e que tanto ajudaram, de vários modos, a realização desta pesquisa, faz com que meus agradecimentos sejam extensos. E neste gesto misto de reconhecimento, carinho, amor e devoção, começo dando graças a Deus e a minha protetora, Santa Bárbara, pela saúde, física e mental, para conseguir concluir essa jornada.

A minha mãe, Maria Luiza, um agradecimento especial, por ser a melhor e mais compreensiva mãe do mundo, cujo amor incondicional tanto me ampara e socorre, e a quem credito minha escolha pelo Direito, pois sei que ser magistrada era seu sonho quando a gravidez, justo de mim, mudou seus planos. Saiba que não conheço pessoa com maior senso de justiça que a senhora. Muito obrigada por me incentivar a continuar, em todas as vezes que pensei em desistir.

Ao meu marido, Luís Augusto, maior incentivador desta conquista, sou grata pelos tão felizes anos juntos. Só um amor recheado de tanta cumplicidade, respeito, e amizade poderia compreender e comemorar uma vitória dessas. Guto, nunca esqueça o quanto amo você.

A minha grande família, pilar do meu existir, em especial às minhas irmãs, Maria das Graças, Débora, e Priscila: por serem exemplos de superação e felicidade. E às minhas sobrinhas, Caroline e Lize: pela certeza de que nossa segunda geração também é vencedora.

Agradeço, ainda, a Lucas Pinto e Luciana Amorim Trindade, grandes amigos e compadres. Ao primeiro, pela ajuda na pesquisa deste trabalho, com o envio de tantos e-mails, notícias e entrevistas atinentes ao assunto. E à segunda, pela companhia, estímulo e incentivo ao longo do curso juntas, especialmente quando Luís Fernando, recém nascido, tanto exigia de mim.

Aos meus mais que amigos, sócios; mais que sócios, companheiros, Ian Quadros e Mariângela Espinheira, agradeço a colaboração e o apoio para que o tempo consumido pela nossa advocacia não impedisse a finalização desta monografia.

Aos meus sogros, Alair e Rosa, agradeço pelas tantas noites de quintas feiras dedicadas a cuidar de Nando na minha ausência, vocês também fazem parte desta caminhada vitoriosa.

Por derradeiro, mas de forma especial, agradeço aos professores Ricardo Malfati, Antonio Adonias e Rodrigo Klippel, pela dedicação à turma, pelas aulas, debates, lições jurídicas e discussões entusiasmadas, que deram verdadeiro sentido ao curso de pós graduação; e por me fazerem lembrar de uma paixão antiga, adormecida há anos em mim: o Direito.

"O futuro tem muitos nomes.
Para os fracos é o inalcançável.
para os temerosos, o desconhecido.
Para os valentes é a oportunidade."

Victor Hugo

RESUMO

O Processo Eletrônico, introduzido no ordenamento jurídico brasileiro pela Lei 11.419 de 19 de dezembro de 2006, trouxe um novo cenário procedimental aos operadores do Direito, no qual se aboliu o uso de papel, fazendo com que o processo não mais possua autos físicos, estes substituídos por uma composição de arquivos digitais, inseridos e armazenados em um determinado sistema computacional, administrado pelo Poder Judiciário. Diante desta nova dinâmica, compreensível e esperado o surgimento de dúvidas inerentes às inovações tecnológicas impostas pelo cotidiano processual que se descortina. Assim, a presente pesquisa tem por objetivo, apresentando os efeitos da era digital sobre o Direito, analisar a nova realidade inserida pela lei citada, e considerando a importância da prova como instituto fundamental do processo – eis que sobre ele forma-se o convencimento do magistrado acerca das razões fáticas da pretensão deduzida pela parte – compreender os mecanismos da impugnação da prova documental no processo eletrônico.

Palavras chave: Processo eletrônico. Prova documental. Impugnação.

ABSTRACT

The Eletronic Procedure Law, introduced in Brazilian legal system by the Law 11.419, December, 19 of 2006, brought a new procedural scenarium to the Law users, which abolished the use of paper, making the lawsuit no longer has physical acts, these replaced by a composition of digital files, entered and stored in a computer system, administered by the Judiciary courts. Faced this new dynamic, understandable and expected the emergence of doubts inherent of technological innovations imposed by the procedural routine forthcome. Thus, this research aims, showing the effects of the digital age on the law, to analyze the new reality entered by the law cited, and considering the importance of evidence as a fundamental institution of the procedure - because above it that way to convince the magistrate about the factual reasons for the claim brought by the part of lawsuit - to understand the mechanisms to refute the documentary evidence in the electronic procedure.

Key words: Eletronic procedure. Documental evidence. Objection.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

PJe – Processo Judicial Eletrônico

PROJUDI – Processo Judicial Digital

e-SAJ – Portal de serviços eletrônicos do Tribunal de Justiça do Estado da Bahia

e-Proc – Sistema de peticionamento eletrônico da Justiça Federal

e-Doc - Sistema Integrado de Protocolização e Fluxo de Documentos Eletrônicos da Justiça do Trabalho

e-SAMP – Processo eletrônico da Justiça do Trabalho

CNJ – Conselho Nacional de Justiça

e-CNJ – Processo Eletrônico do Conselho Nacional de Justiça

e-STJ – Sistema de Peticionamento Eletrônico do STJ

e-STF – Sistema de Peticionamento Eletrônico do STF

STJ – Superior Tribunal de Justiça

STF – Supremo Tribunal Federal

DJE – Diário de Justiça Eletrônico

PDF – Formato de arquivo eletrônico requisitado no processo eletrônico

ICP-Brasil – Infra Estrutura de Chaves Públicas Brasileiras

ITI – Instituto de Tecnologia da Informação

e-democracia – Portal de participação popular da Câmara dos Deputados

Hardware – parte física do computador.

Software – parte lógica do computador.

CIJ – Audiência de conciliação, instrução e julgamento.

SRF – Secretaria da Reeita Federal

AC-OAB – Autoridade Certificadora da Ordem dos Advogados do Brasil.

BACENJUD – Sistema do Banco Central para penhora *on line* em contas correntes.

ICP-OAB – Infraestrutura de Chaves Públicas da Ordem dos Advogados do Brasil

MP – Medida Provisória

CPC – Código de Processo Civil

CF – Constituição Federal

CC – Código Civil

Chip – circuito integrado com suporte em pastilha de silício ou outro material, semicondutor, no qual são gravados ou inseridos componentes eletrónicos que, em conjunto, desempenham uma ou mais funções.

Token - Dispositivo para armazenamento de certificado digital de forma segura.

SUMÁRIO

1 INTRODUÇÃO

Se o Direito como ciência social evolui conforme o próprio caminhar humano, inegável e inexoravelmente será impactado por essa contínua, crescente e irreversível evolução tecnológica que dita o ritmo do crescimento social moderno.

Não se tem dúvidas de que a era digital ou era da informação já influencia e modifica as relações sociais e jurídicas, de um modo geral, na medida em que criou necessidades antes inexistentes fazendo surgir a busca pela adaptação do Direito à dinâmica dessas relações, exigindo, ainda, avanços rápidos dos legisladores e operadores para acompanhar tais mudanças.

Sabe-se que, nesse sentir, tanto o Direito material quanto o processual clamam por maior dedicação do legislador para a sua atualização com vistas a esta nova realidade social, desde definições dos negócios jurídicos realizados virtualmente à proteção intelectual de marcas e patentes de softwares; passando por regulação do setor de Internet, tipificação dos delitos cibernéticos, chegando às regras processuais e procedimentais necessárias a essa nova realidade.

Como exposto anteriormente, inegável e irreversível a evolução do Direito no que pertine a sua inserção nos avanços tecnológicos que se apresentam quase diariamente à sociedade.

A prática dos operadores do direito está diante de inúmeras mudanças, especialmente por conta da implementação do processo eletrônico, disciplinado na Lei 11.419/06, que tornou possível a criação dos inúmeros sistemas de procedimento digital, em que os atos processuais antes praticados em meio físico foram transpostos para a internet.

Parece que o legislador pátrio, talvez pelo efeitos da Era Digital sobre o direito, promoveu a Emenda Constitucional 45 de 2004, que inseriu o inciso LXXVIII ao artigo 5º da Carta Magna, garantido “a todos, no âmbito judicial e administrativo, são assegurados a razoável duração do processo e os meios que garantam a celeridade de sua tramitação.”

Destarte, a soma de evolução digital com o princípio da razoável duração do processo, disposto no normativo acima citado, resultaram na Lei 11.419/06, que, de fato, inova e parece querer um procedimento ágil, célere e mais condizente com o clamor social dos usuários da justiça, que apontam sempre para a morosidade como fator de desconfiança e descrédito dos mesmos em relação a efetiva entrega das tutelas pretendidas ao Estado.

Não se olvida que tal advento legal é um marco legislativo processual sem precedentes, conquanto faça desaparecer os autos na sua forma física, em volumes, em papel, o que, tradicionalmente, sempre foram os instrumentos dos advogados, juízes, membros do Ministério Público e serventuários.

Observe-se o quão significativa é a Lei 11.419/09: de plano ela extingue, ou modifica substancialmente, inúmeros atos processuais disciplinados no CPC, a exemplo da distribuição, autuação e carga dos autos – se virtuais, a distribuição é eletrônica, não há o que se autuar ou o que levar – citações e intimação, que tem previsão de serem feitas através do sistema de portal dedicado ou pelo DJE; a contagem de prazos – eis que o inicio do mesmo se dará após a disponibilização do DJE, etc.

Em suma, a dinâmica processual, do ano de 2006 para cá mudou e muito. E continuará mudando, pois tendo como norte uma incessante busca por imprimir maior celeridade nos feitos e maior efetividade às tutelas postas sob sua proteção, o Estado implementará cada vez mais recursos tecnológicos à serviço dos jurisdicionados.

Partindo da premissa evolutiva, cumpre conhecer o processo eletrônico, essa nova realidade imposta aos operadores do Direito, e as nuances que o cerca, a fim de que, de posse da melhor compreensão e entendimento de seus mecanismos, domine-se esse novo campo processual que surge.

Como tudo o que é novo, resistências não vão faltar, muito menos discussões acaloradas, na doutrina e na jurisprudência. E por ser um tema com tímida produção doutrinária – em função da tenra idade do dispositivo legal que cria o processo eletrônico e do próprio período de implantação nas mais diversas jurisdições – carece de estudos aprofundados sobre suas nuances, aplicabilidade e (in)compatibilidade de aplicação com os demais regramentos pátrios.

É natural, compreensível até, que o processo eletrônico, assim como o Direito Digital, desafie conhecimentos multidisciplinares, especialmente no que diz respeito a sua inerente vinculação com a ciência da computação. Possível e provavelmente, em pouco tempo, a informática jurídica será matéria obrigatória em todos os cursos superiores de Direito.

Utilizando uma comparação temporal, vê- se hoje que o processo eletrônico está para o processo físico, assim como o computador está para a máquina de datilografia. E não saber manejar os recursos que esse novo procedimento processual equivale a permanecer datilografando, quando se possui um computador à mão.

Vencida a resistência cultural, não há porque não se debruçar sobre o processo eletrônico e enfrentar as questões relevantes que o mesmo expõe e que carecem de aprofundamento e estudo próprio.

Tais mudanças, inclusive, já são verificadas em órgãos jurisdicionais que implementaram o processo eletrônico. De acordo com números divulgados pelo CNJ, pelo menos 70% do tempo de tramitação de processos são gastos em movimentos burocráticos entre protocolos, gabinetes e cartórios. No Poder Judiciário do Estado da Bahia, além da comarca de Salvador, outras trinta e três[1] possuem as Varas dos Sistemas dos Juizados Especiais utilizando o processo eletrônico do PROJUDI, e os demais juízos já começaram a utilizar o sistema de automação judiciária chamado e-SAJ.

Apenas no primeiro semestre de 2010, o STJ ganhou 30% (trinta por cento) de área útil com a eliminação de processos em papel e armários, e o volume de processos que lá tramitam foi reduzido pela metade, isto é, de 460 mil, em setembro de 2008, para cerca de 230 mil, no ano passado. A empolgação com o uso do processo eletrônico não se limita a celeridade com que os efeitos tramitam, mas também com a economia que o mesmo representa para os usuários.

Em recente notícia o STJ apontou os efeitos destas mudanças, inclusive a repercussão da inovação:

> Tachada inicialmente como ousada e até impossível, a meta do Superior Tribunal de Justiça (STJ) de eliminar os processos em papel foi atingida. Quase 90% dos 290 mil processos em tramitação são eletrônicos. "O trabalho era gigantesco. Ninguém poderia prever que isso seria alcançado num tempo tão curto. É uma mudança de paradigma", avalia o ministro Ari Pargendler, presidente do STJ.
>
> O processo eletrônico é muito mais do que apenas digitalizar papel. "Na verdade, ele mudou hábitos, mudou mentalidade, mudou cultura", entende o ministro Luis Felipe Salomão. "Quando o ministro Cesar Rocha primeiro me falou da idéia dele de tornar o processo eletrônico o único mecanismo de funcionamento dos processos no STJ, digitalizando todo o papel que existia, eu, sinceramente, confesso que achei que isso seria impossível de ser realizado num curto espaço de tempo", lembra.
>
> O ministro Salomão passou de incrédulo a entusiasta. Para um magistrado que iniciou a carreira disputando máquina de escrever, ver a eliminação de toda burocracia que o processo físico carrega é uma revolução. "Percebo para prestação da justiça uma melhora muito grande, não só em termos de celeridade, mas de segurança, de um melhor controle dos processos dentro do gabinete. Eu só vejo vantagens, não só para o juiz, mas para quem ele serve, que é a população", observa Salomão.
>
> "Pense em 12 mil processos, com uma média, por baixo, de três volumes. Dá 36 mil volumes de aproximadamente 200 páginas. É um absurdo! E isso praticamente sumiu", impressiona-se o ministro Paulo de Tarso Sanseverino com a organização do gabinete, mesmo com o elevado estoque de processos que recebeu quando chegou ao STJ. Além de tornar o ambiente mais agradável, Sanseverino percebeu que seu trabalho tornou-se mais ágil na medida em que não precisa mais aguardar ou se deslocar para ter um processo em mãos.

[1] Obtido por meio eletrônico. Disponível em: <www.tjba.jus.br>. Acesso em: 20 out. 2011.

Enquanto o processo físico leva aproximadamente cem dias para ser distribuído, o processo eletrônico chega ao gabinete do relator em apenas seis dias. A celeridade ocorre porque são eliminadas as chamadas fases mortas do processo, como transporte, armazenamento, carimbos e outros. “A remessa física dos processos tradicionais e, em muitos casos, a sua localização implicava em perda de tempo que hoje pode ser aproveitada em sua análise, permitindo melhor controle e, também, melhor qualidade técnica das próprias decisões”, afirma o ministro Castro Meira.

A facilidade na consulta das peças também ajuda. O ministro Sanseverino observou que nas sessões de julgamento, durante a sustentação oral, quando o advogado aponta algo que deixa o relator em dúvida, em muitos casos não é mais necessário interromper o julgamento com pedido de vista regimental. “É possível ir direto ao ponto no processo. Tiro as dúvidas imediatamente e profiro o voto”, afirma o ministro.

O processo eletrônico também proporcionou importantes benefícios para administração do STJ. Houve expressiva redução de atestados médicos de servidores, principalmente em decorrência alergias, problemas respiratórios e dores da coluna provocadas pelo manuseio e transporte de pilhas de processos em papel. Diminuiu a fabricação de armários e conserto de portas que eram danificadas pelos carrinhos que transportavam processos. Centenas de estantes foram doadas a instituições de caridade.

Apesar das vantagens, a ministra Nancy Andrighi tem outra percepção do processo eletrônico. “É o fim do papel, mas não da cruel espera”, alerta. Para ela, a visão diária dos autos físicos, com suas tarjas coloridas, chama constantemente a atenção do magistrado para o dever de ir além do possível para sanar as angústias contidas em cada processo.

Nancy Andrighi teme que a presença quase imperceptível dos processos virtuais no gabinete prolongue as dores neles contidas. “A reflexão que convido todos a fazer está longe do sentimento de aversão às novidades tecnológicas que infelizmente ainda domina o Judiciário brasileiro. Ao contrário, o que se pretende é ativar intensa vigilância para que não se retroceda na imprescindível jornada de humanização do Judiciário”, explica a ministra.

Advocacia

O processo eletrônico afetou profundamente a forma de atuação dos advogados no STJ. Como ocorre em toda mudança, houve muitas dúvidas, desconfianças e resistência. Foi necessário um período razoável de adaptação. Primeiro os advogados foram convencidos da segurança do sistema. Depois veio a necessidade de adquirir a certificação digital – uma assinatura eletrônica necessária para ter acesso aos autos virtuais e ajuizar petições eletrônicas.

Ultrapassado o impacto inicial, hoje os advogados celebram as vantagens da inovação. “Com o passar do tempo, a utilização do processo eletrônico se revela como um instrumento extremamente eficaz e eficiente, pois amplia a possibilidade de trabalho na medida em que os prazos se ampliam. Os prazos que no processo físico iam até as 19 horas hoje vão até meia-noite”, afirma o advogado Nabor Bulhões.

Guilherme Amorim Campos da Silva conta que o processo eletrônico melhorou sua relação com os clientes. “Muitas vezes o cliente não entende a demora do processo e chega a achar que o advogado não está trabalhando com empenho. Agora podemos mostrar a ele tudo o que acontece com o caso, inclusive as petições da parte contrária.”

O advogado Fernando Neves lamenta a perda do contato físico com os autos ao qual estava tão acostumado ao longo de seus 35 anos de profissão. “Mas esse hábito já está superado, pois as facilidades da nova ferramenta são enormes”, diz. Entre essas facilidades, ele destaca o transporte, arquivamento, acesso remoto aos autos e a agilidade na tramitação.

Se para um profissional que atua em Brasília, sede do STJ, o acesso eletrônico aos autos é uma comodidade, para os de outros estados é uma enorme economia de tempo

e dinheiro. “A economia é significativa porque o deslocamento aéreo é caríssimo, assim como a hospedagem ou a contratação de um correspondente em Brasília. E tudo é repassado ao cliente, diretamente ou no valor dos honorários”, conta Márcio Delambert, advogado do Rio de Janeiro. Muito resistente ao processo eletrônico, ele impetrou o primeiro habeas corpus pela internet há poucas semanas. “Fiquei impressionado com a facilidade. Segui o roteiro do site e no mesmo dia a liminar já estava no gabinete do relator. Achei espetacular”.

Ortodoxo confesso, o jovem advogado Benedito Alves Lima Neto, que vive em São Paulo, reconhece as ganhos obtidos com o processo eletrônico, mas afirma que ainda prefere o físico. “Eu gosto de manusear papéis, gosto dos livros, gosto de biblioteca, gosto muito do papel, acho que o trabalho fica mais pessoal”, explica.

Repercussão Internacional

O sucesso do processo eletrônico despertou o interesse internacional. Membros do Judiciário da Espanha, República Dominicana, Cuba, Peru e Eslováquia vieram ao Brasil para conhecer a ferramenta e assinar acordo de cooperação técnica. “Muitas das delegações estrangeiras chegam ao STJ pensando que o processo eletrônico é uma medida apenas tecnológica. No fim, elas saem daqui impressionadas com a forma como a iniciativa repercute diretamente no trabalho de todos os servidores e magistrados”, conta Rodrigo Penna, coordenador de Cooperação Internacional da Assessoria de Relações Internacionais do Tribunal.

“Não vi nada tão bem elaborado em nenhum lugar do mundo”, afirmou o presidente do Supremo Tribunal de Justiça da República Eslovaca, Stefan Harabin, na mais recente visita de delegação estrangeira ao Brasil. Ele soube do processo eletrônico durante uma reunião em Londres, quando o então presidente do STJ, ministro Cesar Rocha, apresentou o sistema brasileiro aos europeus. “Posso confirmar que não se encontra na Europa nenhum outro sistema tão perfeito, tão sofisticado, do ponto de vista eletrônico”, assegurou Harabin.

O Banco Mundial (Bird) classificou o processo eletrônico brasileiro como uma boa prática internacional e vem recomendando o modelo aos países que buscam aporte financeiro para modernizar seus métodos jurídicos. “O exemplo do Brasil mostra que o processo eletrônico pode levar a impressionantes ganhos de eficiência, reduções de custo, bem como à transparência e ao acesso democrático à informação”, afirmou Makhtar Diop, diretor do Bird para o Brasil.

A experiência brasileira foi discutida pelo banco com Peru, Senegal, Moçambique e outros países africanos de língua portuguesa. Segundo Diop, o bom funcionamento dos sistemas de justiça é um componente essencial do Estado de Direito, razão pela qual é tão importante ao desenvolvimento econômico. Por isso, o Bird apoia iniciativas inovadoras na gestão de processos judiciais.

Desafios

A meta de transformar todos os autos físicos em processo eletrônico foi lançada no final de 2008 pelo então presidente do STJ, ministro Cesar Rocha. O trabalho começou com digitalização de 4.700 processos em grau de Recurso Extraordinário. Já em 2009, a digitalização estendeu-se a outras classes processuais e teve início a tramitação eletrônica. No dia 25 de junho daquele ano, um lote de processos eletrônicos levou dois minutos para sair do Tribunal de Justiça do Ceará, em Fortaleza, e chegar ao STJ. Em 33 minutos, dois processos foram autuados, classificados e distribuídos ao ministro relator.

Gradativamente, todos os tribunais estaduais e federais do país foram aderindo ao sistema. Faltava apenas o Tribunal de Justiça de Minas Gerais, que acaba de assinar termo de cooperação técnica com STJ. Até agora, quase cem mil processos eletrônicos foram remetidos pelos tribunais de justiça e tribunais regionais federais.

Embora já exista a integração com as demais cortes do país, o ministro Ari Pargendler afirma que é preciso avançar, pois 54% dos processos que chegam ao STJ ainda são em papel. “Os tribunais precisam nos encaminhar esses processos por meio eletrônico. Por enquanto, ainda estamos recebendo o maior número de processos em

> autos físicos. Isso nos dá uma grande sobrecarga de trabalho porque temos que transformar o meio físico em meio virtual e isso é feito pelos servidores e estagiários do STJ com grande gasto de tempo e de dinheiro", afirma Pargendler.
>
> A integração também envolveu a Advocacia Geral da União e a Procuradoria Geral da Fazenda Nacional (PGNF), que atuam em milhares de processos no STJ. Justamente por conta do grande número de ações, Cláudio Seefelder, coordenador-geral da Representação Judicial da PGNF, defende um tratamento diferenciado para os entes públicos que agilize o acesso aos autos e o peticionamento eletrônico. "Infelizmente existem picos de consulta em que o sistema fica muito lento e, às vezes, inoperante", reclama.
>
> A Secretaria de Tecnologia da Informação (STI) do STJ informa que a lentidão no sistema é causada, em grande parte, pelo uso inadequado do processo eletrônico. Muitos advogados fazem as peças no computador, imprimem o documento para assinar e digitalizam para então enviá-lo ao STJ. "Com isso, um arquivo que originalmente tinha em média 2 Kbytes, depois de digitalizado passa a ter 200 Kbytes, ou seja, muito mais pesado", explica Carlos Leonardo Pires, responsável pelo processo eletrônico na STI. "O ideal é que os documentos digitados no word ou outro editor de texto sejam gerados diretamente em arquivo PDF a partir do próprio documento eletrônico. O site do STJ traz orientação quanto a este procedimento."
>
> O STJ trabalha no constante aprimoramento de seu sistema eletrônico e na construção de ferramentas para agilizar e facilitar operação do processo eletrônico. Além da integração com entes públicos que permita a troca direta de arquivos eletrônicos - sem digitalização - estão sendo instaladas novas tecnologias de armazenamento e tráfego de rede que irão proporcionar mais velocidade de acesso.[2] (grifos do autor)

O fato é que o Direito Processual Civil conta com alguma vantagem legislativa em relação aos demais ramos, conquanto o advento da Lei 11.419 de 19 de dezembro de 2006 lançou as bases e diretrizes do processo eletrônico já em uso. E tal dispositivo, de fato, trouxe intensas modificações ao cotidiano dos operadores do Direito, eis que, na prática está a transformar o mundo dos autos físicos, com imensos volumes e numerosas páginas, em outro, eletrônico, digitalizado, virtual.

De plano, tal mudança, necessariamente requer novos hábitos e habilidades, considerando que há uma natural resistência do ser humano ao que é novo, especialmente ao que tange o mundo tecnológico, que, não há duvidas irá exigir, cada vez mais dos usuários e administradores do Poder Judiciário como um todo.

A realidade está posta e tanto os jurisdicionados, quanto os operadores do Direito como um todo, já estão diante do processo eletrônico em praticamente todas as jurisdições e instâncias, vendo e trabalhando com peças processuais e assinaturas eletrônicas, autos virtuais, senhas de acesso, certificados digitais e documentos digitalizados.

---

[2] STJ. Obtido em meio eletrônico. Disponível em: <http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=101488> Acesso em: 21 out. 2011

Com toda nova dinâmica trazida pela Lei 11.419/06, incipiente, embora extremamente ativa, é a produção doutrinária e jurisprudencial que gira acerca dos conceitos e práticas do processo eletrônico, muitas vezes de difícil compreensão graças à intrínseca ligação com a ciência da computação e seus, muitas vezes, específicos e complexos conceitos, nomenclaturas e procedimentos.

Clara é irreversibilidade da evolução tecnológica, o que, naturalmente, demandará conhecimento aprofundado do processo eletrônico e seus institutos.

Nesse sentido é que o presente trabalho pretende primeiramente traçar um escorço dos efeitos da Era Digital sobre o Direito, procurando explicar a informatização do judiciário e seus reflexos para os jurisdicionados.

Tais premissas darão lastro à introdução de maiores explicações sobre a Lei 11.419/96 em si, e sobre o procedimento no processo eletrônico, tópico cuja abordagem procura situar o leitor no *modus operandi* do sistema digital, para demonstrar que os diferentes tipos de programas adotados no Brasil carecem de uma padronização, porquanto as divergências no uso de cada procedimento eletrônico dão margem a questionamentos sobre segurança e integração, entre cada um deles e de cada um com os dos tribunais superiores.

Apresentados os preâmbulos do estudo, incumbe relembrar breves notas sobre Teoria Geral da Prova, para, estabelecendo o seu conceito e espécies, especialmente da prova documental, ater-se às explicações sobre documento eletrônico e prova no processo eletrônico. Estes, por demais importantes, onde se busca apontar as fragilidades de segurança no procedimento digital.

Compreendidas as terminações tecnológicas, e a diferenciação entre os sistemas e seus requisitos, adentra-se à impugnação ao núcleo temático da pesquisa, para esclarecer como se dá a realização da prova no processo eletrônico, diferenciando alguns importantes institutos, como a prova eletrônica, o documento eletrônico e o documento digitalizado assinado eletrônica ou digitalmente.

Apenas após tais diferenciações é que se estará apto a melhor compreender a prova documental no processo eletrônico, especialmente o que dispõe o artigo 11 da Lei 11.419/06. Isto porque, lacunosa a legislação, e inédita a doutrina, sobre o tema, cumprindo indagar: qual a forma e o procedimento processual cabível para impugnar a prova documental produzida no processo eletrônico?

A resposta à indagação anterior, sem dúvidas, servirá, não apenas para elucidar o processo eletrônico e a produção de prova no mesmo, mas também apontará, como via reflexa, a responsabilidade pela produção da mesma.

Dentro dos contornos da legislação, na forma do citado artigo 11, pensa-se, inicialmente, que tal responsabilidade é daquele operador do Direito que insere a prova aos autos do processo eletrônico, sem, contudo, haver apontamento do dever da parte que a fornece ao dito operador. Mais ainda, tal resposta tentará lançar luz ao §2º do supracitado artigo 11 da Lei 11.419, para, especificadamente, traçar a forma de impugnação da prova documental no processo eletrônico, seu processamento, se nos autos eletrônico ou não.

Esclarecida o núcleo central da pesquisa, seus efeitos aos advogados e partes também são pontuados ao final do trabalho, que se encerrará com a abordagem do tema pelo projeto do novo Código de Processo Civil e a conclusão do trabalho.

Se os estudos sobre processo eletrônico carecem de aprofundamento em inúmeros tópicos, e não obstante publiquem-se artigos sobre o tema, a sua pesquisa e estudo encontra, no tempo e na velocidade das informações e descobertas, seus maiores obstáculos.

Ao iniciar os estudos do assunto, o projeto desta pesquisa encontrou um cenário que, em apenas um ano, modificou-se extensamente. Este, inclusive, é o desafio daqueles que se debruçam ao estudo do processo eletrônico: a própria natureza de seu procedimento modifica-se tão ou mais rápido quanto seu próprio estudo.

De meados do corrente ano para cá o cenário jurídico do tema sofreu várias mudanças, como o recebimento de um projeto de lei que cria o marco zero da internet, importantíssimo para as relações de direito material, o Conselho Nacional de Justiça apresentou o programa do PJe, um sistema de processo eletrônico, a ser implantado em todos os tribunais do país, e um número grande de artigos e notícias sobre o tema foi publicado.

Talvez esta ebulição acerca do processo eletrônico tenha sido o maior obstáculo do trabalho que se apresenta, conquanto, obrigou a sua revisão e atualização até o praticamente o momento de sua entrega.

A visão do advogado como mero representante dos interesses da parte já não encontra mais eco na simples apresentação de pedidos ao magistrado, passa, sem dúvida, por uma mudança significativa a profissão.

Na colheita do material de pesquisa desta monografia, a fala de Patrícia Peck (2009, p. 342-347) fez sentido aos propósitos que deram margem à escolha do tema:

> Na sociedade digital, o advogado tem de ser um estrategista. A complexidade da sociedade traz maior complexidade jurídica. Já não é suficiente conhecer apenas o Direito e as leis; devem-se conhecer os modelos que conduzem o mundo das relações entre pessoas, empresas mercados, Estados. A postura profissional de estrategista significa assumir um papel determinante para a adequada condução dos negócios no mundo digital. Cabe ao profissional do Direito dar os caminhos e as soluções viáveis, pensadas no contexto competitivo e globalizado de um possível cliente virtual-real, convergente e multicultural.
>
> [...]
>
> Portanto, verificamos que a informatização tem trazido aos profissionais do Direito mudanças não só na maneira de pensar o direito, mas também de trabalhar com ele. Com a informatização dos escritórios e do próprio Poder Judiciário, assim como as profundas alterações em sede processual, não podemos admitir que os juristas não estejam preparados para compreender e discutir essas novas questões. Talvez este seja o momento de pensar em como as Faculdades tenham um mínimo de conhecimento técnico a respeito das mudanças dos paradigmas e forte base teórica sobre os princípios que regem a nova era digital e suas implicações.
>
> [...]
>
> Esse descompasso na formação mais completa de profissionais que sejam estrategistas jurídicos faz com que na seja plantada a semente nesta nova geração de que cabe a eles escrever novas leis, as novas sentenças, os novos contratos e acordos entre as partes, mantendo o equilíbrio e harmonia do Estado de Direito, fazendo com que haja segurança jurídica das relações e evitando-se que as pessoas, desesperadas por não serem atendidas por um Ordenamento mais bem preparado, acabem por buscar "fazer justiça com o próprio *mouse"*.
>
> Finalmente, a sociedade digital exige que os profissionais do Direito deixem de lado algumas rivalidades acadêmicas para discutirem conjuntamente paradigmas como ordenamento, legitimidade e segurança no âmbito de uma sociedade globalizada, convergente digital e em constante mudança. É essa postura que o mercado vai cobrar. É esta nova postura que os profissionais devem adotar para poder atuar no âmbito de uma sociedade digital.

A nostalgia do uso do papel hoje é idêntica a da máquina de escrever quando do surgimento dos computadores pessoais, mas uma nação excessivamente saudosista não consegue evoluir como o próprio caminhar do mundo, vivendo emperrada, inclusive, em burocracias que não consegue ultrapassar.

Ora, em uma sociedade onde o próprio sufrágio é eletrônico há mais de onze anos[3], não faz sentido inexistir marcos civil e penal em legislação sobre internet; não faz sentido o ensino do Direito no país praticamente ignorar as relações jurídicas firmadas eletronicamente; e negar os avanços sociais trazidos com a evolução digital é permanecer no escuro da falta de conhecimento.

---

[3] TSE. Disponível em: < http://tse.jus.br/internet/eleicoes/votoeletronico/informatizacao.htm> Acesso em: 20 out. 2011

Se o presente estudo lançar qualquer feixe de luz sobre o processo eletrônico já terá alcançado seu objetivo: demonstrar que o novo instalou-se no Direito pátrio, e que não apenas o procedimento e o processo mudaram, mas também a advocacia, que não é, nem será, mais a mesma.

2 PROCESSO ELETRÔNICO

O processo eletrônico encontra sua exata definição no capítulo da Lei 11.419/06 que o instituiu: é a informatização do processo judicial, isto é, a transposição dos atos processuais praticados fisicamente para o mundo virtual.

Porém, para melhor compreender este fenômeno jurídico processual experimentado no país, inclusive no que pertine ao objeto da pesquisa que se apresenta, é de suma importância destacar a junção da informática com o Direito, e sua evolução, posto que esta combinação, como reflexo da evolução social, dará o substrato ao surgimento do processo eletrônico como conhecido hoje.

O que se pretende neste capítulo é, traçando um escorço histórico da influência da Era Digital sobre o Direito, apresentar os reflexos da informatização do poder judiciário aos seus jurisdicionados e usuários, a fim de compreender os motivos, quer fáticos quer jurídicos, que conduziram o legislador a transpor para o mundo cibernético os atos processuais.

2.1 ERA DIGITAL E O DIREITO

A Era Digital, ou Era da Informação, é o lapso temporal que se inicia após a Era Industrial, com base apontada para a década de 1980, mas com verdadeiro início em meados do século passado, com o surgimento dos primeiros microcomputadores, da própria rede mundial de computadores, a Internet, e da tecnologia de fibra ótica.[4]

Apesar de transmitir uma aparente imagem de surgimento recente, a informática, mola propulsora desta era, não é uma ciência nova, posto que os computadores já conseguissem comunicar-se entre si desde meados de 1950, sua propagação, é verdade, deu-se com maior força a partir dos anos 90, quando seu uso foi disseminado com maior força, especialmente no Brasil. (ALMEIDA FILHO, 2010, p. 25).

De fato, a disseminação do uso das novas tecnologias impactou, de um modo geral, a forma das relações humanas, principalmente no que tange ao tempo e espaço. Note-se que as

[4] Obtido por meio eletrônico. Disponível em <http://pt.wikipedia.org/wiki/Era_da_Informa%C3%A7%C3%A3o>. Acesso em: 21 out. 2011.

barreiras geográficas parecem não mais existir, e a comunicação entre as pessoas passou a ser instantânea.

As realidades de outras comunidades, anteriormente tão distantes, estão hoje disponíveis a qualquer individuo que tenha acesso a um computador conectado a Internet. E mais, se antes os usuários da informática eram meros espectadores daqueles contextos longínquos, hoje já não o são mais. A facilidade e velocidade do acesso à informação e da comunicação, transformou a rede mundial de computadores de acessório a instrumento de cooptação para as mais diferentes causas e finalidades.

No inicio da década de 90, os usuários de computadores pessoais o tinham mais para uso de ferramentas de editoração de texto e afins, mas já em meados daquela década, passaram às descobertas da comunicação por e-mail e informações de outros lugares; culminando com a explosão do uso do comércio eletrônico, e convivência em redes sociais, já nos dias atuais.

Fato notório e de conhecimento comum que, se em 2001 os ataques terroristas perpetrados por extremistas islâmicos aos Estados Unidos da América eram transmitidos ao vivo, em uma prova inequívoca da globalização da informação; os recentes levantes armados em países árabes do oriente médio, que deram margem à destituição do poder de diversos regimes opressores, demonstraram o uso das redes sociais como uma das ferramentas de interação e arregimentação dos oposicionistas.

A Era da Informação – termo mais apropriado para definição deste contexto histórico – reflete exatamente este contexto no qual as inovações tecnológicas tornaram-se instrumentos de transmissão e disponibilização de informações, em uma velocidade e quantidade nunca antes experimentada pelo ser humano, criando necessidades e experiências anteriormente inexistentes, permitindo uma vivência e integração onde as distâncias físicas não mais representam qualquer obstáculo.

Destarte, os reflexos dessa Era são incontáveis, e se tem, hoje, verdadeiramente, uma nova dinâmica social, onde o individuo não conectado ao mundo virtual é considerado um excluído digital que deve ser inserido no sistema, pois ele, de fato, é atingido, tocado, ainda que contra sua vontade, pelo mundo digital.

Trata-se de um tempo onde tudo parece se (des)materializar virtualmente, de simples operações bancárias à relacionamentos interpessoais; de mera compra e venda à *marketing* digital; de localizadores via satélite à um simples telefonema; da previsão do tempo ao registro das infrações de trânsito. Para onde quer que se olhe há influência desta Era.

Não seria diferente com as relações jurídicas, posto que as mesmas sejam reflexos das relações humanas como um todo. Isto é, o Direito como ciência social surge para disciplinar as relações conflituosas que não mais podem ser regidas, ou resolvidas, pela auto tutela. E se a dinâmica na vida social evolui ou modifica-se, as leis que a regulam terão de também evoluir e inovar, a fim de tutelá-las. E o legislador brasileiro vem, ainda que com certa lentidão para alguns doutrinadores, acompanhando tal evolução.

Historicamente, pontua José Carlos de Araújo Almeida Filho, o uso de meios eletrônicos no país encontrou receptividade do legislador em situações isoladas, como na Lei do Inquilinato (BRASIL, Lei nº 8245/91), onde se admitiu pela primeira vez o uso do *fac símile* para a prática de ato processual, desde que prevista contratualmente.

Destaca o mesmo autor avanços nos esforços legislativos nas décadas de 90 e nos anos 2000, no sentido de implementar práticas processuais por meio eletrônico, com vistas a imprimir celeridade aos feitos, muito mais ativa no processo civil e processo do trabalho, que nas demais áreas do direito, especialmente a penal, onde as práticas processuais eletrônicas cingem-se ao envio de determinadas peças processuais, havendo certa celeuma sobre a possibilidade do interrogatório do acusado *on line* – defendida por Luiz Flávio Gomes, mas repudiada por outros penalistas, que defendem o direito do réu de ser ouvido na presença da autoridade judiciária. (2010, p. 24-37)

O advogado Omar Kaminski mantém um site[5], denominado internet legal, no qual se pode ver a evolução legislativa brasileira ao longo da Era da Informação, com uma lista de todos os normativos criados em informática, telemática e internet no país.

Contudo, de simples leitura dos preceitos ali apontados, percebe-se que tais reflexos desta Era sobre o direito parece ter se voltado muito mais para procedimentos e técnicas específicas, tendo em vista ainda existir uma lacuna legislativa no âmbito de direito material. Neste sentir, crê-se que o legislador – talvez até pelo próprio caminhar do sistema legislativo brasileiro – não esteja conseguindo acompanhar os passos da evolução digital.

Apesar dos esforços, não há no Brasil, como já existem em outros países, normas específicas que disciplinem, por exemplo, os crimes cibernéticos, as transações comerciais *on line*, ou mesmo a responsabilidade civil dos provedores de acesso e provedores de conteúdo. Há, tão somente, projetos de lei que tentam regular tais relações jurídicas, tipificando os crimes

[5] Obtido por meio eletrônico. Disponível em <http://www.internetlegal.com.br/biblioteca/legislacao/> Acesso em: 26 out. 2011.

praticados virtualmente, regulando o direito autoral, e criando um marco civil da internet brasileira, no qual se estabeleceriam os direitos e obrigações dos usuários individuais, empresariais e públicos na rede mundial.

Esses esforços podem ser resumidos nos dois maiores Projetos de Lei em andamento hoje no Poder Legislativo federal: o PL 84/1999 e o PL 2.126/2011. O primeiro seria o marco penal da Internet brasileira, e o segundo o marco civil.[6] Digno de nota que o ritmo legislativo a ser impresso aos projetos desta natureza deve ser mais célere, a fim de acompanhar a própria rapidez desenvolvida nessa área, sendo pouco crível que um projeto de lei, como o PL 84/1999, que já tem mais de 10 (dez) anos em tramitação, consiga estar atualizado com as relações sociais que pretende tutelar, sob pena de o país estar sempre a um passo atrás da sua própria evolução.

Enquanto as normas de direito material caminha, em busca de regulamentações, a norma processual, todavia, foi e é atingida de maneira impactante por inúmeras modificações com vistas, especialmente, a dar maior celeridade ao deslinde das demandas judiciais em curso.

Com efeito, no ano de 2004, com a Emenda Constitucional nº 45, o artigo 5º da Carta Magna ganhou o inciso LXXVIII, que assim determinou: "a todos, no âmbito judicial e administrativo são assegurados a razoável duração do processo e os meios que garantam a celeridade de sua tramitação." (Brasil, 2009)

Sem dúvidas o a garantia constitucional acima, a o estabelecer o principio da razoável duração do processo, serviu de inspiração e lastro ao legislador para a promulgação da Lei 11.419/2006 que instituiu o processo eletrônico.

Conclui-se, então, que o citado diploma, sem dúvidas, constitui o marco processual brasileiro na Era da Informação, em um avanço tido como irreversível pelos doutrinadores e operadores do direito de um modo em geral.

A implantação do processo eletrônico no país é, por ora, o maior reflexo da Era Digital sobre o Direito Processual Civil, e seu estudo demanda maiores apresentações e elucidações, como adiante ver-se-á na presente pesquisa.

---

[6] CANÁRIO, Pedro. *Marco civil enriquece debate de leis para internet.*Obtido em meio eletrônico. Disponível em <http://www.conjur.com.br/2011-ago-27/marco-civil-enriquece-debate-leis-internet-dizem-especialistas> Acesso em: 26 out. 2011

2.2 A INFORMATIZAÇÃO DO JUDICIÁRIO E SEUS REFLEXOS

Rui Barbosa no início da década de vinte do século passado, em um texto de discurso que pretendia ler – acometido por uma doença não pode estar presente à cerimônia, cabendo o discurso ao professo Reinaldo Porchat[7] – para a turma de bacharéis que se graduava na Faculdade de Direito de São Paulo, afirmara que: "Mas justiça atrasada não é justiça, senão injustiça qualificada e manifesta." (BARBOSA, 2003).

Destarte, se a Era Digital reflete-se nitidamente sobre as regras tanto de direito material quanto de direito processual, ela também impacta a máquina do Judiciário, no sentido de que faz surgir para a mesma a necessidade de informatizar suas atividades, não apenas como reflexo da evolução social, mas também como requisito essencial para que seus mecanismos possam dar conta, de maneira célere e eficaz, das demandas que se apresentam e acumulam ano a ano, em uma efetiva prestação jurisdicional mais não apenas justa, mas célere.

Em uma metáfora elucidativa, a recusa em informatizar o judiciário seria a recusa da escrita com caneta esferográfica em preferência ao tinteiro; ou uma máquina de escrever – salvo por nostalgia – em detrimento de um editor de texto. Um contra senso pouco crível, especialmente quando se está diante do volume de ações em trâmite no judiciário pátrio.

Embora J.E. Carreira Alvim e Silvério Luiz Nery Cabral Junior (2008, p. 15) apontem a informatização do Judiciário como significado ou tradução da Lei 11.419/06 e do Processo Eletrônico, parece ser esta uma acepção estrita do tema. Isto porque, a informatização mencionada não pode limitar-se à transposição dos atos processuais para o mundo eletrônico – indiscutivelmente um avanço ímpar – conquanto ela engloba inúmeros outros fatores inerentes à administração da máquina judiciária.

A informatização do judiciário é um fenômeno que precede o processo eletrônico e lhe é muito mais ampla e atemporal. Neste sentido, Alexandre Atheniense (2010, p. 47-68) aponta para a Lei 9.800/99 como marco legislativo naquele sentido, quando se admitiu o peticionamento através de *fac símile*, ainda que com posterior juntada aos autos dos originais. Aponta, ainda, o citado autor, para os diversos institutos legais posteriores a esta norma e precedentes àquele instituto, com intuito claro de inserir não apenas o processo, mas a própria máquina estatal, na nova ordem tecnológica.

---

[7] Obtido por meio eletrônico. Disponível em <http://www.viajus.com.br/viajus.php?pagina=artigos&id=1261&idAreaSel=21&seeArt=yes> Acesso em: 26 out. 2011

De fato, informatização do judiciário como significado de processo eletrônico é um conceito restritivo, quando se observa que até o ano de 2008 nem todas as comarcas do Estado da Bahia dispunham de acesso sistema informatizado do próprio Pode Judiciário[8], requisito básico para aferição da produtividade de juízes e servidores, e para acompanhamento dos processos pelas partes e advogados.

Com efeito, informatizar o judiciário, em verdade, significa a adoção, com contínua atualização, de um conjunto de medidas que possam dotar as unidades jurisdicionais de ferramentas computacionais básicas – tanto de *hardware*: como computadores, impressoras, copiadores, *scanners*, etc., quanto de *software*: programas e sistemas para controle processual, acesso à internet, peticionamento eletrônico, emissão de certidões, arquivos de jurisprudência, etc., – e capacitar magistrados e serventuários para operá-las.

Destarte, neste sentido, os reflexos da informatização do judiciário serão de ordem interna e externa. Internamente, o próprio poder estará apto a uma prestação jurisdicional eficiente e eficaz, deixando de ser uma máquina de entraves burocráticos, para, de fato, promover a justiça de modo célere e correto a que tanto se propõe. Externamente, porque uma demanda processual rápida e eficaz implicará não apenas em satisfação da população e usuários da justiça, mas também, e principalmente, na redução de gastos públicos com pessoal e suprimentos desnecessários.

O jornalista Robson Pereira, em artigo escrito para o site Consultor Jurídico afirma que se fosse criada uma associação representativa dos usuários da justiça, a mesma contaria com aproximadamente vinte milhões de associados, e seria a maior entidade do país. E com tal número de associados, a fictícia associação teria respaldo e voz altiva para exigir mais rapidez, qualidade e menor custo na tramitação dos processos, argumentando que estes três requisitos, aparentemente inconciliáveis, são fáceis de serem postos em prática, desde que o Direito: "utilize-se do desenvolvimento tecnológico, para alcançar e igualar-se e alcance um estágio de modernização compatível àquele já conquistado por praticamente todos os demais segmentos da sociedade".[9] E vai além:

> A solução para a aparente divergência — muito mais de método do que de princípio — pode estar em um CD, com um manual de instrução e a versão 1.0 de uma ferramenta, entregue pelo CNJ na semana passada aos 90 tribunais brasileiros. O software, conhecido como Processo Judicial Eletrônico ou PJE, é um sistema de automação exclusivamente desenvolvido para atender o Judiciário brasileiro. Na

[8] Obtido por meio eletrônico. Disponível em < http://www5.tjba.jus.br/corregedoria/images/pdf/provimento200811.pdf>. Acesso em 26 out. 2011.
[9] Obtido por meio eletrônico. Disponível em <http://www.conjur.com.br/2011-jul-04/letras-juricias-oracao-aos-mocos-processo-judicial-eletronico> Acesso em: 21 out. 2011

> prática, vai transportar para o ambiente digital rotinas hoje realizadas no ambiente físico, eliminando várias tarefas processuais e, consequentemente, tornando mais ágil a tramitação dos processos judiciais. É a Justiça 2.0.
>
> Estima-se que os "atos meramente burocráticos e ordinatórios" chegam a consumir 70% do tempo gasto na tramitação de um processo. Assim, qualquer contribuição tecnológica capaz de cortar tamanho desperdício terá reflexo significativo também no PIB processual: a soma de todos os custos envolvidos, desde o ajuizamento até o trânsito em julgado. Liberado da enfadonha e pouco produtiva burocracia processual, acredita-se que o julgador poderá dedicar-se àquilo que a sociedade espera dele: Justiça mais rápida e com qualidade.
>
> O processo eletrônico traz algumas mudanças significativas na gestão dos tribunais. No método antigo — o atual — um processo permanece mais tempo na secretaria do que no próprio gabinete. Sem a camisa de força dos atos processuais e burocráticos, essa situação se inverte, com ganhos significativos na atividade jurisdicional. Some a isso o fato de o processo permanecer ao alcance dos operadores de Direito 24 horas por dia, sete dias por semana, onde quer que estejam os seus personagens principais.
>
> Claro que dúvidas surgirão e que não serão poucos aqueles que, diante do novo, sempre manifestarão a preferência pelo conforto oferecido pelo método tradicional. Mas quem já passou por isso sabe que, assim como é impossível deter a tecnologia, mais dia menos dia se pegará perguntando como conseguiu passar tanto tempo sem ela. Aos poucos, todas as peças vão se encaixando e o mosaico fica completo. Por que não com o Direito? Por que não com a Justiça?

Neste sentido, o processo eletrônico disciplinado pela Lei 11.419/06, em qualquer dos formatos ou versões que se apresente, parece significar a tradução de informatização do judiciário, mas não pode, nem deve limitar-se a isto, eis que a prestação jurisdicional vai além da tramitação processual célere e econômica, envolvendo outros serviços.

A título exemplificativo tome-se, por exemplo, a disponibilização do serviço de emissão de certidões negativas *on line*. Trata-se de atividade outrora extenuante ao cidadão, posto que prescindisse requerimento prévio, pagamento do emolumento respectivo, para obtenção efetiva dias após o inicio do trâmite. Contudo, a possibilidade de requerer e até mesmo expedir – em casos de inexistência de processos judiciais em nome da parte – desafoga os serventuários que faziam tal atendimento e impressão; facilita a vida do cidadão que não mais terá de se deslocar ao mesmo local uma ou duas vezes.[10]

Esta simples atividade só é possível graças à informatização do órgão judicante expedidor do documento, que proveu o seu sítio na internet de mecanismos hábeis a receber o requerimento e expedir a certidão solicitada.

Noutro giro, a informatização do judiciário, de modo amplo, deve permitir ao usuário da máquina judiciário – cidadão, advogado, membro do Ministério Público, auxiliares da Justiça,

[10] Obtido por meio eletrônico em www.tjba.jus.br e www.trf1.jus.br . Acesso em: 21 out. 2011

e os próprios magistrados – as informações atualizadas dos processos a que os mesmos se encontrem vinculados.

O tema, inclusive, foi alvo de decisão do STJ que assim noticiou[11]:

> As informações veiculadas pelos tribunais em suas páginas de andamento processual na internet, após o advento da Lei n. 11.419/06, devem ser consideradas oficiais, e eventual equívoco ou omissão não pode prejudicar a parte. Este foi o entendimento reafirmado pela Terceira Turma do Superior Tribunal de Justiça (STJ) ao julgar recurso de duas empresas de engenharia e uma companhia de participações que pediam reabertura de prazo para responder a uma ação.
>
> No caso, foi proposta ação declaratória de nulidade de cláusulas contratuais contra as empresas, que foram citadas por correio. De acordo com o artigo 241, inciso I, do Código de Processo Civil, o prazo para responder começaria a transcorrer apenas após a juntada do último aviso de recebimento.
>
> Entretanto, por omissão do cartório judicial, não foi publicada no site do Tribunal de Justiça do Rio Grande do Sul (TJRS) informação sobre a juntada aos autos do aviso de recebimento da última carta de citação e nenhum dos réus respondeu à ação.
>
> Para evitar o reconhecimento da revelia, as empresas se manifestaram nos autos esclarecendo o ocorrido e pedindo a reabertura de prazo para a resposta, mas o magistrado e o Tribunal gaúcho não reconheceram a configuração de justa causa. O relator do recurso especial, ministro Paulo de Tarso Sanseverino, afirmou que compartilhava do entendimento pacificado anteriormente no STJ de que as informações processuais constantes nos sites dos tribunais teriam caráter meramente informativo e que, por não serem oficiais, não serviriam de justa causa para reabertura de prazos. No entanto, o ministro decidiu rever sua posição em função da importância adquirida pelo processo eletrônico.
>
> "Convenci-me de que, no atual panorama jurídico e tecnológico, é imprescindível que se atribua confiabilidade às informações processuais que são prestadas pela página oficial dos tribunais. Não parece razoável que o conteúdo de acompanhamento processual eletrônico dos tribunais não possa ser digno de plena confiabilidade por quem o consulta diariamente. Mesmo apresentando um caráter informativo, deve ter um mínimo de credibilidade", ponderou o relator.
>
> A interpretação de que as informações dos sites não têm caráter oficial foi adotada em vários julgamentos do STJ, inclusive pela Corte Especial, mas na maior parte dos casos antes da Lei n. 11.419/06. Esse entendimento ainda prevaleceu por algum tempo após a mudança legislativa, até que a Terceira Turma, tendo em vista a nova lei, decidiu alterar sua posição sobre o tema ao julgar o Recurso Especial 1.186.276. Sanseverino observou que a disponibilização eletrônica de informações sobre os processos facilita o trabalho dos advogados e o acesso das próprias partes ao conteúdo de andamento do processo. Para o Ministro, se as informações veiculadas não são confiáveis, a finalidade da inovação tecnológica acaba por ser desvirtuada e a informação prestada erroneamente torna-se mais danosa do que a simples ausência de informação.
>
> O relator lembrou ainda que, "na esteira da evolução que a virtualização de processos representou, a confiança nas informações processuais fornecidas por meio eletrônico implica maior agilidade no trabalho desenvolvido pelos cartórios e pelas secretarias judiciais, ensejando maior observância ao princípio da eficiência da administração e, por conseguinte, ao princípio da celeridade processual". Desse modo, a Turma reconheceu a configuração de justa causa e determinou a reabertura do prazo para apresentação de resposta. A decisão foi unânime.

[11] STJ. Obtido por meio eletrônico. Disponível em < http://www.stj.jus.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=102402> Acesso em: 29 jun. 2011

Observe-se que o próprio Tribunal Superior também decidiu:

> PROCESSUAL CIVIL. AGRAVO REGIMENTAL. AGRAVO DE INSTRUMENTO CONTRA DECISÃO QUE INADMITIU RECURSO ESPECIAL NA ORIGEM. COMPROVAÇÃO DE SUSPENSÃO DE PRAZO PROCESSUAL POR INTERMÉDIO DE DOCUMENTO EXTRAÍDO DA INTERNET. POSSIBILIDADE.
>
> 1. As cópias de atos relativos à suspensão dos prazos processuais, no Tribunal de origem, obtidas a partir de sítios eletrônicos da Justiça, contendo identificação da procedência do documento, ou seja, endereço eletrônico de origem e data de reprodução no rodapé da página eletrônica, e cuja veracidade é facilmente verificável, juntadas no instante da interposição do recurso especial, possuem os requisitos necessários para caracterizar prova idônea, podendo ser admitidas como documentos hábeis para demonstrar a tempestividade do recurso, salvo impugnação fundamentada da parte contrária.
>
> 2. Modificação da jurisprudência da Corte Especial.
>
> 3. Agravo regimental provido.
>
> (AgRg no Ag 1251998/SP, Rel. Ministro LUIS FELIPE SALOMÃO, CORTE ESPECIAL, julgado em 15/09/2010, DJe 19/11/2010)

Para atender, então, a este tipo de demanda, sem sombras de dúvidas, os Tribunais devem possuir uma infraestrutura não apenas técnica para suportar as requisições inerentes da atividade que lhe é exigida; mas também humana, devidamente capacitada, para alimentar os sistemas de informação e operar o maquinário computacional necessário.

Nota-se, pois, que os reflexos da informatização do judiciário não podem limitar-se, ainda que de suma importância e significado, ao marco e às disposições do processo eletrônico disciplinado na Lei 11.419, porquanto compreende ainda a capacidade técnica e pessoal de evoluir aquele trabalho desenvolvido pelo Estado.

2.3 A LEI 11.419 DE 19 DE DEZEMBRO DE 2006

Nos seus enxutos vinte e dois artigos, a lei citada, considerada como marco da informatização judiciária por alguns doutrinadores, apresentou ao ordenamento jurídico pátrio uma nova forma de forma de apresentação de lides ao judiciário: a digital.

O fruto da lei é o processo eletrônico, definido em seu artigo primeiro, como visto no inicio deste capítulo, como a prática por meio eletrônico de todos os atos processuais conhecidos e realizados antes em meio físico, ou seja, é a transposição, para o mundo digital, do processo enquanto "relação jurídica processual em movimento" (KLIPPEL; BASTOS. 2011, p. 181).

Sem dúvidas, o conteúdo deste diploma legal representa a mais significativa alteração processual havida no país, como reflexo, não apenas dos efeitos da Era Digital sobre a sociedade, mas, principalmente, dos anseios da opinião pública carente de mais celeridade nas decisões judiciais nos litígios em exame.

Com vistas a proporcionar esta tão buscada efetividade jurisdicional, a lei que institui o Processo Eletrônico no país valeu-se do principio constitucional da razoável duração do processo, erigido no inciso LXXVIII, do artigo 5º, da Constituição Federal de 1988, como seu pilar de sustentação.

Apesar de inédita a lei, o princípio que lhe dá substrato não é tão inédito assim, posto que a razoável duração do processo pode, facilmente, ser retirada das garantias de acesso à justiça, ou mesmo das assertivas processuais de celeridade.

Nos dizeres de Rodrigo Klippel e Antonio Adonias Bastos (2011, p. 78):

> O principio da duração razão razoável do processo foi inserido pela EC 45/04 e corresponde aos reclames da sociedade por um processo mais ágil e que entregue seu produto em tempo hábil às partes, evitando o que Andrea Proto Pisani chama de dano marginal, ou seja, o dano que a própria demora do processo traz ai direito das partes.
>
> Embora se possa considerar que a duração razoável do processo já era uma exigência contida no conteúdo jurídico do principio do acesso à justiça, é importante que o legislador constitucional tenha especificado essa cláusula, para o fim de que não reste qualquer dúvida acerca de sua essencialidade para a garantia do direito de acesso à ordem jurídica justa.

Não basta, entretanto, que a entrega da tutela seja célere, mas justa e garantidora dos direitos fundamentais das partes. Na lição de Daniel Amorim Assumpção Neves (2010, p. 72-73):

> Deve ser lembrado que a celeridade nem sempre é possível, como também nem sempre é saudável para a qualidade da prestação jurisdicional. O legislador **não pode sacrificar direitos fundamentais das partes** visando somente a obtenção da celeridade processual, sob pena de criar situações ilegais e extremamente injustas. (grifo do autor).

Isto porque a celeridade não pode ser apenas o norte do judiciário, mas sim uma dos seus objetivos, pois rapidez sem qualidade ou em desrespeito a outras normas não refletirá um estado democrático de direito.

Observa-se, contudo, que o viés da celeridade que tanto se almeja parece ser aquele em que o judiciário, não mais consumindo tempo com trâmites burocráticos, utilize, ou melhor, dê ao magistrado e a atividade judicante não apenas e tão somente horas livres para poder apreciarem mais e mais processos, mas sim garantir a qualidade no exercício do judiciário.

É verdade, igualmente, que o clamor social por uma justiça onde a entrega da tutela pretendida não leve anos para ser efetivada, possui clara conotação e pendor para celeridade do que pela qualidade dos julgados em si – preocupação esta, muito mais dos operadores do direito, que, de um modo geral temem que esta justiça apressada venha a ser pobre em qualidade jurídica e, muito mais perigoso, violadora de outros direitos e garantias fundamentais.

Sem dúvidas, há inúmeros fatores que podem levar a lide a uma longa duração, desde o comportamento dos litigantes e seus advogados, até mesmo a própria complexidade da causa. E não é que o legislador processual não tenha pensado em soluções para imprimir maior rapidez às demandas. Para tanto, ao longo dos últimos dez anos, o CPC sofreu alterações significativas nesta intenção, tais como o julgamento *prima facie* previsto no art. 285-A; a lei 9.099/95 que instituiu os Juizados Especiais; a súmula impeditiva de recursos; a própria comunicação processual por via eletrônica do artigo 154, §2º; o julgamento antecipado de mérito do artigo 330 o processo sincrético, com a fase de cumprimento da sentença, entre outros. (NEVES, Daniel. 2010, p. 74).

Não obstante os esforços legislativos processuais neste sentido, seja por falta de infraestrutura física ou de pessoal, ou razões outras de ordem não jurídica, o fato é que, significativamente, não se verificaram na prática a tão buscada celeridade.

O surgimento da Lei 11.419/06, então, parece, inicialmente, servir ao propósito de permitir maior rapidez na efetivação da tutela processual perseguida em juízo. Com efeito, transpor atos físicos para a realidade imaterial da internet, tem como finalidade mor a celeridade, claro, mas acaba também por trazer significativas economias para o judiciário.

A novidade jurídica, fez surgir uma pluralidade de sistemas processuais – cujas conseqüências serão alvo de considerações mais adiante nesta pesquisa – para este tipo de procedimento, a exemplo do PROJUDI e e-Proc, na vanguarda da implementação da nova legislação, trazendo uma dinâmica processual, inicialmente, muito mais célere e cômoda para os usuários.

Com eles, desaparecia a figura da distribuição, autuação e numeração de páginas processuais; assim como a ida do advogado ou do membro do Ministério Público para apresentação de suas peças iniciais; carga de autos – e sumiço dos mesmos – também se tornaram figuras do passado. Então, diante de tantas vantagens, como não ser a favor do processo eletrônico? Impossível. E estava comprovado que o espírito do legislador havia sido compreendido.

Celeridade e razoável duração do processo haviam sido cooptadas pela Lei 11.419, trazendo o direito processual brasileiro, assim como a atividade judicante, para o século XXI.

Ao se ler o conteúdo de apresentação do PJe pelo CNJ, fica clara a noção de que os objetivos da implementação deste sistema – que pretende unificar os sistemas de processo eletrônico no país – pelo órgão é celeridade e redução de gastos, como ora se vê:

> O processo judicial eletrônico, tal como o processo judicial tradicional, em papel, é um instrumento utilizado para chegar a um fim: a decisão judicial definitiva capaz de resolver um conflito. A grande diferença entre um e outro é que o eletrônico tem a **potencialidade** de reduzir o tempo para se chegar à decisão.
>
> A redução do tempo pode ocorrer de várias maneiras: extinguindo atividades antes existentes e desnecessárias em um cenário de processo eletrônico, tais como juntadas de petições, baixa de agravos de instrumento, juntadas de decisões proferidas por Cortes especiais ou pelo Supremo Tribunal Federal; suprimindo a própria necessidade de formação de autos de agravo em razão da disponibilidade inerente do processo eletrônico; eliminando a necessidade de contagens e prestação de informações gerenciais para órgãos de controle tais como as corregedorias e os conselhos; atribuindo ao computador tarefas repetitivas antes executadas por pessoas – e, portanto, propensas a erros –, tais como a contagem de prazos processuais e prescricionais; otimizando o próprio trabalho nos processos judiciais, acrescentando funcionalidades antes inexistentes capazes de agilizar a apreciação de pedidos e peças processuais; deslocando a força de trabalho dedicada às atividades suprimidas para as remanescentes, aumentando a força de trabalho na área fim; automatizando passos que antes precisavam de uma intervenção humana; permitindo a execução de tarefas de forma paralela ou simultânea por várias pessoas.
>
> Essas medidas têm como resultado a redução do tempo de atividades acessórias ao processo judicial, permitindo que sejam praticados mais atos tendentes à solução do processo e, portanto, agilizando a solução dos conflitos.
>
> Uma comparação razoável seria imaginar o Judiciário como um veículo que tem que transportar uma carga de um ponto a outro. A carga seria a decisão judicial, o motor, os magistrados e servidores; e o tempo e o combustível, o custo do processo judicial. Em um processo tradicional, o Judiciário seria um caminhão pesado, gastando mais combustível e levando mais tempo para chegar ao destino porque seu motor tem que mover, além da carga "útil", a carga do próprio caminhão. **No processo eletrônico, o Judiciário seria um veículo de passeio, com um motor mais leve, que consegue levar a carga ao destino mais rápido e com um custo menor.**[12]
>
> Embora seja apenas um meio, o processo eletrônico traz algumas mudanças significativas na gestão dos tribunais. Há uma verdadeira revolução na forma de trabalhar o processo judicial. A essa revolução deve corresponder uma revisão das rotinas e práticas tradicionais, porquanto o que havia antes deve adaptar-se à nova realidade.
>
> A primeira grande mudança é relativa à guarda do processo.
>
> No regime tradicional, o processo judicial fica nas mãos e sob a responsabilidade do diretor de secretaria, do escrivão, do magistrado e dos advogados. Com o processo eletrônico, essa responsabilidade recai sobre quem tem a atribuição de guardar os dados da instituição – a área de tecnologia da informação. O processo eletrônico passa a poder estar em todos os lugares, mas essa facilidade vem acompanhada da necessidade de ele não estar em qualquer lugar, mas apenas naqueles lugares apropriados – a tela do magistrado, do servidor, dos advogados e das partes. Isso faz com que a área de tecnologia da informação se torne **estratégica**, pareando-se, do

[12] (grifo nosso)

> ponto de vista organizacional, com as atividades das secretarias e dos cartórios judiciais.
>
> A segunda grande mudança deve ocorrer na distribuição do trabalho em um órgão judiciário. Em varas de primeiro grau e em órgãos que processam feitos originários, boa parte do tempo do processo é despendido na secretaria, para a realização de atos processuais determinados pelos magistrados. **Suprimidas as atividades mecânicas, haverá uma atrofia de secretarias e cartórios, ao que corresponderá uma redução do tempo necessário para que um processo volte aos gabinetes, que se verão repletos de processos em um curto espaço de tempo. Há a necessidade, portanto, de deslocar a força de trabalho das secretarias e cartórios para os gabinetes dos magistrados. Essa é uma mudança que demonstra de forma cristalina como o processo eletrônico pode levar a uma melhoria na atividade jurisdicional, já que é lá, no gabinete, que são produzidos os atos que justificam sua existência.**[13]
>
> O terceiro grande impacto ocorre na cultura estabelecida quanto à tramitação do processo judicial. Embora ainda não tenham ocorrido mudanças legislativas a respeito, é certo que o processo eletrônico, em razão de sua ubiquidade, dispensa práticas até hoje justificáveis e presentes nos códigos de processo, como a obrigatoriedade de formação de instrumento em recursos. Mais que isso. Não há mais a necessidade de uma **tramitação linear** do processo, o qual, podendo estar em vários lugares ao mesmo tempo, retira qualquer justificativa para a concessão de prazos em dobro em determinadas situações. Não bastasse isso, como se verá adiante, o PJe inova substancialmente a própria forma de trabalho utilizada.
>
> Finalmente, há o impacto do funcionamento ininterrupto do Judiciário, com possibilidade de peticionamento 24 horas, 7 dias por semana, permitindo uma melhor gerência de trabalho por parte dos atores externos e internos. Além disso, a disponibilidade possibilita que se trabalhe de qualquer lugar do mundo, a qualquer hora, o que também causará gigantescas modificações na forma como lidamos com o processo.[14]

Não há dúvidas, pois, que o espírito do legislador foi respeitado, e, de fato, por fazer desaparecerem atos processuais que não mais fazem sentido à prática eletrônica, tais como, distribuição, autuação, carga de autos, publicação em imprensa oficial, há clara redução do tempo consumido para tais atos, bem como custos, a exemplo de papel e impressão.

A atrofia apontada pelo CNJ acima, em secretarias e cartórios, já ocorre em unidades com sistemas de processo eletrônico implantados. Todavia, o deslocamento de pessoal para os gabinetes, para a produção dos atos que justificam a existência do processo, tais como decisões interlocutórias, sentenças e despachos de mero expediente parece ser uma prática ainda a ser alcançada.

Neste ponto, então, o aparente sentido de celeridade perde força, conquanto – e aí crível a afirmação de Daniel Amorim Assumpção Neves (2010, p. 73) ao afirmar que a morosidade do judiciário possui razões que são estranhas ao processo civil – quando não há o deslocamento

---

[13] (idem)
[14] CNJ. Obtido por meio eletrônico. Disponível em <http://www.cnj.jus.br/programas-de-a-a-z/sistemas> Acesso em: 26 out. 2011

de pessoal da anterior atividade burocrática, atrofiada pela desnecessidade do meio eletrônico, para que realizem os atos fundamentais nos gabinetes, haverá paralisação dos feitos da mesma forma, conquanto haverá um afunilamento na pessoa do magistrado, que, decerto, não terá condições de atender aquele volume sozinho.

No Estado da Bahia, em toda a capital e em 33 (trinta e três) comarcas do interior,[15] o sistema PROJUDI encontra-se em funcionamento, mas ainda há disparidades que fazem crer inexistir – ou ser mal administrado/utilizado – esse fluxo migratório de pessoal para compor o trabalho dos gabinetes.

Apenas a título exemplificativo, tome-se o quadro abaixo, no qual dois processos iniciados e em tramitação no sistema PROJUDI, nos quais a autora deste trabalho atua como advogada da parte autora, com competência de dois diferentes Juizados Especiais de Salvador. A simples descrição dos andamentos, em cada um dos feitos, demonstra que o problema da celeridade, de fato, pode não ser resolvido com a simples implantação do Processo Eletrônico.

Observe-se que não há justificativa, aparente ou plausível, para que a entrega da tutela jurisdicional de primeiro grau possa consumir quantidades de dias tão díspares em feitos de menor complexidade como são aqueles apreciados pelos Juizados Especiais.

Quadro 1 – Processos do PROJUDI em Salvador/BA[16].

Processo 032.2009.006.266-5 (958 dias em tramitação)	**Processo 032.2011.106.791-7** (61 dias em tramitação)
ANDAMENTOS	
12/03/2009 – ajuizamento, distribuição e designação de audiência CIJ.	**26/08/2011** – ajuizamento, distribuição e designação e audiência CIJ.
01/07/09 – audiência CIJ realizada: autos conclusos para decisão sobre revelia.	**19/10/2011** – audiência CIJ realizada: autos conclusos para sentença.
22/07/09 – decisão decreta da revelia e ordena designação de audiência de instrução.	**24/10/2011** – sentença proferida.
24/07/09 – secretaria marca audiência de instrução.	
30/03/2010 – audiência de instrução não realizada por força da greve dos servidores Judiciário.	
31/05/10 – secretaria certifica não realização da audiência.	
19/07/10 – secretaria marca nova data de audiência.	
13/09/2010 – audiência de instrução realizada: autos conclusos para sentença.	
22/06/2011 – sentença proferida	
TEMPO DE ENTREGA DA TUTELA JURISDICIONAL DE 1º GRAU	
830 DIAS	**58 DIAS**

[15] TJBA. Disponível em: <https://projudi.tjba.jus.br/projudi/> e <http://www5.tjba.jus.br/corregedoria/images/pdf/01_juizadosinterior.pdf> Acesso em: 27 out. 2011

[16] Fonte: TJBA. Disponível em: <https://projudi.tjba.jus.br/projudi/> Acesso em: 26 out. 2011.

Vê-se, pois, que fatores alheios ao processo eletrônico em si devem ser considerados para que se justifique um comparativo deste tipo. Isto é, a simples transposição dos autos e atos para o meio eletrônico, pura e simplesmente, não tem o condão de alavancar o judiciário em um curto espaço de tempo.

É preciso, como de fato apontou o CNJ, que o recurso pessoal por trás do aparato eletrônico seja, e esteja, apto a dar vazão ao volume de atos decorrente da eliminação de outros tantos trazidos pela inovação legal.

As unidades judiciais que já conseguiram implementar o uso diuturno do processo eletrônico, e que, ao mesmo tempo, permitiram o deslocamento de pessoal retirado da atrofia dos atos não mais necessários por força da nova lei, tem – e já demonstram – que um processo com sentença de mérito proferida em primeiro grau em menos de sessenta dias é o mais próximo do ideal de celeridade e razoável duração do processo que este país jamais viu.

2.4 PROCEDIMENTO NO PROCESSO ELETRÔNICO

A Lei 11.419 minudenciou quase todas as ocorrências necessárias ao procedimento no processo eletrônico, desde o envio de petições, a forma e prazo para citações e intimações eletrônicas.

Fez surgir, ainda, um estreitamento dos conhecimentos da ciência da informática com o direito – já experimentada pelos ramos de direito material, porém muito mais vivida por especialistas em determinadas áreas, como propriedade intelectual e comércio exterior – no âmbito processual. E neste ponto, diga-se que, o processo enquanto instrumento, como ferramenta indispensável ao acesso à justiça, diz respeito a um número muito mais significativo de operadores.

Neste aspecto, este estreitamento trouxe, como tudo que é novo e desconhecido, uma imensa reticência por parte daqueles advogados, magistrados, serventuários e jurisdicionados que não possuíam conhecimento, ou mesmo não tinham experiência, com o mundo dos computadores, periféricos (impressoras e scanners), internet, *e-mail*, etc. E até mesmo por parte daqueles que, apesar de conhecerem e utilizarem dos mesmos, viram-se diante de novos conhecimentos necessários à simples apresentação de uma petição inicial.

Isto se deve ao fato de que, ao determinar em seu artigo 14 que: "**Os sistemas a serem desenvolvidos pelos órgãos do Poder Judiciário** deverão usar, preferencialmente, programas com código aberto, acessíveis ininterruptamente por meio da rede mundial de computadores, **priorizando-se a sua padronização**." [17] abriu um vasta implantação de sistemas diferenciados por todo o país, como os mais diversos requisitos de informática.

Do inicio da vigência da Lei para cá, na prática, cada tribunal adotou um sistema de informatizado diferente, tanto para a prática de atos eletrônicos, quanto para a própria implantação do processo eletrônico em si.

Antes acostumados ao papel e tinta, o mundo jurídico viu-se obrigado a compreender o significado de e-mail, portal dedicado, assinatura digital, certificado digital, ICP-Brasil, arquivos de extensão pdf, scaneamento, kilobites, megabytes, digitalização, dentre tantos outros termos inerentes à ciência da computação, agora inseridos e necessários aos usuários do judiciário.

Em linhas gerais, o procedimento no processo eletrônico, independentemente do sistema informatizado adotado, é relativamente simples, exigindo da pessoa que vai manuseá-lo alguns conhecimentos de informática, e da máquina onde serão acessados programas e requisitos computacionais específicos.

Previamente, o usuário (advogado, parte ou membro do Ministério Público) deve estar cadastrado junto ao judiciário do qual se pretende a tutela. Os cadastros são feitos parte na internet, no portal daquela autoridade judicante, parte presencialmente, onde são inseridos e conferidos os dados de identificação do usuário, a quem se concede um código e senha, cujo uso em conjunto comporá a chamada assinatura digital.

Esse cadastramento é necessário, não apenas para que o usuário utilize o sistema disponibilizado pela aquela autoridade judiciária, mas também para que o mesmo seja citado e/ou intimado, posteriormente, dos atos processuais praticados. De posse da assinatura digital, o usuário poderá acessar o portal utilizado por aquela autoridade judiciária, dando inicio a novos processos ou mesmo acompanhando os ali já existentes.

Via de regra, as peças processuais são arquivos de computador, com um limite máximo de tamanho (pré estipulado na unidade de medida computacional denominada megabytes) – em sua maioria no formato pdf, a fim de garantir maior segurança, já que esta modalidade de arquivo digital não admite inserção/alteração de dados posterior – que são inseridos nos

[17] (grifo nosso)

respectivos sistemas do processo eletrônico, depois de conferidos pela assinatura digital, ou por um certificado digital, melhor apresentados e definidos no item 3.3 do capítulo subsequente.

Também os atos praticados por serventuários e magistrados seguem os requisitos elencados até aqui, sendo que o protocolo das peças recebe código numérico de validade e o processo não mais possui páginas, e sim eventos ou itens, com números e ordenação temporal.

As intimações possuem regra própria, definida no artigo 4º da lei 11.419/06, podendo ou não o usuário receber comunicação prévia da mesma via e-mail, avisando-lhe que há uma intimação para ele no portal dedicado. A leitura do e-mail não inicia a contagem dos prazos, que se dá a partir do momento em que o usuário abre a intimação no portal dedicado, ou, acaso não aberta, automaticamente após dez dias da disponibilização da mesma no sistema.

Os prazos podem ser cumpridos até as 24h (vinte e quatro horas) do último dia de seu vencimento. E não sendo possível o seu protocolo, com a inserção no portal, por motivos de inoperância do sistema, o próprio normativo legal determina que o ato pode ser praticado no primeiro dia útil subsequente.

Sobre este aspecto, Samuel Cersósimo levanta a problemática da prova da inoperância do sistema para os advogados:

> A Lei de Informatização do Processo Judicial (Lei 11.419/06) foi competente ao prever a possibilidade do sistema de processo eletrônico ficar "fora do ar" por qualquer motivo técnico logo no momento em que o advogado tenta peticionar eletronicamente. Para esta hipótese, em se tratando de petição para cumprir prazo fatal, a lei determina que o prazo seja devolvido para o próximo dia útil seguinte à resolução do problema. Assim é o texto legal:
>
> Art. 10. A distribuição da petição inicial e a juntada da contestação, dos recursos e das petições em geral, todos em formato digital, nos autos de processo eletrônico, podem ser feitas diretamente pelos advogados públicos e privados, sem necessidade da intervenção do cartório ou secretaria judicial, situação em que a autuação deverá se dar de forma automática, fornecendo-se recibo eletrônico de protocolo.
>
> § 1o Quando o ato processual tiver que ser praticado em determinado prazo, por meio de petição eletrônica, serão considerados tempestivos os efetivados até as 24 (vinte e quatro) horas do último dia.
>
> § 2o No caso do § 1o deste artigo, se o Sistema do Poder Judiciário se tornar indisponível por motivo técnico, o prazo fica automaticamente prorrogado para o primeiro dia útil seguinte à resolução do problema.
>
> Fonte: Lei 11.419/2006

> Essa interpretação foi recentemente confirmada pelo Tribunal Superior do Trabalho, no **RR-150000-08.2008.5.18.0001**.
>
> O que chamou atenção foi a interpretação que tentou dar ao dispositivo a decisão anterior do TRT, ao declarar que "a indisponibilidade do sistema prorroga o prazo para prática do ato processual apenas se ele 'tiver que se ser praticado em determinado prazo, por meio de petição eletrônica', como diz a lei (art. 10, § 1º, da Lei nº 11.419/09)". Logo. quis entender que o prazo não poderia ser devolvido, já que a petição não tinha que ser apresentada obrigatoriamente em meio eletrônico, podendo ter sido apresentada nos moldes convencionais. Quando o §1º se refere ao "ato processual [ter] que ser praticado em determinado prazo, por meio de petição eletrônica,", ele apenas quer chamar atenção à questão do prazo, e não a uma suposta obrigatoriedade de o peticionamento ser eletrônico. A lei em momento algum trata da obrigatoriedade ou não do uso do meio eletrônico para o peticionamento.
>
> A menção ao prazo se justifica porque tanto o §1º como o §2º se referem a uma elasticidade do prazo fatal. Logo, não se aplicam a um ato que não esteja no último dia do prazo, tampouco a atos não sujeitos a prazo algum. Daí a referência no texto. A conjunção "..., por meio de petição eletrônica, ..." é meramente explicativa e, inclusive, desnecessária.
>
> O relator do Recurso de Revista, Ministro Alberto Luiz Bresciani de Fontan Pereira (3ª Turma do TST), foi brilhante ao declarar que "não pode o julgador dar interpretação diversa da vontade do legislador". Felizmente, foi dele a palavra final.
> Fonte: Notícias do Tribunal Superior do Trabalho.
>
> Agora, deixo a seguinte provocação: Como o advogado provará que o problema técnico foi no sistema e não no seu computador? No caso do e-DOC, o TST divulga um providencial Histórico de Indisponibilidade do Sistema. E quanto aos tribunais que não fazem isso?
>
> Vale dizer que uma Ata Notarial no meio da noite, para provar que o sistema estava fora do ar está fora de cogitação[18]. (grifos do autor)

Parece que zelo e cautela são as primeiras respostas ao problema, posto que o cumprimento dos prazos pelo advogado seja uma obrigação processual e ética, logo não deve ser deixada para o último minuto do dia fatal par ao seu cumprimento.

Em um segundo momento, há de se destacar que o cumprimento do prazo, ainda que no processo eletrônico, pode ser feito por meio físico, como a ida à unidade receptora para protocolo presencial e posterior inserção no sistema.

---

[18] Obtido por meio eletrônico. Disponível em: <http://blog.viasdefato.com/2010/03/indisponibilidade-do-sistema-de.html> Acesso em: 27 out. 2011.

Há de se interpretar o espírito do legislador no sentido de que se crê seja obrigação – como de fato assim procedem STJ, TST e outros tribunais – da autoridade judiciária receptora informar a inoperância do sistema em determinados períodos, a fim de que o usuário não seja prejudicado por tal falha.

Por derradeiro, quanto à comprovação de que o sistema estava fora do ar ou inoperante, de fato, uma Ata Notarial, cuja produção à noite soa pouco crível – especialmente considerando-se o cenário cartorário do Estado da Bahia – poderá dar lugar ao mecanismo do *timestamp* ou carimbo do tempo, que vem a ser "um documento eletrônico emitido por uma parte confiável, que serve como evidência de que uma informação digital existia numa determinada data e hora no passado." [19] O uso do *timestamp,* contudo, ainda depende de aprovação pelo ICP-Brasil, mas sinaliza uma solução futura provável ao problema narrado.

Logo abaixo, a título ilustrativo, vê-se quadro disponibilizado pelo STJ com os períodos de indisponibilidade dos seus sistemas eletrônicos[20]:

Quadro 2 – Indisponibilidade dos sistemas eletrônicos do STJ:

Últimos registros incluídos

Aplicação	Período da indisponibilidade
Visualizador do Processo Eletrônico	26/08/2011 10:26 a 26/08/2011 12:10
Aplicação	**Período da indisponibilidade**
Diário de Justiça Eletrônico	26/08/2011 10:26 a 26/08/2011 12:10
Aplicação	**Período da indisponibilidade**
Peticionamento Eletrônico	26/08/2011 10:26 a 26/08/2011 12:10
Aplicação	**Período da indisponibilidade**
Visualizador do Processo Eletrônico	30/06/2011 16:59 a 30/06/2011 19:06
Aplicação	**Período da indisponibilidade**
Peticionamento Eletrônico	30/06/2011 16:59 a 30/06/2011 19:06
Aplicação	**Período da indisponibilidade**
Diário de Justiça Eletrônico	30/06/2011 16:59 a 30/06/2011 19:06
Aplicação	**Período da indisponibilidade**
Peticionamento Eletrônico	27/06/2011 12:00 a 28/06/2011 12:00
Aplicação	**Período da indisponibilidade**
Peticionamento Eletrônico	12/02/2011 14:30 a 12/02/2011 18:00

[19] Fonte: ITI. Disponível em: <www.iti.gov.br> Acesso em: 27 out.2011
[20] Fonte: STJ. Obtido por meio eletrônico. Disponível em: < https://ww2.stj.jus.br/out/in/indisponibilidade/lista/> Acesso em: 27 out. 2011

A descrição feita até aqui do procedimento no processo eletrônico, aparentemente dá margem a uma compreensão relativamente complexa do processo como todo, mas não o é. Na prática, com poucas lições aos afeitos ou não à informática, qualquer pessoa pode operar os sistemas existentes e disponíveis.

A problemática que se apresenta no procedimento do processo eletrônico cinge-se às diferenças entre os sistemas utilizados pelas unidades judiciárias de todo país, eis que, como a própria lei facultou a cada autoridade judicante a criação de sistemas informatizados para tal finalidade, permitiu, pois, em verdade a criação de diversos e diferentes procedimentos, que variam entre as esferas do judiciário, tanto de um Estado para outro, quanto de um grau de jurisdição para outro.

O que deveria ser uma facilidade, especialmente para aqueles advogados com atuação em diversos estados, uma série de dificuldades, não apenas pela necessidade de conhecimento dos diferentes tipos de sistemas, mas também pela diferença dos requisitos computacionais exigidos por cada tribunal, alguns deles incompatíveis entre si.

A pluralidade de sistemas cria, ainda, outro obstáculo: a não integração entre eles. Ou seja, como os portais são diferentes, muitas vezes, um recurso extraordinário para o STF, por exemplo, originado no sistema PROJUDI não segue automaticamente para aquele Pretório, porque o e-STF não aceita a codificação daquele sistema onde tramitou o processo eletrônico.

Neste impasse, vê-se, na prática, um retrocesso – e um ônus ao recorrente: a impressão das peças que compõem os autos eletrônicos do PROJUDI, para scaneamento, cadastro e remessa posterior no e-STF. Um contra senso à finalidade em si da Lei 11.419.

A padronização dos sistemas de processo eletrônico pretendida pelo CNJ, através do PJe, tem o louvável ideal de permitir a integração entre todos os tribunais, inclusive em graus de jurisdição diferentes. Além disso, representará significativa economia para os tribunais, considerando que o *software* foi criado em *open source*, ou seja, fonte livre, pelo próprio Conselho, sem custos de contratação de empresas de tecnologia da informação, nem com pagamento de licenças de uso.

Cumpre destacar, ainda, que o domínio de um sistema de processo judicial eletrônico único, facilitará o uso pelos operadores do direito, de sobremodo daqueles mais reticentes às inovações, já que esta habilidade, inclusive alvo do julgado abaixo transcrito, evitará que o desconhecimento do procedimento cause algum dano processual à parte:

> PROCESSO ELETRÔNICO. **ALEGAÇÃO DE ERRO NO PROCEDIMENTO DE DIGITALIZAÇÃO**, O QUE PROVOCOU A REQUISIÇÃO DOS AUTOS PARA CONFERÊNCIA. INVERACIDADE, CONTUDO, DA ALEGAÇÃO. INCIDENTE PROCESSUAL MANIFESTAMENTE INFUNDADO. ALEGAÇÃO DE **LITIGÂNCIA DE MÁ-FÉ CONFIGURADA**. MULTA DO ARTIGO 18 DO CÓDIGO DE PROCESSO CIVIL.
>
> PRINCÍPIO DA PROPORCIONALIDADE.
>
> 1.- Tendo sido alegado, no agravo regimental, que a ilegibilidade do protocolo aposto no recurso especial se deu por falha no procedimento de digitalização do feito, fez-se necessária a requisição de subida dos autos originais para conferência.
>
> 2.- Constatado que, ao contrário do alegado, não houve falha da digitalização, é de se concluir que a alegação infundada, havendo criado incidente processual, de que resultou a procrastinação do desfecho do caso nesta Corte, é nociva ao próprio processo de modernização processual por intermédio da necessária informatização, mas não se aplica ao caso a multa prevista no artigo 14, parágrafo único, do Código de Processo Civil, pois essa, só pode ser cominada na hipótese do inciso V do mesmo artigo, isto é, quando se tenha criado obstáculo ao cumprimento de um provimento judicial de natureza antecipatório ou final.
>
> 3.- Embargos de Declaração acolhidos unicamente para reduzir o valor da multa.
>
> (EDcl no AgRg no Ag 1329882/PR, Rel. Ministro SIDNEI BENETI, TERCEIRA TURMA, julgado em 28/06/2011, DJe 01/07/2011) [21]

Destarte, um procedimento unificado por um sistema padrão para todos os estados e tribunais do país, como tenciona o CNJ com o PJe, seguramente permitirá maior facilidade na compreensão do uso daquele sistema pelos usuários do mesmo, além, claro, de maior controle e aferição de validade e idoneidade não apenas do usuário, mas também dos documentos e provas por ele produzido dentro do processo eletrônico.

Digno de nota, ainda, que a proposta do PJe do CNJ parece interessar ao direito processual, no que pertine a sua integração com outros órgãos públicos, como é o caso da SRF. Decerto, estar-se-ia diante da possibilidade de troca de informações muito úteis ao andamento do feito eletrônico, tais como endereços do réu que se oculta, assim como localização de seus bens. Aliás, tais contribuições revestem-se de força argumentativa junto a qualquer advogado, ou parte, para fins de convencimento de uso de uma nova tecnologia, pois qualquer um deles que já tenha experimentado a demora na efetivação da tutela jurisdicional, por falta de tais informações, com certeza preferirá um processo eletrônico deste tipo.

No que tange ao objeto do estudo deste trabalho, a questão que o procedimento no processo eletrônico apresenta como de interesse à pesquisa, dizem respeito aos requisitos de segurança, autenticidade e validade, exigidas tanto dos usuários quanto da inserção de documentos.

---

[21] Grifos nosso.

Observe-se que as diferenças existentes entre cada um dos sistemas hoje utilizados no país, interferem naqueles requisitos, dando margem ao questionamento e mesmo à impugnação dos atos praticados sem conformidade com cada um dos sistemas existentes. Ou seja, compreender a condição de validade de cada um deles importará ao usuário o domínio intelectual imprescindível para contestar a prova documental nos autos eletrônicos, que, é o núcleo central da presente pesquisa.

3 A PROVA E SUA TEORIA GERAL.

"A acusação é apenas um infortúnio enquanto não verificada pela prova." [22], dizia Rui Barbosa, (1892, p. 113-114). A frase, dita em um dos discursos do citado autor, parece bem resumir a importância do instituto para o processo civil. É ela quem irá fundamentar o convencimento do magistrado acerca das razões fáticas que cada parte na lide aduz em seu favor.

Embora alguns autores afirmem que a prova não seria um direito fundamental, a melhor doutrina defende o contrário. Por ser decorrente do princípio constitucional do devido processo legal, a prova é, pois, direito fundamental, conquanto inservível o direito de acesso à justiça, se aos litigantes não fossem permitida a produção da prova em seu favor Destaca-se, ainda, que na qualidade de signatário do Pacto de San Jose[23], o Brasil confirma a prova como direito fundamental, e como tal possui todas as prerrogativas do regime das garantias constitucionais da Carta Magna.

Podem-se destacar, igualmente, os princípios informadores do direito probatório:

a) Princípio da Comunhão ou Princípio da Aquisição da Prova – no qual se observa que, uma vez deferida pelo magistrado a produção da prova requerida, a mesma insere-se no processo, integrando-o de tal modo que não mais pertencerá à parte que a requereu ou a realizou. Ou seja, não se pode falar de disponibilidade da prova após a sua produção;

b) Princípio do Livre Convencimento Motivado do Juiz – diferentemente dos sistemas positivo legal (onde a lei dá o peso da prova) e da livre convicção (no qual o magistrado escolhe a prova que lhe convencer, sem a obrigação da fundamentação desta escolha, o Brasil adotou oeste principio, através do qual o juiz, uma vez convencido da sua decisão, deve fundamentá-la, podendo ser a mesma, inclusive, contrária a algum elemento probante dos auto;

c) Vedação do uso da prova ilícita – o sistema jurídico brasileiro (art. 5º, LVI, da CF) não admite o uso de prova obtida por meio ilícito, a exemplo da escuta telefônica não autorizada por decisão judicial.

---

[22] Grifo nosso.
[23] Pacto de San Jose. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D0678.htm> Acesso em: 29 out. 2011

Relembre-se aqui que a prova ilícita é tão repudiada pelo ordenamento jurídico, que em recentes decisões, o STJ determinou a anulação de vários inquéritos policiais e ações penais decorrentes de operações realizadas pela Polícia Federal – estas de grande repercussão social e política – em função da ilicitude na colheita das provas que deram margem às mesmas:

> PENAL E PROCESSO PENAL. HABEAS CORPUS. **OPERAÇÃO SATIAGRAHA**.PARTICIPAÇÃO IRREGULAR, INDUVIDOSAMENTE COMPROVADA, DE DEZENAS DE FUNCIONÁRIOS DA AGÊNCIA BRASILEIRA DE INFORMAÇÃO (ABIN) E DE EX-SERVIDOR DO SNI, EM INVESTIGAÇÃO CONDUZIDA PELA POLÍCIA FEDERAL.
>
> MANIFESTO ABUSO DE PODER. IMPOSSIBILIDADE DE CONSIDERAR-SE A ATUAÇÃO EFETIVADA COMO HIPÓTESE EXCEPCIONALÍSSIMA, CAPAZ DE PERMITIR COMPARTILHAMENTO DE DADOS ENTRE ÓRGÃOS INTEGRANTES DO SISTEMA BRASILEIRO DE INTELIGÊNCIA. INEXISTÊNCIA DE PRECEITO LEGAL AUTORIZANDO-A. PATENTE A OCORRÊNCIA DE INTROMISSÃO ESTATAL, ABUSIVA E ILEGAL NA ESFERA DA VIDA PRIVADA, NO CASO CONCRETO. VIOLAÇÕES DA HONRA, DA IMAGEM E DA DIGNIDADE DA PESSOA HUMANA. INDEVIDA OBTENÇÃO DE PROVA ILÍCITA, PORQUANTO COLHIDA EM DESCONFORMIDADE COM PRECEITO LEGAL. AUSÊNCIA DE RAZOABILIDADE. AS NULIDADES VERIFICADAS NA FASE PRÉ-PROCESSUAL, E DEMONSTRADAS À EXAUSTÃO, CONTAMINAM FUTURA AÇÃO PENAL. INFRINGÊNCIA A DIVERSOS DISPOSITIVOS DE LEI. CONTRARIEDADE AOS PRINCÍPIOS DA LEGALIDADE, DA IMPARCIALIDADE E DO DEVIDO PROCESSO LEGAL INQUESTIONAVELMENTE CARACTERIZADA. A AUTORIDADE DO JUIZ ESTÁ DIRETAMENTE LIGADA À SUA INDEPENDÊNCIA AO JULGAR E À IMPARCIALIDADE.
>
> UMA DECISÃO JUDICIAL NÃO PODE SER DITADA POR CRITÉRIOS SUBJETIVOS, NORTEADA PELO ABUSO DE PODER OU DISTANCIADA DOS PARÂMETROS LEGAIS.
>
> ESSAS EXIGÊNCIAS DECORREM DOS PRINCÍPIOS DEMOCRÁTICOS E DOS DIREITOS E GARANTIAS INDIVIDUAIS INSCRITOS NA CONSTITUIÇÃO. NULIDADE DOS PROCEDIMENTOS QUE SE IMPÕE, ANULANDO-SE, DESDE O INÍCIO, A AÇÃO PENAL.
>
> 1.Uma análise detida dos 11 (onze) volumes que compõem o HC demonstra que existe uma grande quantidade de provas aptas a confirmar, cabalmente, a participação indevida, flagrantemente ilegal e abusiva, da ABIN e do investigador particular contratado pelo Delegado responsável pela chefia da Operação Satiagraha.
>
> 2. Não há se falar em compartilhamento de dados entre a ABIN e a Polícia Federal, haja vista que a hipótese dos autos não se enquadra nas exceções previstas na Lei nº 9.883/99.
>
> 3. Vivemos em um Estado Democrático de Direito, no qual, como nos ensina a Profª. Ada Pellegrini Grinover, in "Nulidades no Processo Penal", "o direito à prova está limitado, na medida em que constitui as garantias do contraditório e da ampla defesa, de sorte que o seu exercício não pode ultrapassar os limites da lei e, sobretudo, da Constituição." 4. No caso em exame, é inquestionável o prejuízo acarretado pelas investigações realizadas em desconformidade com as normas legais, e não convalescem, sob qualquer ângulo que seja analisada a questão, porquanto é manifesta a nulidade das diligências perpetradas pelos agentes da ABIN e um ex-agente do SNI, ao arrepio da lei.
>
> 5. Insta assinalar, por oportuno, que o juiz deve estrita fidelidade à lei penal, dela não podendo se afastar a não ser que imprudentemente se arrisque a percorrer, de forma isolada, o caminho tortuoso da subjetividade que, não poucas vezes, desemboca na

> odiosa perda da imparcialidade. Ele não deve, jamais, perder de vista a importância da democracia e do Estado Democrático de Direito.
>
> 6. Portanto, inexistem dúvidas de que tais provas estão irremediavelmente maculadas, devendo ser consideradas ilícitas e inadmissíveis, circunstâncias que as tornam destituídas de qualquer eficácia jurídica, consoante entendimento já cristalizado pela doutrina pacífica e lastreado na torrencial jurisprudência dos nossos tribunais.
>
> 7. Pelo exposto, concedo a ordem para anular, todas as provas produzidas, em especial a dos procedimentos nº 2007.61.81.010208-7 (monitoramento telefônico), nº 2007.61.81.011419-3 (monitoramento telefônico), e nº 2008.61.81.008291-3 (ação controlada), e dos demais correlatos, anulando também, desde o início, a ação penal, na mesma esteira do bem elaborado parecer exarado pela douta Procuradoria da República.
>
> (HC 149.250/SP, Rel. Ministro ADILSON VIEIRA MACABU (DESEMBARGADOR CONVOCADO DO TJ/RJ), QUINTA TURMA, julgado em 07/06/2011, DJe 05/09/2011) – (grifos nossos)

O julgado acima parece não coadunar com a celeuma doutrinária acerca da admissão de prova ilícita – a exemplo dos casos em que a mesma beneficia o réu – com a mitigação do princípio constitucional que a veda, reafirmando o contrário, ser aquela previsão absoluta não admitindo sua relativização.

Quanto ao objeto, a prova tem por regra a comprovação dos fatos controvertidos para as partes, relevantes para o juiz, e determinados. A exceção aos fatos é a prova do direito, que ocorre quando a lide disser respeito a direito internacional ou municipal.

Assim, o elenco de argumentos de cada parte no processo representa o conjunto fático que envolve a pretensão resistida de cada um deles, e a aferição da verdade de cada contexto proposto é o objeto da prova.

O exame das provas é feito pela cognição do processo, posto que através do mesmo é que se formará o convencimento, desenvolvido através das atividades de percepção e juízo. Para o direito italiano, que fortemente influenciou o ordenamento pátrio, a cognição divide-se em duas fases: a inspeção e avaliação das provas.

Sobre os elementos objetivos há o exercício da atividade do sujeito, a fim de que sirvam os mesmos como prova, sendo que as fases para tal atividade são sempre a percepção e o juízo. Note-se que há percepção até mesmo na prova indireta, desde que se exercite sobre a fonte de prova, e não sobre o fato a ser provado. Por outro lado, há juízo ainda que direta a prova, conquanto o órgão judicial deva argüir se existe o não o fato ser comprovado. Tais fases da atividade do verificador recebem os nomes de inspeção e de avaliação (CARNELUTTI, 2000, p. 545-546).

A presunção pode ser legal, ato de raciocínio realizado pelo legislador, de modo absoluto ou relativo. Como também pode ser judicial, quando o ato daquela avaliação e valoração é praticado pelo magistrado em cada caso concreto. Cumpre notar que o magistrado pode prolatar sentença baseada em indícios, conquanto fundamente a sua decisão e a lógica que o levou àquela conclusão de presumir tais indícios, até porque, como já visto, vale no ordenamento pátrio o princípio do livre convencimento motivado.

Ainda dentro do procedimento, cumpre lembrar que no direito pátrio não há hierarquia entre provas, tendo todas elas a mesma força, e não há uma que sobressaia em relação à outra. O Princípio do Livre Convencimento Motivado, lembra Patrícia Peck, vem da CF e reflete na legislação processual). E assim o art. 131 do CPC diz que "o juiz apreciará livremente a prova, atendendo aos fatos e circunstâncias constantes nos autos, ainda que não alegados pelas partes; mas deverá indicar, na sentença, os motivos que lhe formaram o convencimento" (2009, p. 157). Nesse mesmo sentido, a legislação penal, a princípio mais rigorosa, acresce:

> A livre apreciação da prova não significa a formação de uma livre convicção. A análise a ponderação do conjunto probatório são desprendidas de freios e limites subjetivamente impostos, mas a convicção do julgador deve basear-se nas provas coletadas. Em suma, liberdade possui o juiz para examinar e atribuir valor às provas, mas está atrelado a elas no tocante à construção de seu convencimento em relação ao deslinde da causa. E, justamente por isso, espera-se do magistrado a indispensável fundamentação de sua decisão, expondo as razões pelas quais chegou ao veredicto absolutório ou condenatório, como regra (NUCCI, 2009, p. 19).

Nesta senda, não há que se confundir prova com indícios ou presunções. Os indícios não são prova são um norte, uma orientação de algo que possa ter ocorrido, dando o ponto de partida para a possibilidade da ocorrência de fato. Já a presunção é ato de inteligência praticado pelo magistrado, com base em indícios avaliados e valorados.

Noutro giro, o sistema americano, conforme destaca Patrícia Peck (2009. p. 157), há uma hierarquia na valorização das provas dentre os tipos de prova:

> a) *Real evidence*: evidências materiais, objetos físicos que podem ser levados à corte, como, por exemplo, a arma de um crime;
>
> b) *Documentary evidence*: evidência documental, contendo duas regras:
>
> - *best evidence rule*: o documento original deve ser sempre apresentado em juízo;
>
> - *parol rule*: quando a prova é um documento assinado por duas partes, é valido somente o que está escrito, e nenhum acordo verbal poderá modificá-lo.
>
> c) *Testimonial evidence*: testemunha de fatos.

Apesar da valoração hierárquica não estar prevista no ordenamento pátrio, forçoso relembrar que a simples separação entre documentos públicos e privados, parece assim o fazer, dando maior destaque àqueles que estes últimos.

Quanto à finalidade da prova, não se fale mais em verdade real ou absoluta, posto que se saiba que essa pretensão é utópica e inalcançável, conquanto a simples atuação de vários sujeitos sobre determinados fatos, torna impossível a sua obtenção, como afirma Daniel Amorim Assumpção Neves: "Atualmente considera-se a verdade como algo meramente utópico e ideal, jamais alcançada, seja qual for a ciência que estiver analisando o conhecimento humano dos fatos." (2010, p.379).

Para o autor citado, no processo resta a evidenciada tal impossibilidade, diante da atuação de diversos sujeitos, das partes que apresentam seus fatos e provas do modo que lhes forem mais favoráveis; dos auxiliares, que ao reconstituírem os mesmos não o farão de forma exata; e, do próprio magistrado, que não participou dos mesmos e os analisará de acordo com suas próprias considerações.

Sobre o assunto, Luiz Guilherme Marinoni e Sergio Cruz Arenhart (2009, p. 37-38) manifestam-se:

> Tem-se, assim, ser impossível atingir-se a verdade sobre certo evento histórico. Pode-se ter uma elevada probabilidade sobre como ele se passou, mas nunca a certeza da obtenção de verdade. E isso se torna ainda mais evidente no processo. Aqui se está diante de uma controvérsia. Os litigantes, ambos, acreditam ter razão, e suas versões sobre a realidade dos fatos são, normalmente, diametralmente antagônicas. Sua contribuição para a pesquisa da realidade dos fatos é parcial e tendenciosa. O juiz, deve portanto, optar por uma das verdades dos fatos apresentadas, o que nem sempre é fácil e (o que é pior) demonstra a fragilidade da operação de descoberta da verdade realizada. As provas são geralmente distoantes. Mesmo a confissão é argumento perigoso, já que pode representar, como, aliás, não é raro, distúrbio psíquico do seu autor, ou mera tentativa de acobertamento dos fatos.

Se essa busca é utópica e inalcançável, o que se deve procurar? A verdade mais próxima possível daqueles fatos apresentados em juízo, como definiu Daniel Assumpção:

> O que se deve buscar é a melhor verdade possível dentro do processo, levando-se em conta as limitações existentes e com a consciência de que a busca da verdade não é um fim em si mesmo, apenas funcionando com um dos fatores para a efetiva realização da justiça, por meio de uma prestação jurisdicional de boa qualidade. Ainda que se respeitem os limites impostos à busca da verdade, justificáveis à luz de valores e garantias previstos na Constituição Federal, o que se procurará no processo é a obtenção da verdade possível. Por *verdade possível* entende-se a **verdade alcançável no processo,** que coloque o juiz mais próximo possível do que efetivamente ocorreu no mundo dos fatos, o que se dará pela ampla produção de provas, com respeito às limitações legais. (grifos do autor)

Os meios para o magistrado chegar próximo da verdade possível são a produção da mesma através do modelo dispositivo, em que apenas a parte a realiza, ou pelo modelo inquisitivo, onde o magistrado pode determinar a produção de algum ato probante, este adotado no Brasil.

Essas acepções iniciais são de fundamental importância à pesquisa, conquanto, a produção de prova no processo eletrônico agregará sujeitos, ou melhor, requisitos de validade, que podem comprometer ainda mais essa busca pela verdade alcançável.

Note-se que não bastando dialética fática existente entre autor e réu na lide, agregam-se à prova no processo eletrônico, necessidades inerentes ao procedimento na forma digital, cuja inobservância, quer por ignorância ou dolo, afetará, ainda mais, o resultado pretendido.

Surgem, agora, novos elementos imprescindíveis à verificação da verdade, ainda que a possível processualmente, tais como autenticidade do usuário que opera o sistema, e a validade do documento apresentado ou inserido no sistema – não apenas o seu conteúdo.

No processo eletrônico, a produção de prova – especialmente a documental – agregou novos procedimentos para a sua colheita e apresentação, importando, agora, aos operadores do direito o conhecimento das tecnologias alhures citadas, como forma de buscar essa verdade processual alcançável.

3.1 CONCEITO E ESPÉCIES

A prova, obviamente, não pertence só ao campo do direito, possuindo plurais conceitos e significados nas mais diferentes áreas do conhecimento. Nos dizeres de Daniel Amorim Assumpção Neves[24] (2010, p. 377):

> Não se trata de tema pacífico na doutrina a conceituação de prova, dificuldade acentuada pela diversidade de sentidos que pode ter o termo "prova". O termo é utilizado no direito e fora dele, não sendo estranho aos leigos (por exemplo, a tradicional exigência de uma namorada decepcionada: "então prove que me ame!"; ou ainda a sugestão de um garçom: "por que a você não prova essa nova cerveja?" etc.). E, mesmo dentro do campo do direito, encontra-se muita divergência no tratamento conceitual do tema, até porque são diversas as áreas afeitas à questão prova. Costuma-se dizer, com inegável acerto, que o **termo "prova" é plurissignificante**, dentro e fora do mundo do direito em geral, e do processo em particular.
>
> Contudo, apontar as diversas acepções, seja no sentido amplo ou restrito da palavra, não é o que se pretende neste momento. Aqui se busca a melhor definição que importe ao estudo processual, posto que seja o universo sob estudo.

[24] Citando: Cambi, 2001, p. 46; Garcia, Prova civil, 6.1, p. 28.

Seguindo o mesmo autor citado acima:

> Há doutrinadores que preferem conceituar a prova como sendo os meios ou elementos que contribuem para a formação da convicção do juiz a respeito da existência de determinados fatos. Outros entendem a prova como a própria convicção sobre os fatos alegados em juízo. Há ainda os que preferem conceituar a prova como um conjunto de atividades de verificação e demonstração, que tem por objetivo chegar à verdade relativa às alegações de fatos que sejam relevantes para o julgamento.[25] (2010, p. 378)

Nesse sentido, "a prova, em direito processual, é todo meio retórico, regulado pela lei, e dirigido, dentro dos parâmetros fixados pelo direito e de critérios racionais, a convencer o Estado-juiz da validade das proposições, objeto de impugnação, feitas no processo." (MARINONI; ARENHART, 2009, p. 57).

Esse conjunto de atos tendentes à comprovação da verdade dos fatos, dirigido ao juiz como meio de o mesmo convencer-se das razões que cada parte aduz em seu favor, é o conceito que melhor se adequa ao estudo pretendido, considerando as circunstâncias que envolvem o procedimento no processo eletrônico.

A prova subdivide-se, ainda, na tradicional classificação da prova: quanto ao fato, em diretas e indiretas; quanto ao sujeito, como pessoais e reais; quanto ao objeto, em testemunhais, documentais e materiais; e, quanto à preparação, em causais ou pré constituídas. (NEVES, 2010, p. 378)

Apesar de o Código de Processo Civil, no seu Capítulo VI, elencar os tipos de provas, em espécie, notadamente o depoimento pessoal, a confissão, a exibição de coisa ou documento, a documental, a testemunhal, a pericial e a inspeção judicial, o artigo 332 afirma que: "Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa."

Segundo Rodrigo Klippel e Antonio Adonias Bastos (2011, p. 395) o rol ali exposto é:

> *Numerus apertus* (enumerativo), visto que é possível que outros, ali não prvistos, sejam criados devido ao avanço da sociedade e utilizados pelo julgador para julgar a veracidade ou não das *alegações* pertinentes à causa (em regras fáticas, mas excepcionalmente referentes à existência do direito – art. 337 do CPC). (grifos dos autores)

A possibilidade de não limitação às espécies de prova predeterminadas pelo legislador processual é, sem dúvidas, ponto de extrema importância ao presente estudo, eis que aqui

[25] Daniel Amorim Assumpção Neves citando: Amaral Santos; Alexandre Câmara; Vicente Greco Filho e Cândido Dinamarco.

justamente se observa o reflexo da evolução social no direito, a ponto de permitir a inovação do procedimento com a instituição do processo eletrônico.

A junção da prova documental com o permissivo legal do artigo 332 do CPC é que irá dar margem à compreensão do que seja produção de prova em meio eletrônico, e produção de prova documental no processo eletrônico, para, a partir daí, responder o problema chave da presente pesquisa, qual seja, a impugnação da prova documental no processo eletrônico.

3.2 PROVA DOCUMENTAL E SEU VALOR PROBANTE

Quando se fala em prova documental, imediatamente tem-se em mente a idéia de papel, coisa palpável, física. Crê-se que essa associação direta decorra da dificuldade humana em pensar no abstrato, no imaterial como inexistente ou invisível.

De fato, a prova documental pode ser resultante de um documento escrito, compreendendo seus originais e suas cópias. Também pode ser aqueles escritos exarados por tabelião, como os que realizados pelo particular, sendo por causa desta conceituação, que há subdivisão dos documentos quanto à forma (originais ou cópias), e quanto à sua causa eficiente, em autênticos e particulares. (CASTRO, 2000, p. 227).

Porém esta definição torna-se inservível no que diz respeito ao conceito de prova documental a que se pretende o estudo em comento, primeiramente porque ao atrelar-se a prova documental a documento escrito, seu meio físico será sempre o papel, que não encontra correspondência ou existência na forma eletrônica, onde também não existe distinção entre originais e cópias. Contudo, mais adiante ver-se-á a conceituação de documento eletrônico.

Não obstante inexistir hierarquia entre as provas no ordenamento pátrio, até por força do princípio do livre convencimento motivado do magistrado, inegável é o impacto e efeitos da prova documental no processo, que, Carnelutti, (2000, p. 646): “Sem prova ao contrário, o juiz deve considerar como verdadeiro o fato representado”.

Isto se deve ao fato de que a prova documental dá ao julgador, de imediato, o conhecimento daquele fato que se busca provar, sem aparente interferência valorativa – não se crê que ela seja inexistente, porque a sua simples produção passa, necessariamente, pelas mãos de outrem, que pode alterar-lhe, senão quanto aos seus fatos, a sua forma – que não a do próprio

juiz. Na prova documental, pois, a participação humana no fato, resume-se à formação do documento e à reconstrução do fato.

Em seu livro Direito Digital, Patrícia Peck Pinheiro (2009, p.149-150) pontua as razões da natural resistência que o ser humano tem ao novo, ao inédito, ao desconhecido, o que, de fato, não é – e nem poderia ser – diferente no mundo jurídico, onde os operadores são ensinados a pensar em papel, na segurança que ele proporciona, mas essa é uma questão cultural, porquanto, o próprio Código Civil ensina que os pactos podem ser orais e a manifestação de vontade expressada por qualquer meio. Aponta a citada autora:

Quem disse que porque está no papel é o documento original? Afinal, todo fax é cópia, apesar de estar em papel. Já o e-mail eletrônico é o original e sua versão impressa é cópia.

Logo, na verdade, percebemos que o ser humano é um ser material por natureza, tendo apenas a espiritualidade como elemento imaterial. Todo o resto necessita de representação física para se poder ter o sentimento de posse, de propriedade. Esse sentimento não será resolvido nem mudado pelo Direito tradicional nem pelo Direito Digital. O que se tem de fazer é encontrar caminhos em que a tecnologia possibilite da esta impressão de materialidade aos documentos eletrônicos.

Esta associação imediatista pode, ainda, ter como causa a terminação que lhe é dada pelo CPC, quando fala em documento às vezes como papel escrito, e às vezes como representação de acontecimento fático. O certo é que, em verdade, a materialidade física da prova documental, como sinônimo de documento, é apenas um dos meios em que um documento reveste-se.

Deixar de lado a premissa de que nem toda prova documental tem como meio o papel é pré requisito para a compreensão de que este universo engloba outras tantas formas de apresentação, especialmente quando se considera o meio eletrônico.

Na acepção de Daniel Amorim Assumpção Neves, a prova documental:

> O conceito amplo de documento o define como qualquer coisa capaz de representar um fato, não havendo nenhuma necessidade de a coisa ser materializada em papel e/ou conter informações estritas. Algum escrito em outra superfície que não seja papel, tal como o plástico, metal, madeira etc., desde que represente um fato é considerado um documento dentro desse conceito amplo. Da mesma forma, uma fotografia, uma tabela, um gráfico, gravação sonora ou filme cinematográfico também será considerado um documento. Num conceito mais restrito, documento é o papel escrito.
>
> Apesar de o conceito restrito representar a ampla maioria das espécies de documentos na praxe forense, o direito brasileiro adotou o conceito amplo, sendo significativa a quantidade de diferentes espécies de coisas que são consideradas como documentos

> para fins probatórios, tais como os dados inseridos na memória do computador ou transmitidos por via eletrônica.

Coadunando tal entendimento, Luiz Guilherme Marinoni e Sérgio Cruz Arenhart (2009, p. 529-530), apud Comoglio, Ferri e Taruffo:

> Segundo COMOGLIO, FERRI E TARUFFO, "à categoria das *provas documentais* se reduzem em geral todas as *coisas* que aparecem idôneas a *documentar* um fato, ou seja, a narrá-lo, a representá-lo ou a reproduzi-lo". Conquanto genérica, a definição presta-se bem para demonstrar a impossibilidade de assimilação de prova documental por prova escrita. As figuras se confundem, sendo possível haver prova documental não escrita (fotografia, por exemplo), bem assim prova escrita não documental (v.g., o laudo pericial).
>
> A representação aludida, portanto, não se resume à mera escrituração de declarações. Ao contrário, abrange o registro de sons, imagens, estados de fato, ações e comportamentos, além dos "documentos criados através das tecnologias modernas da informação e das comunicações, como os dados inseridos na memória do computador ou transmitidos através de uma rede de informática, e em geral os assim ditos documentos informáticos." (*documenti informatici*, no original). (grifos dos autores)

A prova documental que aqui se propõe o estudo é exatamente esta: tudo aquilo que tenham aparência de idoneidade, e que sirva a documentar um fato, seja para narrá-lo, representá-lo ou a reproduzi-lo, mas de maneira eletrônica.

Isto é, a prova documental que interessa compreender é ela enquanto documento eletrônico, que no próximo item se busca explicar. Neste ponto, surgem as naturais indagações acerca da validade do documento eletrônico como prova, quando esta é originada (cópia de disco rígido de um computador, por exemplo), produzida (v.g., qualquer impresso scaneado) ou mesmo transmitida em meio eletrônico (*e-mails* enviados ou recebidos), para a finalidade convectiva quer em um procedimento físico ou digital.

O tortuoso estudo, em verdade, tem como premissa o conhecimento de conceitos e definições próprias da ciência da informática, para que se possa compreender que o documento eletrônico como prova no processo disciplinado pela Lei 11.419/06.

3.3 DOCUMENTO ELETRÔNICO E A PROVA NO PROCESSO ELETRÔNICO

Como já visto no item anterior, documento é o meio físico no qual se apresenta ou armazena uma informação, um fato, seja para narrar, representar ou mesmo reproduzir, de forma que impeça, ou permita detectar, a eliminação ou alteração. No dizer de Chiovenda, (1998, p.

151); “documento é toda representação material destinada a reproduzir determinada manifestação de pensamento, como uma voz fixada duradouramente.”

Pode-se, então, concluir que documento eletrônico pode ser conceituado como aquele registro cujo meio físico é, em verdade, um suporte eletrônico, desde que apto ao armazenamento de informações, e impeça alterações, ou viabilize a detecção de eliminação ou adulteração de seu conteúdo.

Nesse sentido, existem vários meios para a produção de documento eletrônico, a exemplo de textos, planilhas, bancos de dado, arquivos de som e vídeo, imagens – não apenas fotografias –mensagens eletrônicas de e-mail, mensagens de texto enviadas pelo celular; interrogatório de réu preso via videoconferência, e, até mesmo, procuração eletrônica[26]. Infere-se daí que o documento eletrônico é uma das espécies de prova documental.

Sem dúvidas, a simples idéia de documento não físico, ou melhor, em meio de suporte que não seja papel é, à primeira vista, desafiador, sendo este o grande obstáculo na compreensão e aceitação dos documentos eletrônicos, cujo termo em si foi definido no Brasil, pela Medida Provisória 2.200-2, de 24 de Agosto de 2001, em vigor até hoje, já que expedida anteriormente à Emenda Constitucional nº32:

> 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. (BRASIL, 2001).

Destarte, do teor da norma acima transcrita vê-se que o ordenamento garantiu ao documento eletrônico a presunção de verdadeiro quanto aos signatários, o que, mais adiante, indicará o primeiro problema a ser enfrentado quanto a prova no processo eletrônico

Cumpre dizer, ainda, que o texto da MP citada faz referência ao artigo 131 do antigo CC de 1916, substituído pelo artigo 219 do novo Código Civil, que o manteve na íntegra:

---

[26] Obtido por meio eletrônico. Disponível em: <http://www.documentoeletronico.com.br/procuracao-eletronica.asp> Acesso em: 28 out. 2011

> 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. (BRASIL, 2009).

Não se tem dúvidas, *a priori,* acerca da admissão do documento eletrônico no ordenamento jurídico brasileiro, contudo, para compreender o que é documento eletrônico e como ele pode ser utilizado como prova no processo, impende listar e esclarecer os termos técnicos que envolvem a matéria.

Inicialmente, o ITI, autarquia federal ligada à Casa Civil, que administra o ICP-Brasil, define, de forma palatável a quem é avesso à tecnologia – inclusive possui um glossário[27] que integra o anexo desta pesquisa – conceitos necessários ao entendimento do assunto, sendo importante destacar as relevantes ao tema:

> **Certificação Digital**
>
> A certificação digital é uma ferramenta de segurança que permite ao cidadão brasileiro realizar transações no meio eletrônico, que necessitem de segurança, como assinar contratos, obter informações sensíveis do governo e do setor privado, entre outros exemplos.
>
> O Brasil conta com um Sistema Nacional de Certificação Digital que é mantido pelo Instituto Nacional de Tecnologia da Informação. Aqui você encontra a tradução das siglas dos órgãos e dos processos que compõe esse Sistema e assim pode entender o seu funcionamento.
>
> **ICP-Brasil**
>
> A Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação do cidadão quando transacionando no meio virtual, como a Internet.
>
> Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI além de desempenhar o papel de Autoridade Certificadora Raiz - AC Raiz, também, tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.
>
> **Certificado Digital**
>
> O certificado digital da ICP-Brasil, além de personificar o cidadão na rede mundial de computadores, garante, por força da legislação atual, validade jurídica aos atos praticados com seu uso. A certificação digital é uma ferramenta que permite que aplicações, como comércio eletrônico, assinatura de contratos, operações bancárias, iniciativas de governo eletrônico, entre outras, sejam realizadas. São transações feitas de forma virtual, ou seja, sem a presença física do interessado, mas que demandam identificação inequívoca da pessoa que a está realizando pela Internet.
>
> Tecnicamente, o certificado é um documento eletrônico que por meio de procedimentos lógicos e matemáticos asseguraram a integridade das informações e a autoria das transações. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora que, seguindo regras

[27] Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/Legislacao/Glossario_ICP-Brasil_-_Versao_1.2.pdf> Acesso em: 27 out. 2011.

emitidas pelo Comitê Gestor da ICP-Brasil e auditada pelo ITI, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas.

Os certificados contêm os dados de seu titular, tais como: nome, número do registro civil, assinatura da Autoridade Certificadora que o emitiu, entre outros, conforme detalhado na Política de Segurança de cada Autoridade Certificadora.

AC- Raiz

A Autoridade Certificadora Raiz da ICP-Brasil é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subseqüente ao seu.

A AC-Raiz também está encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as Autoridades Certificadoras - ACs estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor.

AC - Autoridade Certificadora

Uma Autoridade Certificadora é uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Desempenha como função essencial a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada).

Cabe também à AC emitir listas de certificados revogados - LCR e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação - DPC. Além de estabelecer e fazer cumprir, pelas Autoridades Registradoras a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação feita.

AR - Autoridade de Registro

Entidade responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC que tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.

Assinatura Digital

A assinatura digital é uma modalidade de assinatura eletrônica, resultado de uma operação matemática que utiliza criptografia e permite aferir, com segurança, a origem e a integridade do documento. A assinatura digital fica de tal modo vinculada ao documento eletrônico que, caso seja feita qualquer alteração no documento, 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.

Assinatura Digitalizada

A assinatura digitalizada é a reprodução da assinatura de próprio punho como imagem por um equipamento tipo scanner. Ela não garante a autoria e integridade do documento eletrônico, porquanto não existe uma associação inequívoca entre o assinante e o texto digitalizado, uma vez que ela pode ser facilmente copiada e inserida em outro documento. (grifo nosso)

Criptografia

> A palavra criptografia tem origem grega e significa a arte de escrever em códigos, de forma a esconder a informação na forma de um texto incompreensível. A cifragem ou processo de codificação, é executada por um programa de computador que realiza um conjunto de operações matemáticos e transformam um texto claro em um texto cifrado, além de inserir uma chave secreta na mensagem. O emissor do documento envia o texto cifrado, que será reprocessado pelo receptor, transformando-o, novamente, em texto legível, igual ao emitido, desde que tenha a chave correta.
>
> **Tipos de Criptografia**
>
> Existem dois tipos de criptografia: simétrica e assimétrica. A criptografia simétrica é baseada em algoritmos que dependem de uma mesma chave, denominada chave secreta, que é usada tanto no processo de cifrar quanto no de decifrar o texto. Para a garantia da integridade da informação transmitida é imprescindível que apenas o emissor e o receptor conheçam a chave. O problema da criptografia simétrica é a necessidade de compartilhar a chave secreta com todos que precisam ler a mensagem, possibilitando a alteração do documento por qualquer das partes. A criptografia assimétrica utiliza um par de chaves diferentes entre si, que se relacionam matematicamente por meio de um algoritmo, de forma que o texto cifrado por uma chave, apenas seja decifrado pela outra do mesmo par. As duas chaves envolvidas na criptografia assimétrica são denominadas chave pública e chave privada. A chave pública pode ser conhecida pelo público em geral, enquanto que a chave privada somente deve ser de conhecimento de seu titular. (sic) [28]

A ICP-OAB[29], por seu turno, tenta explicar em uma linguagem mais palatável aos advogados estes conceitos:

> **Documentos Eletrônicos**
>
> Um dos grandes desafios de nossos tempos é a possibilidade de substituir documentos em papel por documentos eletrônicos. O documento eletrônico nada mais é do que uma seqüência de números binários (isto é, zero ou um) que, reconhecidos e traduzidos pelo computador, representam uma informação. Um arquivo de computador contendo textos, sons, imagens ou instruções é um documento eletrônico. O documento eletrônico tem sua forma original em *bits*, ou seja, não é impresso ou assinado em papel: sua circulação e verificação de autenticidade se dão em sua forma original, eletrônica. São evidentes as vantagens quanto ao armazenamento, transmissão e recuperação de documentos eletrônicos, se comparados com o papel. (grifo nosso)
>
> A dificuldade em portar os documentos para o meio eletrônico reside em atribuir-lhes segurança comparável à que se obtém dos documentos físicos. Diversamente do que ocorre com o documento em papel, não há como lançar uma assinatura manuscrita em um documento eletrônico como forma de demonstrar a sua autoria; além disso, documentos eletrônicos podem ser facilmente alterados, sem deixar vestígios físicos apuráveis. É **necessário, pois, utilizar um mecanismo técnico que possa permitir conferir a autenticidade e a integridade de um documento eletrônico. Por autenticidade, quer-se designar a certeza quanto à pessoa que criou o documento que, em termos jurídicos, presta a declaração nele constante. Por integridade, entende-se a não adulteração de um documento, posteriormente à sua criação**.
>
> A única maneira reconhecidamente segura de atribuir autenticidade e a integridade a documentos eletrônicos é o uso de assinaturas digitais produzidas por criptografia assimétrica. (grifos nossos).
>
> **Assinaturas Digitais com Chaves Criptográficas Assimétricas**

[28] Grifos nossos.
[29] Obtido em meio eletrônico. Disponível em: <http://cert.oab.org.br/cert_assin.htm> Acesso em: 20 out. 2011.

As assinaturas digitais são, na verdade, o resultado de uma complexa operação matemática que trabalha com um conceito conhecido por criptografia assimétrica. A operação matemática utiliza como variáveis o documento a ser assinado e um segredo particular, que só o signatário eletrônico possui: a chamada chave privada. Como somente o titular deve ter acesso à sua chave privada, somente ele poderia ter calculado aquele resultado, que, por isso, se supõe ser único e exclusivo, como uma assinatura.
Para conferir a assinatura digital, não é necessário ter conhecimento da chave privada do signatário, preservando, assim, o segredo necessário para assinar. Basta que se tenha acesso à chave pública que corresponde àquela chave privada. A conferência da assinatura também é feita por operações matemáticas que, a partir do documento, da chave pública e da assinatura, podem atestar que tal assinatura foi produzida com a chave privada correspondente, sem a necessidade de se ter acesso a essa chave privada. E, **se o documento houver sido adulterado, posteriormente ao lançamento da assinatura digital, o resultado da operação matemática irá acusar esta desconformidade, invalidando a assinatura**.

Desta forma, se a conferência anunciar uma assinatura válida, isto significa que: a) a assinatura foi produzida com o uso da chave privada correspondente à chave pública; b) o documento não foi modificado depois de produzida a assinatura. (grifos nosso)

O Par de Chaves Criptográficas

Para que uma pessoa, então, possa gerar uma assinatura digital, deve primeiramente possuir um par de chaves assimétricas, exclusivamente seu, formado pela chave privada e pela chave pública. Ao contrário do que o senso comum levaria a crer, essas chaves não mantêm qualquer vínculo com o corpo ou com dados biométricos de seu titular. São números de grande expressão (algo em torno de 300 algarismos) geradas aleatoriamente pelo computador, e sua segurança consiste justamente em terem sido geradas da forma mais aleatória possível, garantindo estatisticamente que não se possa nunca repetir o processo para gerar outro par de chaves idêntico, evitando a fraude. O par de chaves é calculado simultaneamente, de modo que, para uma dada chave privada, só exista uma chave pública que lhe sirva como par.

Fruto de operações matemáticas complexas e de critérios de aleatoriedade, o par de chaves é calculado pelos computadores, mediante o uso de *"softwares"* específicos, que trabalhem com criptografia assimétrica. Os programas navegadores, também conhecidos como *"browsers"*, são exemplos de *"softwares"* bastante conhecidos que realizam estas funções.

Certificados Eletrônicos

Como o par de chaves não mantém qualquer vínculo com o corpo de seu titular, é necessário algum mecanismo que permita atestar que a chave pública utilizada na conferência da assinatura realmente pertença a uma dada pessoa, já que é fácil gerar chaves e atribuir-lhes o nome de outrem. As operações matemáticas só podem atestar que a assinatura digital foi produzida com a chave privada que faz par com a chave pública utilizada na conferência. Algum elemento outro deve servir para convencer o destinatário da mensagem que a chave pública em questão realmente pertence ao sujeito nela indicado. Uma das formas de se fazer isso é por meio dos certificados eletrônicos.
Os certificados eletrônicos consistem assim em uma declaração, de um ente certificante, acerca da titularidade das chaves de uma outra pessoa, que está sendo certificada. Esse ente é também conhecido como "terceiro de confiança" porque sua declaração deve ser tendente a gerar, para o destinatário da informação que nele confie, a certeza quanto à sua autoria.

Um certificado eletrônico contém a chave pública da pessoa certificada, os dados pessoais que a identificam, que devem ter sido conferidos pelo ente certificante ao expedir o certificado, e a assinatura digital do ente certificante.

> A conferência do certificado, por sua vez, deve ser feita com o uso da chave pública do ente certificante. Isso normalmente produz outra dúvida: e como saber se a chave pública que assinou o certificado é realmente do ente certificante? Uma infra-estrutura de chaves públicas pressupõe que os usuários do sistema acreditem na autenticidade de uma chave inicial, a chamada chave raiz, que é auto-assinada, isto é, o seu certificado é assinado com a própria chave privada do par. Algum fato deve induzir no usuário a crença de que esta chave é verdadeira. No caso da ICP-OAB, por exemplo, a chave raiz será declarada por ato formal do Conselho Federal, publicado no Diário Oficial. A confiança na chave raiz produz confiança nas chaves de entes certificantes que tenham sido certificados pela raiz e, abaixo destes, dos usuários que tenham sido certificados pelos entes certificantes. A confiança na chave raiz produz confiança das chaves de entes certificantes por ela certificadas, e, abaixo desse entes, dos usuários que estes vieram a certificar. A essa seqüência de certificações se dá o nome de "caminho de certificação", que pode ser verificado no próprio certificado.

Impende consignar, ainda, aqui que, embora muitas vezes confundido com assinatura digital e assinatura digitalizada, o conceito de **assinatura eletrônica** é diverso daqueles, constituindo, **em verdade, qualquer mecanismo, não necessariamente criptografado, capaz de identificar o emitente de um documento digital**. Em geral, assinatura eletrônica é entendida como a combinação de nome de usuário e senha, sem uso de criptografia.

Por que estas definições são tão importantes? Porque somente o somatório destes conhecimentos é capaz de definir documento eletrônico, bem como dar a exata compreensão de que os **atos praticados dentro do processo eletrônico também vão constituir documentos eletrônicos,** a fim de compreender onde residem os problemas na impugnação dos mesmos.

É neste aspecto do impedimento de alteração ou violação que o documento eletrônico guarda singularidades que mais transitam pela ciência da informática que pelo direito em si. Em verdade são acepções tecnológicas que tornam possível o entendimento necessário a produção do documento eletrônico, sua validade e autenticidade, assim como de seu uso com prova.

Elucidativo, ainda, trazer às conceituações dos requisitos do documento eletrônico, explicadas no artigo de Patrícia Peck, que assim expõe:

Todo documento eletrônico deve possuir dois pressupostos para ter força probante, quais sejam:

> Autenticidade: É um processo idôneo por meio do qual se possa garantir a real autoria dos termos de um documento eletrônico. O documento autêntico é aquele que não permite a dúvida quanto à identificação de seu autor. Nos documentos físicos a autenticidade é comprovada através da firma ou da assinatura, e ainda existe a possibilidade de ser reconhecida por um tabelião que atestará sua legitimidade. Integridade: É a possibilidade de atestar a inteireza do documento eletrônico após sua transmissão, bem como apontar eventual alteração irregular de seu conteúdo. Em outras palavras o documento íntegro é aquele que dá certeza de que permanece inalterado.

> Os dois requisitos supracitados estão presentes em todos os países que regulamentaram regime jurídico dos documentos eletrônicos. Exemplo é UNCITRAL (United Nations Commission on International Trade Law), criada pela Assembléia Geral da Organização das Nações Unidas que criou uma Lei Modelo que tem por finalidade servir de estrutura à formulação das legislações pátrias, fazendo com que estas, na medida do possível, possam conviver harmoniosamente no ambiente globalizado. [30]

Com efeito, vê-se que documento eletrônico pode ser definido como qualquer instrumento capaz de armazenar um conteúdo informativo fático, cuja alteração ou eliminação seja de difícil prática ou de fácil demonstração.

A sua utilização como prova encontra respaldo no anteriormente citado artigo 332 do CPC, que admite qualquer meio lícito como tal, mas cite-se aqui, também, o artigo 225 do Código Civil, ao dizer que "as reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão."

Entendido o documento eletrônico, onde reside a problemática de seu uso no processo eletrônico? Na sua validade, autenticidade e segurança.

Como visto no intróito deste trabalho, sabe-se que a existência de vários sistemas criados para implantar o processo eletrônico no país, deu margem a procedimentos operacionais distintos entre si, que, de fato, podem ser questionados.

Mormente ser a assinatura digital, expedida por autoridade certificadora competente, mediante criptografia é o que valida, autentica e assegura o documento eletrônico no que tange a sua origem e emissão, o legislador admitiu no art. 2º da Lei 11.419, a possibilidade de uso da assinatura eletrônica (nome de usuário mais senha) sem tais requisitos.

Esta possibilidade é ferrenhamente criticada pelos especialistas em segurança digital, assim como por alguns autores de obras sobre o processo eletrônico. Alexandre Atheniense (2010, p. 122 e 123) chega a afirmar que a assinatura eletrônica sem uso de certificado digital é um acinte à Carta Magna e ao Estatuto da OAB (por exigir excessivos meios de identificação do advogado) – fundamentos, inclusive, das ADIs nº 3880, 3869 e 30445, contra a Lei 11.419/06, em trâmite no STF[31].

---

[30] Obtido em meio eletrônico. Disponível em: <http://uj.com.br/publicacoes/doutrinas/3410/DOCUMENTO_ELETRONICO_E_A_PROVA_ELETRONICA> Acesso em: 27 out. 2011.

[31] STF. Disponível em: <www.stf.jus.br> Acesso em: 27 out. 2011

Perceptível que a idéia de simples assinatura eletrônica – tais como as exigidas pelo PROJUDI e pelo e-Proc – descomplica a vida do usuário, especialmente daqueles sem muitas habilidades computacionais, e, sem dúvida, custa-lhe nada frente aos valores de R$ 100,00 (cem reais) a R$ 200,00 (duzentos reais), considerando o *hardware* necessário à utilização,[32] cobrados pela AC-OAB para emissão do certificado digital no *chip* da carteira da Ordem.

Aqui se abra um parêntese para os fundamentos jurídicos que legitima, a OAB a ser autoridade certificadora:

> Documentos eletrônicos e assinaturas digitais podem ser considerados documentos, no sentido jurídico da expressão, segundo tem sido afirmado pela doutrina nacional e internacional.
>
> Com a edição da Medida Provisória nº 2.200/01, houve reconhecimento legal expresso do uso de assinaturas digitais por processo criptográfico para atribuir autenticidade e integridade a documentos eletrônicos. O texto final, em vigor, da Medida Provisória nº 2.200-02, de 24 de Agosto de 2001, após alterações sofridas nas duas reedições, deixa claro, em seu artigo 10, parágrafo 2º, que a validade jurídica de documentos eletrônicos não está sujeita à certificação oficial da ICP-Brasil, criada pelo referido diploma. Assim têm-se mostrado, aliás, a tendência das novas legislações que vêm regulando a matéria em outros países, notadamente na Europa e Estados Unidos.
>
> Tratando-se da identificação de advogados, e conseqüente declaração da qualidade de Advogado do titular do certificado, a ninguém mais compete fazê-lo, senão à Ordem dos Advogados do Brasil. Nenhuma outra instituição, pública ou privada, tem o poder de conceder a alguém documentos de identificação que o declarem ser advogado. **Portanto, conquanto outras entidades certificadoras, públicas ou privadas, possam expedir certificados ao público em geral, e também aos advogados, somente a certificação expedida pela Ordem dos Advogados do Brasil pode atestar a regular inscrição do titular em seus quadros, podendo ser utilizada para identificar o profissional perante as repartições em que atua**. (grifo nosso)
>
> **Lei Federal nº 8.906, de 4 de julho de 1994:**
>
> Art. 3º. O exercício da atividade de advocacia no território brasileiro e a denominação de advogado são privativos dos inscritos na Ordem dos Advogados do Brasil - OAB.
>
> § 1º. Exercem atividade de advocacia, sujeitando-se ao regime desta Lei, além do regime próprio a que se subordinem, os integrantes da Advocacia-Geral da União, da Procuradoria da Fazenda Nacional, da Defensoria Pública e das Procuradorias e Consultorias Jurídicas dos Estados, do Distrito Federal, dos Municípios e das respectivas entidades de administração indireta e fundacional.
>
> § 2º. O estagiário de advocacia, regularmente inscrito, pode praticar os atos previstos no Art. 1º, na forma do Regulamento Geral, em conjunto com advogado e sob responsabilidade deste.
>
> Art. 4º. São nulos os atos privativos de advogado praticados por pessoa não inscrita na OAB, sem prejuízo das sanções civis, penais e administrativas.
>
> Parágrafo único. São também nulos os atos praticados por advogado impedido - no âmbito do impedimento - suspenso, licenciado ou que passar a exercer atividade incompatível com a advocacia.

[32] Fonte: Autoridade Certificadora OAB. Disponível em: < http://www.acoab.com.br/acoab/site/compre> Acesso em: 28 out. 2011

> [...]
>
> Art. 13. O documento de identidade profissional, na forma prevista no Regulamento Geral, é de uso obrigatório no exercício da atividade de advogado ou de estagiário e constitui prova de identidade civil para todos os fins legais.
>
> [...]
>
> Art. 54. Compete ao Conselho Federal:
>
> [...]
>
> X - dispor sobre a identificação dos inscritos na OAB e sobre os respectivos símbolos privativos;
>
> [...]
>
> Art. 58. Compete privativamente ao Conselho Seccional:
>
> [...]
>
> VI - realizar o Exame de Ordem;
>
> VII - decidir os pedidos de inscrição nos quadros de advogados e estagiários;
>
> VIII - manter cadastro de seus inscritos;

Com razão a ICP-OAB, porquanto se a definição de documento eletrônico passa, necessariamente pelo certificado digital, admitir o não uso do mesmo é ir contra as orientações de segurança cibernética desenvolvidas pela ciência da informática, para obter-se o quê? Mais segurança? Menos custo? Simplicidade no acesso? Não parece crível que tais argumentos sejam dignos de acolhida.

Observe-se que o simples uso de senha e *login* de usuário combinados é um sistema por demais arriscado para se aferir a veracidade de um documento ou de seu produtor. Tome-se, por exemplo, os serviços de *internet banking* dos mais diversos bancos do país. Apesar de não exigirem (ainda) certificado digital de seus clientes, também não mais praticam apenas o uso de assinatura eletrônica simples, exigindo em conjunto de medidas de segurança que vão desde a instalação de programas específicos de proteção nos computadores dos clientes, ao uso de *chip*[33] nos cartões magnéticos, senhas diferenciadas para internet e *tokens*[34] para acesso às contas e realização de transações bancárias *on line.*

Assim, é no mínimo curioso, indagar por quais motivos os sistemas de processo eletrônico (e-STJ e e-STF) não são realizados mediante assinatura eletrônica sem certificação? Muito certamente porque as duas mais altas cortes do país não se atreveriam a valer-se de sistemas de processo eletrônico sem a mínima garantia de autenticidade, validade e segurança para os usuários e documentos ali indicados e processados.

---

[33] Obtido em meio eletrônico. Disponível em: <http://www.infopedia.pt/lingua-portuguesa/chip;jsessionid=ahvoQ6C38UEBBMMQg+f4Hw__> Acesso em: 15 out. 2011

[34] Glossário da ICP-Brasil. Anexo B deste trabalho.

Diante da fragilidade que envolve o tem da segurança dos documentos eletrônicos, Luiz Guilherme Marinoni e Sérgio Cruz Arenhart, citando doutrina francesa, apresentam um quadro com os meios de autenticação digital mais utilizados hodiernamente, para sugerir, inclusive, o uso misto deles, a fim de que eventual falha de uma técnica, possa ser compensada por outra, "o que pode outorgar aos documentos eletrônicos fiabilidade semelhante àquela hoje desfrutada pelos documentos obtidos pelas vias tradicionais.".

Quadro 3 – Meios de Autenticação Digital

SERVIÇOS X TÉCNICAS MODERNAS DE IDENTIFICAÇÃO	**IDENTIFICAÇÃO DAS PARTES**		**CONTEÚDO DA MENSAGEM**		**VONTADE DE SE APROPRIAR DO CONTEÚDO**
	Emissor	**Receptor**	**Modificações feitas por uma parte ou um terceiro**		
CONFIDENCIALIDADE					
Criptografia simétrica	Sim	Sim	Não	Sim	?
Criptografia assimétrica simples	Não	Sim	Sim	Sim	?
Criptografia assimétrica com dupla cifragem	Sim	Sim	Sim	Sim	?
PESSOAS					
Código Secreto (PIN)	Sim	Não	Não	Não	Sim
Cartas passivas	Sim	Não	Não	Não	Sim
Cartas Ativas	Sim	Não	Não	Não	Sim
Reconhecimento físico	Sim	Não	Não	Não	Sim
Assinatura dinâmica	Sim	Não	Não	Não	Sim
DOCUMENTOS					
Assinatura Eletrônica	Sim	(Sim)	Sim	Sim	Sim

Fonte: ANTOINE, Mireille; ELOY, Marc; BRAKELAND, Jean-François, *Le droit de La preuve face aux nouvelles tecnologies de l´information,* p.63. (MARINONI; ARENHART, 2009, p.546).

Edilberto Barbosa Clementino (2007, p. 95-96), confirmando a preocupação com a segurança, afirma que:

> Não interessa saber se um Documento Eletrônico teve origem em um determinado Computador, porque ainda nesse caso poder-se-iam levantar questionamentos a respeito da Autenticidade do Documento, haja vista que qualquer pessoa com acesso àquele Computador poderia atribuir-se falsa identidade. Além disso,o interessado em remeter algum Documento estaria "preso" a um determinado computador, sob pena de suas mensagens não serem confiáveis.

> A certeza da Autenticidade deve ser uma característica que diga respeito à pessoa do signatário do Documento e não de um equipamento que este utilize. É necessário que, no Processo Judicial Eletrônico, tenha-se absoluta certeza de que o remetente indicado seja efetivamente o signatário daquele Documento eletronicamente produzido e transmitido. Essa garantia relativa à autoria do Documento leva ao Princípio do não-repúdio, que significa que o autor do Documento não poderá alegar sua autoria.

Não se pode imaginar um processo eletrônico sem certificado digital, conquanto, os atos ali praticados nada mais são senão documentos eletrônicos. A petição inicial, a sentença, as decisões, etc., produzidas nos sistemas que assim trabalham, a exemplo do PROJUDI e e-Proc, são documentos eletrônicos e como tais deveriam, de fato, ter a mínima segurança – estabelecida, diga-se, pela própria MP que conceituou documento eletrônico – respeitada.

A situação imaginária possível, por exemplo, seria a de inserção de uma sentença ou mesmo uma penhora *on line* através do sistema BACENJUD, realizada por outro usuário que não o magistrado. Como provar que aquele documento eletrônico não foi emitido pelo juiz, se para tal ato, em alguns sistemas de processo digital basta a assinatura eletrônica? Difícil, mas completamente plausível, por exemplo, no PROJUDI.

A própria ICP-OAB assim informa[35]:

> A OAB e a segurança tecnológica de suas certificações
>
> Nenhuma tecnologia propicia segurança inatacável; ninguém, com responsabilidade, omitiria os riscos envolvidos no uso de assinaturas digitais.
>
> Verdadeiramente, as operações matemáticas utilizadas nas assinaturas digitais têm sido analisadas há mais de duas décadas pela comunidade científica, mostrando-se sólidas e confiáveis. Entretanto, embora seja o coração do sistema, o aspecto matemático da questão é apenas um dos elos de uma corrente. Se decifrar os códigos criptográficos utilizados tem se mostrado inviável, isso não quer dizer que inexistam outros meios de ataque ou fraude. O importante para o usuário, pois, é saber quais são os pontos mais sensíveis, para poder dispensar cuidados adequados.
>
> Partindo da premissa que nenhuma barreira física ou técnica pode ser considerada intransponível, a ICP-OAB, para merecer a confiança de toda a sociedade, e em especial, da Advocacia e dos Tribunais, apóia-se, como elemento fundamental de segurança, na mais completa transparência de seus procedimentos, realizando conferências e deixando registros auditáveis que possam servir de contraprova, em caso de eventual falha. (grifos nosso)
>
> Os sistemas criptográficos utilizados são padrões abertos, de domínio público, amplamente escrutinados pelos especialistas de todo o mundo.
>
> A identificação do advogado exige comparecimento pessoal e identificação perante um funcionário da Seção ou Subseção de origem. Este é o único meio possível de garantir que outra pessoa não está solicitando um certificado em seu nome; e, dadas as informações do certificado - os números identificadores únicos - inclusas no requerimento escrito que o advogado deve apresentar, distingue-se exatamente qual certificado está sendo entregue ao requerente, deixando contraprova física. Tanto a

[35] Obtido por meio eletrônico. Disponível em: < http://cert.oab.org.br/uso_seg.htm> Acesso em: 29 out. 2011.

OAB guarda prova da solicitação, quanto o advogado guarda prova em meio físico sobre os dados do certificado que efetivamente lhe pertence.

Como mais uma medida de segurança, os certificados da ICP-OAB serão expedidos por prazo nunca superior a três anos, prazo dentro do qual novo certificado deve ser requerido.

O uso seguro de certificados eletrônicos pelos advogados

É opinião comum, na comunidade de segurança da informação, que o ataque mais fácil a assinaturas digitais consiste em tentar-se apropriar da chave privada do usuário. Aliás, exatamente na ponta do usuário encontra-se a posição mais frágil do processo de emissão e conferência de assinaturas eletrônicas.

A OAB, assim, não tem preocupação apenas com a segurança de sua própria chave privada e com a expedição e controle dos certificados que emite. Tem, igualmente, preocupação em informar a seus inscritos dos riscos existentes e soluções necessárias para controlá-los, no trato desse novo e tão importante instrumento, a assinatura digital.

O ponto mais sensível na segurança do usuário é o da guarda de sua chave privada. Esta chave deve ficar em poder exclusivo do seu titular, portanto, somente a ele compete guardá-la com segurança. Se um terceiro conseguir acesso à sua chave privada, poderá gerar assinaturas digitais em seu nome, sem nenhuma possibilidade técnica de demonstrar-se a falsidade. Além disso, o invasor estará habilitado a decifrar toda a sua correspondência privada que tiver sido codificada com a correspondente chave pública.

Por isso, conforme explicitado nas instruções fornecidas, é imperioso que: a) o certificado seja gerado em computadores pessoais do advogado; b) o certificado não seja instalado em computadores de uso público; c) que a proteção com senha seja utilizada, adotando-se senha complexa. Diante destes cuidados, para praticar uma fraude, o invasor precisaria obter a chave privada que está gravada no disco rígido do seu computador e conhecer a senha utilizada na proteção, sem a qual a chave não poderá ser violada. Existem programas de computador especialistas em violar senhas, realizando diversos tipos de ataque, por isso é conveniente conhecer as instruções sobre a **escolha de senha segura**.

É também seriamente recomendável que o usuário não instale "softwares" de procedência desconhecida ou duvidosa no computador onde está armazenado o seu certificado, e tome a mais completa precaução contra ataques de vírus ou cavalos-de-tróia. A possibilidade técnica de um vírus, ou cavalo-de-tróia, adentrar seu computador, capturar a chave gravada no disco, "observar" sua digitação no teclado para aprender a senha, para, após, enviar tudo isso a um criminoso, sem que o usuário sequer perceba, é concreta e real.

É altamente recomendável aos usuários a instalação de softwares anti-vírus, que impeçam a infecção por esses programas malignos, bem como a utilização de um sistema de proteção contra acesso indevido em seus computadores, conhecido no jargão técnico por *"firewall"*. Há várias opções disponíveis desses sistemas, a baixos custos, ou mesmo gratuitas.

Outra observação relevante diz respeito ao tamanho das chaves. Atualmente, os "browsers" disponibilizados ao grande público geram chaves de 1024 bits, que podem ser consideradas seguras por mais alguns anos. No atual estágio de desenvolvimento da ciência e da tecnologia, considera-se não existir poder computacional instalado que seja suficiente para quebrar chaves de 1024 bits. Versões de "browsers" mais antigas, sujeitas a anteriores restrições de leis norte-americanas que controlavam exportação de produtos e tecnologia de criptografia forte, não permitiam a criação de chaves com mais de 512 bits. Embora exija certo poder computacional para fazê-lo, já foi demonstrado que é possível fraudar chaves desta magnitude. Neste caso, a atualização do "browser" é também seriamente recomendável.

Desnecessário dizer que o certificado contendo a chave privada (que, em princípio, está instalado no computador que fez a requisição, e armazenado na cópia de

> segurança que foi gerada) deve ser de uso pessoal e exclusivo do seu titular, não devendo ser cedido ou emprestado em hipótese alguma. A entrega da chave privada a um terceiro é ato de ainda maior risco do que a entrega de cartões bancários ou de crédito; a "restituição" da chave privada ao titular não assegura que uma cópia exata e idêntica não possa ter sido feita, vez que se trata apenas de um arquivo eletrônico, fácil e prontamente duplicável. Nunca, sob qualquer pretexto, permita ou conceda acesso de terceiros à sua chave privada. (grifos nosso)
>
> Havendo suspeita de que a chave privada tenha caído em poder de terceiros, deve-se prontamente requerer a revogação do certificado eletrônico junto à OAB.
>
> Certificados eletrônicos contendo tão somente a chave pública são livremente distribuídos, estando inclusive disponíveis para acesso online. Estes certificados são utilizados somente para conferir a assinatura ou para enviar mensagens eletrônicas criptografadas ao titular. Não se assuste em vê-los circulando.
>
> Somados todos estes fatores, e considerando que esta será certamente a primeira experiência de cada um de nós advogados no uso operacional de chaves criptográficas assimétricas, firmamos a posição de limitar o uso dos certificados a fins profissionais, evitando que o advogado possa ser alvo de ataques criminosos tendentes a subtrair-lhe a chave privada para causar-lhe prejuízo patrimonial. Certamente, ficando restrito à prática de atos profissionais, o uso indevido de certificados subtraídos ou forjados fica mais fácil de ser detectado, corrigido e apurado, bem como pode afastar o interesse daqueles que possam querer obter nossas chaves para cometer outros tipos de fraude.

Registre-se o que Luiz Guilherme Marinoni e Sérgio Cruz Arenhart afirmam (2009, p. 543-544):

> Partindo-se para a seara dos documentos informáticos – guarnecidos na memória de computadores ou resultantes de processamento por equipamentos informatizados – as questões não são menores. Também aqui não se tem nenhuma garantia prévia de que as informações retiradas do computador guardam alguma conformidade com a realidade. A inexistência de um registro físico dos dados e a facilidade de manipulação das informações armazenadas tornaram extremamente “volátil” a documentação, e, no mais das vezes, imprestável o meio para fixação de fatos e representação de idéias. Novamente, pode-se imaginar que, enquanto não contestadas as informações extraídas do computador, é razoável fiar-se em tais documentos para a prova de fatos e de declarações; entretanto, em havendo contestação, mais uma vez, mostrar-se-á como totalmente inútil o mecanismo,, devendo a parte buscar a prova que pretende através de outros meios.[...]
>
> É claro que novos elementos da tecnologia permitem, já, imprimir certa segurança na transmissão de dados pela via da internet, logrando conferir a documentos transmitidos pela via eletrônica maior grau de confiabilidade. Assim é que surgem, no meio informático, as mensagens criptografadas, as assinaturas eletrônicas etc., utilizadas já na rede de computadores como formas de permitir alguma segurança na transmissão de dados e na verificação de documentos inseridos na internet.

O documento eletrônico admissível no processo digital, pois, há de atender as regras mínimas de segurança, existentes justamente para atender tal finalidade, sob pena de ter-se um sistema eficaz em tempo e custo, mas inseguro e passível de falhas.

Muito pior, parece que o descrédito dos próprios advogados aos sistemas de processo eletrônico em nada contribui para a solução dos problemas atinentes à segurança do

documento eletrônico e seu uso no procedimento digital, como se vê de recente matéria de Pedro Canário[36] sobre o tema:

> O processo eletrônico pode trazer muitos benefícios à população, principalmente por diminuir a burocracia e o tempo de tramitação das ações judiciais. Mas, para os advogados, ele ainda pode ser um grande problema. Dos 672,1 mil advogados registrados na OAB, apenas 68,8 mil têm certificados digitais para fazer peticionamentos eletrônicos e ter acesso à Justiça digital.
>
> Esse número representa pouco mais de 10% de todos os profissionais do país, segundo dados da Certisign, empresa que emite a maior parte dos certificados para os advogados. Por outro lado, é uma cifra que cresce com relativa rapidez. A Certisign cadastrou 31,9 mil novos registros entre janeiro e agosto deste ano, o que já é um salto de 28% em relação ao ano passado inteiro, com 24,8 mil novos certificados digitais. Frente 2009, porém, o ano de 2010 registrou um crescimento de quase 120%.
>
> **Paulo Cristóvão Silva Filho**, juiz auxiliar do Conselho Nacional de Justiça, entretanto, lembra que existem outras entidades certificadoras no país. Sendo assim, ele afirma que o Brasil tem entre 200 mil e 250 mil advogados ativos, segundo a OAB. Desses, cerca de 35 mil têm certificações digitais, o que dá em torno de 20% — ainda baixo, segundo ele. Entre as entidades que registram certificações, estão Serpro, Caixa Econômica Federal e a Associação dos Advogados de São Paulo (Aasp).
>
> O número ainda é baixo, segundo Paulo Cristóvão, mas é porque ainda não há a obrigatoriedade do certificado. "Há uma acomodação natural de permanecer com o *status quo*", afirma. Quando houver a obrigatoriedade, prevê, essa demanda vai aumentar naturalmente.
>
> O juiz auxiliar informa que o CNJ e o Judiciário ainda não tornaram as certificações obrigatórias a pedido da OAB. A Ordem, diz, quer que antes sejam feitas mais campanhas de inclusão digital e de redução de preços, para que depois haja a obrigação. Uma certificação digital da Certisign, já impressa num chip na carteira da OAB, sai por R$ 120. Uma leitora do chip custa, em média, R$ 160.
>
> **Injustiça digital**
>
> Segundo o presidente do Conselho Federal da OAB, **Ophir Cavalcante**, no entanto, os números da Certisign são "injustos". Ele explica que alguns tribunais criaram sistemas de cadastro, por meio de login e senha, sem exigir certificados digitais, e muitos advogados os usam. E esses não são computados nos dados da companhia certificadora.
>
> Mesmo assim, Ophir reconhece que a advocacia anda a passos lentos em direção à inclusão digital. Ele aponta dois fatores principais: resistência cultural e falta de estrutura do Judiciário e dos tribunais. O último motivo, diz, é técnico e passa pela falta de "maquinário adequado" da maior parte dos tribunais brasileiros, que não têm condições de armazenamento de arquivos, ou computadores suficientes. "Há sistemas que não aguentam processos com mais de mil páginas, por exemplo."
>
> Paulo Cristóvão, do CNJ, entretanto, afirma que a maioria dos tribunais faz isso propositadamente. Eles impõem limites de tamanhos de documentos que podem ser peticionados eletronicamente, como é o caso do Supremo Tribunal Federal, que permite 10 MB por documento. "Imagine que você peticiona um arquivo mil páginas, ou uns 20 MB, mas a pessoa que vai receber tem uma conexão de internet discada. Os tribunais fazem isso para garantir o direito de defesa, para que todos possam ter acesso a todos os documentos."

[36] Conjur. Disponível em: <http://www.conjur.com.br/2011-set-24/advocacia-ainda-nao-preparada-processo-eletronico.> Acesso em: 29 set. 2011.

Quanto à resistência cultural, Ophir Cavalcante, da OAB, explica que a maior parte dos advogados vem de gerações que não estão acostumadas com o computador. Passaram toda sua vida profissional lidando com processo em papel, e de repente têm de lidar com documentos digitais, em telas de computadores. Isso, inclusive, exige uma série de investimentos "anormais" aos advogados, como scanner, ou a máquina leitora de certificados digitais.

"Falta de sensibilidade"

Esses investimentos, continua Ophir, são outro motivo importantíssimo para o atraso dos advogados, em relação ao Judiciário, no processo eletrônico. "Pessoas físicas não têm a mesma velocidade de investimento que o Estado, que já gastou milhões de reais com diversas versões diferentes de programas", explica.

Parte desses investimentos foi nos chips das carteirinhas, onde vêm inscritos os certificados digitais. Ophir Cavalcante informa que, há dois anos, o Instituto de Tecnologia da Informação do governo federal (ITI) optou por uma tecnologia de certificação. Ano que vem, porém, essa tecnologia-padrão vai mudar, de novo por determinação do ITI, segundo o presidente do Conselho da OAB.

Ou seja: "os advogados tiveram de gastar dinheiro com esses chips, para refazer suas carteirinhas [um certificado digital custa R$ 120], e agora vão ter de gastar de novo por essa falta de sensibilidade do governo com o assunto", reclamou o advogado.

Desigualdade regional

Os estados também são diferentes em relação à inclusão digital dos advogados. O Paraná é o estado mais conectado, com 54% de seus profissionais com registros na Certisign — ou 20,8 mil pessoas, dos quase 40 mil advogados do estado.

O paranaense **José Ricardo Cavalcanti de Albuquerque**, da Comissão de Direito Eletrônico do Conselho Federal da OAB, defende a teoria de que os advogados não têm certificados digitais porque não são obrigados. Ele explica que o alto índice de advogados com certificado de seu estado se dá por conta da Justiça do Trabalho local. Lá, conta, quase 80% dos tribunais trabalhistas já são inteiramente digitais. Além disso, todos os Juizados Especiais Federais já são adeptos do processo eletrônico.

Além disso, a OAB paranaense começou, em 2009, a criar centros de inclusão digital para ajudar os advogados a entrar no mundo da tecnologia. Nesses lugares há computadores, leitoras de certificados e profissionais qualificados a ajudar quem ainda não conseguiu se entender com o peticionamento eletrônico.

José Ricardo Albuquerque era o coordenador da Comissão de Direito Eletrônico da OAB-PR na época. Ele lembra que o programa surgiu por causa da falta de estrutura fornecida pelo Judiciário para que os advogados passassem a se certificar. "Infelizmente, os tribunais não se concentram tanto em dar essa estrutura, e aí a OAB arcou com o custo dessa responsabilidade."

A OAB do Rio de Janeiro teve idéia semelhante. Decidiu, por iniciativa da Caixa de Assistência dos Advogados do Rio (Caarj), no fim do ano passado, criar os centros de inclusão digital e dar aulas gratuitas para os advogados. As mesmas aulas foram gravadas em vídeo e hoje são transmitidas no site da entidade. Além disso, vendem a certificação pelos R$ 120 exigidos pela Certisign e fornecem as leitoras gratuitamente.

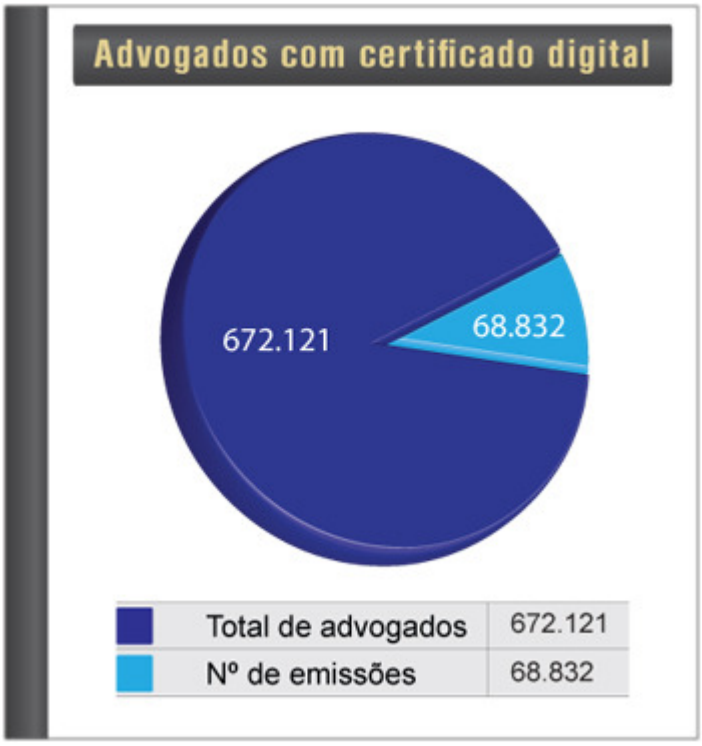
O resultado foi um salto na quantidade de advogados com certificados digitais. No ano passado, eram 1,3 mil certificados, e só até agosto deste ano, a cifra já pulou para 10,7 mil. Hoje, 11% dos advogados fluminenses têm a certificação da OAB, fornecida pela Certisign.

Dois pesos

> Já São Paulo, pelos dados da Certisign, é praticamente um estado no papel. Dos 226 mil advogados registrados na OAB, apenas 5,9 mil têm a certificação da companhia. Ou seja: 89% dos advogados paulistas não têm condições de peticionar eletronicamente.
>
> Acontece que a maiorias das certificações digitais do estado é feita pela Associação dos Advogados de São Paulo (Aasp), por meio da Imprensa Oficial de SP. A entidade tem 17 mil de advogados certificados. Levando em conta que a Aasp tem 90 mil advogados cadastrados.
>
> Mas não é a obrigatoriedade que explica São Paulo, e sim a concorrência. Enquanto, a certificação da Certisign custa R$ 120, fora os custos da leitora, a Aasp oferece um pacote que sai mais de R$ 100 mais barato. O advogado pode, em SP, comprar a certificação, a carteirinha (no caso da Aasp, a certificação não fica na carteirinha da OAB, mas num documento separado) e a leitora saem por R$ 99.
>
> Segundo o CNJ, é, sem dúvida, o preço mais barato do mercado. Onde não há pacotes, o advogado é obrigado a gastar, em média, R$ 240 para se certificar.

A matéria acima discorre bem sobre o tema e ainda ilustra bem a situação da certificação digital dos advogados quando apresenta os quadros a seguir:

Quadro 4 – Gráfico percentual advogados com certificação digital



Fonte: Conjur[37]

[37] Disponível em: <http://www.conjur.com.br/2011-set-24/advocacia-ainda-nao-preparada-processo-eletronico.> Acesso em: 29 set. 2011

Quadro 5 – Gráfico percentual advogados com certificação digital por estado.

Estado	Total de advogados (OAB)	Certificados digitais de 2010 (Certisign)	Certificados digitais até agosto de 2011 (Certisign)
Paraná	38.506	9.046	7.259
Rio de Janeiro	115.096	1.355	10.740
São Paulo	226.005	2.464	2.409

Fonte: Conjur[38]

De fato, parece que o problema não está só na questão financeira dos certificados, mas passa também pela obrigatoriedade do advogado possuir tal assinatura digital. É que enquanto essa necessidade for dispensável pelos sistemas de processo eletrônico que dispensam o seu uso, comodamente não se verá aumento desses números.

Digno de nota, ainda, que a certificação digital é inservível para fins de compartilhamento nas bancas jurídicas. Não se trata de software ou hardware compartilhável, mas sim de uso personalíssimo e individual, tal qual a própria carteira da Ordem.

Pode-se mesmo dizer que o certificado digital é o documento que atesta, no mundo virtual, ser o advogado quem é no mundo real. E se no mundo real não há "empréstimo" da Carteira da OAB, também não existe tal prática na internet.

Sobre o tem o próprio STJ em recente posicionamento deu a exata dimensão da necessidade da assinatura digital – e não a eletrônica, mais comum e barata – no processo quando assim pontuou:

> EMBARGOS DE DECLARAÇÃO NOS EMBARGOS DE DECLARAÇÃO. RECURSO ESPECIAL. PETIÇÃO DIGITAL. **FALTA DE IDENTIDADE ENTRE O NOME DO ADVOGADO INDICADO NA PEÇA RECURSAL E A ASSINATURA ELETRÔNICA. RECURSO INEXISTENTE**.
>
> 1. **Inexiste recurso na hipótese em que não há identidade entre a assinatura digital constante do documento enviado eletronicamente e o nome do advogado indicado como autor da petição** (arts. 1º, § 2º, III, da Lei n. 11.419/2006 e 18, § 1º, c/c o 21, I, da Resolução STJ n. 1 de 10.2.2010).
>
> 2. Embargos de declaração não conhecidos.
>
> (EDcl nos EDcl no REsp 1128778/BA, Rel. Ministro JOÃO OTÁVIO DE NORONHA, QUARTA TURMA, julgado em 02/08/2011, DJe 09/08/2011) – grifos nosso.

[38] Disponível em: <http://www.conjur.com.br/2011-set-24/advocacia-ainda-nao-preparada-processo-eletronico.> Acesso em: 29 set. 2011

Observe-se que o recurso sequer existiu, não se tratando de requisito ou condição no plano da validade ou eficácia, mas sim da existência. Seria forçoso concluir daí que os atos eletrônicos praticados sem certificado digital no PROJUDI ou e-Proc também inexistem, pois que se estaria diante de um prejuízo maior aos jurisdicionados que já obtiveram a tutela pretendida, mas nota-se a importância da segurança proporcionada pela assinatura digital ao documento eletrônico, seja como peça processual, seja como prova.

Com efeito, nota-se que a prova no processo eletrônico, necessariamente passa pelo conceito de documento eletrônico. Este, por seu turno, exige pré-requisitos tecnológicos, a fim de que se possa aferir sua autoria (seja do usuário que o inseriu, seja daquele que efetivamente produziu), autenticidade e integralidade, posto que sem os mesmos o risco e insegurança permeará o procedimento.

4 IMPUGNAÇÃO DA PROVA DOCUMENTAL NO PROCESSO ELETRÔNICO

Inegável e indubitável que o processo eletrônico em si, bem como o uso do documento eletrônico. Rechaçando qualquer dúvida sobre existência e utilização de ambos, Alexandre Atheniense[39], em um breve artigo pontua:

> A Lei da Informatização do Processo Judicial encerrou a discussão sobre a validade dos documentos eletrônicos no processo judicial. O conceito de documento eletrônico, principalmente como pensam muitos no universo jurídico, não pode ser limitado à imagem digitalizada de um escrito, como muitos pensam. Seu alcance é muito mais amplo, se considerarmos como a indicação de um fato com suporte em uma seqüência de bits, captada pelos nossos sentidos com uso de um equipamento e um software específico nos transmite uma determinada informação.
>
> A nova Lei, dentre outras inovações, deu um passo importante para consagrar o princípio da fé pública do advogado na juntada de peças, para admitir que qualquer documento eletrônico anexado aos autos por este terá sua fé reconhecida. O advogado poderá declarar as peças juntadas no processo eletrônico como autênticas sob sua responsabilidade pessoal e, caso haja qualquer questionamento neste sentido, é necessária a interposição de argüição de falsidade. É certo que esta regra afetou diretamente o interesse dos notários que tinham grande expectativa de prestar serviço na autenticação de documentos gerados em formato digital. Pelo texto da lei está claro que este serviço será, portanto, dispensável.
>
> Outra agilidade promovida pela lei é quanto ao intercâmbio de dados entre os órgãos do Poder Judiciário facultando aos atores processuais juntar ao processo extratos digitais, que nada mais são que relatórios emitidos por base de dados, como por exemplo, um extrato eletrônico de instituição bancária relatando sobre o fundo de garantia de certa pessoa. Esse intercâmbio vem sendo muito utilizado no que se refere à penhora on line, regulamentada pelo Código de Processo Civil, na qual o juiz requisita ao banco, onde o devedor tem conta, o bloqueio de certa quantia de dinheiro. Para o envio do extrato digital não será necessário à impressão destes dados em papel, será suficiente a remessa do extrato em formato digital por meio eletrônico, através de requisição do juiz, eliminando a perda de tempo com a burocracia gerada pelas rotinas inerentes ao manuseio do papel. Os extratos digitais e os documentos digitalizados terão a mesma força probante dos originais, desde que não seja comprovada qualquer fraude.
>
> Uma dúvida recorrente quando tratamos de digitalização de documentos reside ao fato de qual será o prazo de preservação do documento digitalizado cujo original tiver sido gerado em papel. O legislador determinou que estes sejam preservados pelos detentores até o transito em julgado da sentença ou até o prazo final para a interposição da ação rescisória.
>
> A prova no processo judicial é extremamente importante na medida em que contribui, diretamente, para a formação do convencimento do julgador acerca da lide. Porém as provas obtidas por meio eletrônico ainda encontram forte resistência para serem aceitas formalmente nos processos judiciais, o que potencializa as dúvidas quanto ao valor probante destas frente às provas tradicionais. Entretanto, quanto ao valor probante, não há de se questionar diferenças existentes entre a prova tradicional e a obtida pelo meio eletrônico. Apenas pode ser discutida a idoneidade e a veracidade dos dados armazenados, da mesma forma que é questionável o conteúdo de um documento tradicional.

[39] Obtido por meio eletrônico. ATHENIENSE, Alexandre Rodrigues. *Documentos eletrônicos no processo digital*. Conteudo Juridico, Brasilia-DF: 06 mar. 2009. Disponivel em: <http://www.conteudojuridico.com.br/?artigos&ver=2.23320>. Acesso em: 30 out. 2011

As provas obtidas por meio eletrônico diferem das demais apenas quanto à forma de armazenamento, já que acompanhando o avanço da tecnologia da informação, o armazenamento das informações passaram do papel para os bits, substituindo a grafia tradicional e o uso do papel pelos impulsos eletrônicos.

A aceitação das provas, nesta modalidade, pelo ordenamento jurídico brasileiro é garantida pela regra genérica, prevista no artigo 332, do Código de Processo Civil, segundo a qual os "meios legais" equivalem aos "moralmente legítimos" considerando todos "hábeis para provar a verdade dos fatos em que se funda a ação ou a defesa" ainda que não previstos expressamente no Código. Pelo artigo 225 do Código Civil, é ainda possível afirmar que "quaisquer reproduções eletrônicas" fazem prova plena desde que não haja impugnação pela sua exatidão. Portanto, o aspecto essencial a ser analisado quanto às provas é o seu conteúdo, se este viola ou não norma material ou constitucional. O formato da prova não deve ser questionado, pois o conteúdo probatório terá valor seja armazenado em papel, ou em meio eletrônico.

Um aspecto relevante que poderá ser questionado em relação aos meios de prova informatizados, é quanto à idoneidade dos dados, pois apesar de todos os meios de proteção disponíveis a esse tipo de armazenamento de dados, estes ainda poderão ser passíveis de modificações. Tendo em vista esse aspecto torna-se conveniente o emprego de meios eletrônicos de autenticação, capazes de oferecer aferir maior confiabilidade, com uso da certificação digital, diante da possibilidade de identificação se um determinado documento eletrônico teve a seqüência binária alterada.

A certificação digital e a assinatura eletrônica são regulamentadas pela MP-2.200-2 que instituiu a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil). Sua finalidade é 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, que se refere a qualquer mecanismo, não necessariamente criptográfico. Os documentos assinados digitalmente, podem ser considerados como prova inequívoca e têm valor probante erga omnes. Mas ainda que o documento eletrônico não tenha sido assinado é possível verificar a autenticidade e integridade através da devida perícia técnica.

Entre as provas obtidas por meio eletrônico podemos citar as mensagens de correio eletrônico, textos veiculados em sites, as gravações de áudio, vídeo e imagem, fotos digitais, e outros dados armazenados em computadores ou outra mídia eletrônica, que podem ser utilizados para provar o fato alegado pela parte no processo. Uma das maiores dificuldades relacionadas com as provas obtidas na Internet é o seu perecimento, já que, por exemplo, um site que veicula informações denegrindo a honra de alguém, pode sair do ar de uma hora para a outra. Neste caso, a pessoa atingida poderia imprimir a página no momento que percebeu a ofensa, mas esse documento poderia gerar dúvidas. Cumpre destacar que nesse caso é possível a elaboração de uma ata notarial em relação a um ambiente eletrônico. Basta para isso, que a parte requeira a um Tabelião que relate os fatos que presenciou diante do monitor, comprovando a existência e todo o conteúdo visualizado, arquivando os endereços acessados, imprimindo as imagens coletadas no próprio instrumento notarial.

Por último, podemos realçar que, embora a lei não determine requisitos de aceitação do documento eletrônico, temos percebido que em algumas regulamentações está sendo limitado o tamanho dos documentos eletrônicos enviados, por questões de armazenamento, ou ainda, por ocupação das bandas de download e de upload. Tal questão é merecedora de futuras discussões para evitarmos o cerceamento de defesa que pode ocorrer nesta limitação imposta.

Desta forma, concluímos que o valor probante das provas obtidas por meio eletrônico é o mesmo dos meios tradicionais e a forma em que estão armazenados os dados em nada influi na licitude desta, podendo apenas existir graduação quanto à autenticidade dos dados gravados, interferindo assim no critério de caracterização sobre idoneidade

> da prova digital para distinguir se está é inequívoca ou não dependerá do cotejo de fatos e do livre convencimento do magistrado.
>
> **Esta modalidade de prova é cada vez mais freqüente, visto que a tendência é de que aumente o número de atos ilícitos e crimes pela internet, bem como seja difundido entre os tribunais a utilização do processo judicial eletrônico. Devem, os profissionais do Direito, aprimorar os seus conhecimentos quanto a este tipo de prova principalmente quanto aos meios de aferição de sua autenticidade o que por muitos, ainda é bastante desconhecido**. (grifos nosso)

Não restando dúvidas quanto à aplicabilidade prática da prova documental no processo eletrônico, impende consignar que nesta condição, passível é a mesma também de impugnação, nos termos e moldes da lei processual civil e da própria Lei 11.419.

Inicialmente, destaca-se que um documento indica um fato com um conteúdo representativo, e, na acepção de Carnelutti (2000, p. 514) "sendo a representação sempre obra do homem, o documento mais do que uma coisa, é um *opus* (resultado de um trabalho)". Assim, quanto à representatividade, intrínseco pensar em confiabilidade.

Sem dúvidas, a simples divisão dos documentos, em públicos e privados, demonstra uma diferença em relação à força probante de cada um deles, mormente o principio do livre convencimento motivado do juiz, tal divisão ainda hoje é relevante na valoração das provas, por ainda imprimir aos documentos públicos mais valor, na busca da verdade processual possível.

Destarte, a regra do artigo 373 do CPC é no sentido de que: "o documento particular, de cuja autenticidade se não duvida, prova que o seu autor fez a declaração, que lhe é atribuída", presumindo-se verdadeira a declaração feita pelo documento particular.

No mesmo sentido, o art. 225 do CC afirma serem: "as reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão."

Acrescente-se, ainda, a presunção de que goza o documento, desde que certificado digitalmente, na forma da MP 2200/01, quer públicos, quer privados, e tem-se, como regra, que a prova documental produzida em tais condições acima tem conteúdo válido até que se prove em contrário.

O que se objetiva com uma impugnação de uma prova documental, aqui incluso o documento eletrônico, é a sua falsidade ou sua autenticidade. De acordo com Castro (2000, p. 255): "É, em geral, indispensável, para que os documentos particulares façam prova em juízo, que a

parte que deles quer servir-se prove a verdade do seu objeto, se a parte contrária nega a sua veracidade".

Para o CPC, em seu artigo 387, a falsidade consiste em formar um documento não verdadeiro, ou alterá-lo, e a forma de sua impugnação é aquela prevista nos artigos 390 e seguintes do mesmo diploma legal:

> Art. 390. O incidente de falsidade tem lugar em qualquer tempo e grau de jurisdição, incumbindo à parte, contra quem foi produzido o documento, suscitá-lo na contestação ou no prazo de 10 (dez) dias, contados da intimação da sua juntada aos autos.
>
> Art. 391. Quando o documento for oferecido antes de encerrada a instrução, a parte o argüirá de falso, em petição dirigida ao juiz da causa, expondo os motivos em que funda a sua pretensão e os meios com que provará o alegado.
>
> Art. 392. Intimada a parte, que produziu o documento, a responder no prazo de 10 (dez) dias, **o juiz ordenará o exame pericial**.
>
> Parágrafo único. Não se procederá ao exame pericial, se a parte, que produziu o documento, concordar em retirá-lo e a parte contrária não se opuser ao desentranhamento.
>
> Art. 393. Depois de encerrada a instrução, o incidente de falsidade correrá em apenso aos autos principais; no tribunal processar-se-á perante o relator, observando-se o disposto no artigo antecedente.
>
> Art. 394. Logo que for suscitado o incidente de falsidade, o juiz suspenderá o processo principal.
>
> Art. 395. A sentença, que resolver o incidente, declarará a falsidade ou autenticidade do documento (grifo nosso).

Inexistindo impugnação ao documento, o mesmo há de ser considerado verdadeiro, gozando de presunção relativa, passível de modificação a qualquer tempo, desde que quando demonstrada a sua obtenção mediante erro, dolo ou coação (arts. 138 e ss, 141 e ss, 151 e ss, todos do CC, com o trato de cada vício, como defeitos do negocio jurídico). (MONTENEGRO FILHO, 2009, p. 465).

A norma processual determina a realização de perícia para a averiguação de sua autenticidade, cuja importância parece aumenta, quando o documento impugnado tratar-se de documento eletrônico, eis que o objetivo do perito será identificar as questões técnicas que, nestes casos, muito provavelmente irão ultrapassar o domínio intelectual do magistrado, eis que irá adentrará a ciência da informática.

Mister ainda destacar a questão da aferição temporal para a impugnação da prova documental no processo eletrônico. A relevância do tempo aqui pode ser crucial em inúmeros documentos eletrônicos, a exemplo da comprovação de propriedade intelectual, ou do cumprimento de um

prazo processual no sistema da Lei 11.419/06, que admite a sua entrega até as 24h (vinte e quatro horas) do dia fatal do protocolo.

Seria possível a aplicação do art. 370 do CPC para os problemas em relação a um documento particular não datado?:

> Art. 370. A data do documento particular, quando a seu respeito surgir dúvida ou impugnação entre os litigantes, provar-se-á por todos os meios de direito. Mas, em relação a terceiros, considerar-se-á datado o documento particular:
>
> I - no dia em que foi registrado;
>
> II - desde a morte de algum dos signatários;
>
> III - a partir da impossibilidade física, que sobreveio a qualquer dos signatários;
>
> IV - da sua apresentação em repartição pública ou em juízo;
>
> V - do ato ou fato que estabeleça, de modo certo, a anterioridade da formação do documento.

Esta regra parece ser suficiente para prova documental física, mas ao processo eletrônico não, considerando que os dispositivos computacionais de data e hora, tanto de criação quanto de modificação de um arquivo, por exemplo, refere-se às mesma informações do computador em que é criado, cuja alteração trata-se de uma das mais simples modificações ao usuário.

Neste sentido, a certificação digital é de extrema importância ao processo eletrônico, uma vez que a mesmo imprime maior segurança ao quesito tempo, tanto para o documento eletrônico em si, quanto a sua inserção nos autos do procedimento digital.

Noutro giro, além da autenticidade, importa à prova documental eletrônica, ainda, a sua autoria, isto porque o próprio CPC determinar que se a autoria de um documento não é explícita, considerar-se-á autor aquele que o assinou ou, acaso apócrifo, aquele que determinou sua realização, a exemplo dos livros comerciais e registros domésticos.

Ora, se os documentos cujo meio físico é o papel a assinatura de próprio punho define seu autor, o documento eletrônico terá por “assinatura” o certificado digital de quem o criou, apresentando sua procedência e dando a credibilidade necessária àquele documento.

Neste aspecto, impende consignar que o artigo 388 do CPC determina que se a veracidade da assinatura não puder ser comprovada, o documento particular perderá a sua fé:

> Art. 388. Cessa a fé do documento particular quando:
>
> I - lhe for contestada a assinatura e enquanto não se lhe comprovar a veracidade;
>
> II - assinado em branco, for abusivamente preenchido.

> Parágrafo único. Dar-se-á abuso quando aquele, que recebeu documento assinado, com texto não escrito no todo ou em parte, o formar ou o completar, por si ou por meio de outrem, violando o pacto feito com o signatário.

Crê-se perfeitamente aplicável à regra acima exposta aos documentos eletrônicos e à prova no processo eletrônico, sendo certo que os documentos e atos ali praticados sem assinatura digital hão de cessar a sua fé, já que esta deveria constitui requisito mínimo para a autoria do mesmo.

Patricia Peck Pinheiro (2009, p. 155) afirma que: "além de não existir nenhum óbice jurídico, o documento eletrônico assinado digitalmente torna factível a visualização de qualquer tentativa de modificação do documento por meio da alteração da sequência binária".

Não há, quer virtualmente, quer fisicamente, garantias de segurança ou de certeza absoluta de qualquer documento, a exemplo dos inúmeros golpes noticiados diuturnamente, com uso de CPF´s, certidões de óbito, e contratos sociais de empresas fantasmas. Contudo, a exigência da assinatura digital, assim como outros dispositivos de segurança, permitem ampliar essa segurança para limites adequados à manutenção da paz social, devendo cada um, individualmente, zelar e ser responsável pela segurança de suas senhas de modo a ajudar a coibir tais práticas, cada vez mais comuns (PINHEIRO, 2009, p. 164).

Assim parece que a impugnação à prova documental é cabível no processo eletrônico, seguindo a premissa estabelecida no artigo 390 do CPC. As dúvidas que começam a surgir são quanto forma e prazo de apresentação daquele incidente, conquanto algumas particularidades da mesma, em relação ao art. 11 da Lei do Processo Eletrônico, bem como a sua própria natureza a àquela dos sistemas de processo digital.

4.1 O ARTIGO 11 DA LEI 11.419/06

Augusto Marcacini, em 1998, escreveu um artigo que ainda é bastante apropriado ao entendimento do tema, onde, ao definir os conceitos, pontuou:

> ***b) O documento eletrônico diante do regime jurídico da prova documental.***
>
> Abordadas as questões em torno da autoria e autenticidade do documento eletrônico, em que medida é possível aplicar a eles as demais regras vigentes sobre a prova documental?
>
> Um primeiro ponto que passo a considerar diz respeito à data do documento. Além da data que pode estar mencionada no corpo do documento, consta também da assinatura

eletrônica a data e hora em que foi gerada. Aqui não temos qualquer diferença em relação ao documento físico: tanto um como outro podem ser falsamente datados pelos seus signatários. No caso da data constante da assinatura eletrônica, basta modificar a data do sistema (i.e., a data assumida pelo computador que está sendo utilizado para gerar a assinatura) e, em seguida, assinar o documento eletrônico. Por isso, aplicam-se integralmente ao documento eletrônico as disposições do art. 370 do CPC, com ressalva feita ao inciso III, pois a impossibilidade física que impede de assinar graficamente pode não impedir o sujeito de assinar eletronicamente[32-A].

Até que algum sistema seja juridicamente reconhecido como apto a provar - também por vias eletrônicas - a data dos documentos eletrônicos, pode-se pensar em publicar em jornal as suas assinaturas digitais. Ou, quem sabe, imprimi-las em uma folha de papel a ser apresentada ao Registro de Títulos e Documentos[32-B]. Sendo as assinaturas únicas para aquele documento, a certeza quanto à data daquelas prova a deste.

Se somente podemos assegurar a integridade do documento eletrônico mediante sua conferência com a correspondente assinatura, disto resulta que documentos não assinados são irremediavelmente suscetíveis de alteração. Como conseqüência, a previsão contida no CPC quanto a documentos não assinados é inaplicável aos documentos eletrônicos, pois é impossível provar-lhes a autoria e a veracidade.

Do mesmo modo, inexiste neste campo a possibilidade do documento ser assinado em branco e abusivamente preenchido. Qualquer preenchimento posterior, abusivo ou não, invalida a assinatura eletrônica.

Os pontos fracos do sistema residem basicamente na eventual apropriação indevida da chave privada e na autenticidade da chave pública. E isto traz repercussões no estudo da falsidade dos documentos eletrônicos.

Quanto a este primeiro problema, ele pode ser evitado na medida em que o titular da chave tome cautelas para sua proteção. Entretanto, nenhuma cautela é suficiente para evitar situações em que, mediante alguma forma de coação física, o sujeito seja obrigado a fornecer a sua chave privada e a "frase-senha"[33]. Mas o problema, aqui, é o mesmo do mundo físico: alguém poderia coagi-lo a subscrever um documento ou um cheque. De qualquer modo, é importante lembrar que se terceiros tiverem acesso à chave privada, poderão subscrever documentos como se fossem o seu verdadeiro titular, sem que isto deixe qualquer vestígio. Se por outros meios de prova puder ser demonstrado que houve a apropriação e uso ilícito da chave privada, deverá o juiz levar isto em conta, negando valor ao documento eletrônico.

Analisemos, agora, a questão da autenticidade da chave pública. Por autenticidade da chave pública queremos dizer a certeza de que ela provém do seu titular. Qualquer um poderia gerar um par de chaves e atribuir-lhe o nome de qualquer pessoa, existente ou imaginária[33-A]. A autenticidade do documento eletrônico é conferida sem dificuldade por qualquer usuário de computador, com o uso do programa de criptografia e de posse da chave pública do seu subscritor. Mas, e se a própria chave pública não for autêntica? Esta conferência o programa não tem como realizar. O que fazer, então, para contornar o problema?

Para solucionar controvérsias acerca da autenticidade de chaves públicas, podemos nos valer de uma série de procedimentos, que adiante proponho, e que permitirão relacionar uma dada chave pública a seu titular. Disto será tratado no próximo tópico. Por ora, continuemos com a problemática da falsidade de documentos eletrônicos.

Diante das linhas acima traçadas, é possível afirmar que, quanto a um documento assinado eletronicamente pelo uso de criptografia assimétrica, a argüição de falsidade só poderá ser baseada em *"falsidade de assinatura"*. Isto porque a adulteração do conteúdo do documento é inviável, vez que faz perder o vínculo entre este e a assinatura. Dentro deste prisma, é de se dizer que o documento eletrônico assim assinado é dotado de um maior grau de confiabilidade que o próprio documento tradicional. O próprio *software* de criptografia, ao conferir a assinatura, acusa que o documento adulterado não corresponde a ela. Já o documento cartáceo necessita de um exame pericial para constatar-se eventual alteração; e, com o evoluir da técnica, certamente surgem meios mais e mais poderosos para alterar documentos físicos.

Por *"falsificação da assinatura digital*" quero dizer a criação de um par de chaves falso, atribuído ao suposto signatário. A verdadeira assinatura digital, legitimamente gerada pelo seu titular, não tem como ser falseada[33-B]. No fundo, inexiste falsidade a ser apurada no próprio documento eletrônico; o problema em análise se resume exclusivamente na verificação da autenticidade da chave pública. Sabendo ser autêntica a chave pública, o próprio programa de computador permitirá conferir a autenticidade e integridade do documento eletrônico.

De quem seria o ônus da prova, se argüido que a chave pública não é autêntica? Tal alegação se assemelha com a hipótese do artigo 389, II, do CPC. Ao se alegar falsidade de assinatura do documento físico, assim como ao se alegar não-autenticidade da chave pública atribuída à parte, é questionada a autoria do documento. Assim, se podemos dizer, baseados neste artigo 389, II, que compete a quem produz o documento provar-lhe a autoria, a regra se estende a este caso. Compete à parte que produz o documento eletrônico provar a autenticidade da chave pública que afirma ser do suposto signatário, e com a qual iremos conferir a assinatura digital.

Por outro lado, diante da argüição de apropriação e uso indevido da chave privada verdadeira, o ônus da prova competirá a quem alegar este fato. Quando a segurança de uma chave privada for posta em dúvida, é possível que ela seja revogada. Alguns problemas, entretanto, podem ser vistos aqui: por primeiro, a necessidade de publicidade da revogação; em segundo lugar, a impossibilidade de se atribuir, por si só, certeza às datas da revogação ou da assinatura indevidamente efetuada pelo criminoso com o uso da chave privada apropriada. Daí, talvez o problema da datação de documentos eletrônicos deva ser observado com o máximo de cautela e, no mais das vezes, será conveniente estabelecer meios seguros de provar a data do documento eletronicamente assinado[33-C]. Voltarei, adiante, a abordar este problema, no item "d", infra.

Para encerrar mais este sub-item, analisemos as relações entre o documento eletrônico original e as cópias físicas dele extraídas. Como já afirmado anteriormente, a cópia em papel do documento eletrônico não exibirá qualquer assinatura, mas apenas o conteúdo do documento. Mesmo assim, reiterando o que foi afirmado ao final do tópico anterior, tal cópia não será desprezível enquanto meio de prova. A parte poderá juntá-la aos autos, afirmando ser a reprodução de documento cujo original se encontra em meio eletrônico, devidamente subscrito pelas partes mediante assinatura digital. Não impugnada pela parte contrária a conformidade da cópia juntada aos autos, terá ela o mesmo valor probante que o original. Contestada a veracidade da cópia, necessário será fazer-se o confronto com o original eletrônico; mas a parte que levianamente argüir sua falsidade poderá ser considerada litigante de má-fé, nos termos e nas circunstâncias já aludidos acima.

c) Da força probante dos documentos eletrônicos: dependência ou não de alterações legislativas?

Embora já existam normas a respeito de assinaturas digitais em ordenamentos jurídicos estrangeiros, no Brasil nada há a tratar da matéria. Até o momento em que escrevo estas linhas, a única norma nacional que menciona este tipo de assinatura é a Instrução Normativa nº 17, de 11 de dezembro de 1996, editada pelo Ministério da Administração Federal e Reforma do Estado. Ainda assim, tal ato apenas se resume a determinar que *"no prazo de 360 (trezentos e sessenta) dias serão implementadas aplicações que tratem da utilização de documentos eletrônicos e do uso de assinatura digital"* (art. 4, § 6º), no âmbito das atividades governamentais.

Temos, também, em trâmite, o Projeto de Lei nº 2.644/96, apresentado pelo deputado Jovair Arantes, que faz menção ao uso de documentos e assinaturas eletrônicos[34]. O projeto, porém, é bastante tímido, e, em apenas oito artigos praticamente se resume a reconhecer a existência de documentos e assinaturas eletrônicos.

Em seu artigo 1º, o projeto diz que: *"Considera-se documento eletrônico, para os efeitos desta Lei, todo documento, público ou particular, originado por processamento eletrônico de dados e armazenado em meio magnético, optomagnético, eletrônico ou similar"*. A disposição peca pelo equívoco lógico de

definir uma coisa a partir dela própria (*"documento eletrônico... é todo documento..."*). No artigo 2º, temos que *"Considera-se original o documento eletrônico autenticado por assinatura eletrônica, processado segundo procedimentos que assegurem sua autenticidade e armazenado de modo a preservar sua integridade"*. Ao dizer que o documento eletronicamente assinado é considerado "original", pouco significado jurídico contém o artigo. Seria mais preciso dizer que tal documento eletrônico, assim assinado, terá a mesma eficácia do documento físico. Mesmo porque, conforme exposto anteriormente, não há significado em buscar distinguir, entre documentos eletrônicos, qual é o original. Os demais artigos nada acrescentam ao tema, limitando-se a prescrever deveres do administrador do sistema de computadores e a tipificar penalmente algumas condutas.

A primeira lei, no mundo, a regulamentar o uso de assinaturas eletrônicas provém do Estado de Utah, nos Estados Unidos, tendo entrado em vigor em 1995[35]. Trata-se de uma lei extensa e extremamente detalhista. Com estrutura e técnica diversas daquelas empregadas na nossa legislação, esta lei contém toda uma seção destinada a estabelecer definições várias - são, ao todo, trinta e sete definições -, que vão desde conceitos técnicos publicamente conhecidos, como *bit* ou *criptografia assimétrica*, até o significado de *assinatura digital*. Em linhas gerais, a lei estabelece qual deve ser o conteúdo dos "certificados de autenticidade" das chaves públicas, quem pode exercer as funções de *"certification authority"*, como estes entes deverão operar, seus deveres e responsabilidades, que critérios devem ser observados para expedição do "certificado de autenticidade", como se dá a suspensão, revogação e expiração destes certificados, bem como quais são os efeitos de uma assinatura digital, para destacar os temas mais relevantes.

Em seguida, também em 1995, entrou em vigor na Califórnia lei regulamentando o uso de assinaturas eletrônicas[36]. Menos abrangente do que a do Estado de Utah, que se aplica a qualquer pessoa que queira se utilizar de assinaturas digitais, a legislação da Califórnia é voltada apenas ao uso de assinaturas eletrônicas em documentos apresentados a órgãos públicos[37]. Muito mais enxuta, esta lei define apenas o que se entende por "assinatura digital", atribuindo-lhe a mesma força e efeitos de uma assinatura manual, e declarando que seu uso é opcional.

Hoje, em quase todos os cinqüenta estados norte-americanos há lei, ou em vigor, ou em estudo, tratando da utilização de assinaturas digitais. Ao redor do mundo, podemos mencionar a existência de recente legislação já aprovada a este respeito, em 1997, na Alemanha, Itália e Malásia[38] e, aqui na América Latina, a Argentina recentemente adotou norma a permitir o uso de assinatura digital perante os órgãos públicos[39], à semelhança da legislação californiana.

Antes, porém, de propor alterações legislativas, ou a criação de serviços especializados por parte de órgãos públicos, partirei da nossa realidade atual, estabelecendo critérios pelos quais, mesmo hoje, um documento assinado eletronicamente pode ser aceito como prova.

Como já abordado nos itens precedentes, é perfeitamente possível enquadrar o documento eletrônico na teoria e disposições legais relativas à prova documental. Assim, com as considerações mais que farei a seguir, concluo ser possível desde já utilizar documentos eletrônicos como prova de atos e fatos jurídicos, pois nenhuma afronta é feita ao nosso sistema jurídico. Todavia, algumas cautelas ou formalidades a mais haverão de ser tomadas, enquanto não houver disposição legal acerca do uso e validade das assinaturas digitais. E, por outro lado, é forçoso admitir que o documento eletrônico não poderá ser *sempre* utilizado em substituição do documento cartáceo, na falta de alguma regulamentação estatal.

O maior problema a solucionar está relacionado com a autenticidade da chave pública. Diante da atual falta de qualquer meio institucional para dar fé pública a uma chave pública, nada impede que duas partes troquem suas chaves públicas e, por meio de um documento físico, reconheçam validade e eficácia das assinaturas e documentos eletrônicos que puderem ser conferidos por meio destas chaves. Seria essencial, neste documento físico, imprimir as chaves públicas que estão sendo trocadas (é possível imprimi-las em papel, embora sua aparência - uma longa e

incompreensível seqüência de caracteres - seja um tanto quanto exótica), ou, ao menos, dados que as identifiquem tais como o tamanho da chave utilizada, seu identificador (*"key ID")* e suas *"fingerprints"*[40], o que, aliás, será mais racional[41].

Diante de tal documento prévio, e considerando-se a liberdade de contratar, entendo que os documentos eletrônicos futuramente assinados pelas partes servirão plenamente como prova, e não será possível a qualquer dos contratantes repudiar a chave pública utilizada para conferir as assinaturas digitais[41-A].

Eventualmente, será possível atribuir autenticidade a chaves públicas por meio de sua notoriedade. Para citar um exemplo, as chaves públicas do criador do PGP acompanham o programa, de modo que milhares de usuários ao redor do mundo a conhecem. Em nota anterior, neste artigo, divulguei a *"Key ID"* e a *"fingerprint"* de minhas chaves, de modo que isto poderia ser levado em conta para demonstrar qual é a minha chave pública. Em situações tais, competiria ao juiz analisar o quão notória é, de fato, a chave pública do signatário e, baseado na sua prudência e bom senso, atribuir-lhe ou não autenticidade conforme as peculiaridades do caso.

Futuramente, a prova de autenticidade de chaves públicas poderá ser feita por *"certificados de autenticidade"* emanados de um terceiro a quem se atribuir fé pública para fazê-lo. A este oficial, tem-se atribuído a designação de "Cibernotário".

Resolvido o problema da autenticidade da chave pública, a autenticidade do documento eletrônico é fato que pode ser verificado por qualquer pessoa, por meio do programa de criptografia que a utiliza.

Concluo, pois, que nada há a impedir a utilização de documentos eletrônicos, seja como forma para se documentar atos jurídicos, seja como meio de prova a ser produzido em juízo. Até porque, nos termos do artigo 332, do CPC, *"todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis a provar a verdade dos fatos, em que se funda a ação ou a defesa"*. Não me parece imoral o uso de documentos eletrônicos, razão pela qual não haveria porque restringir sua utilização... Muito menos ilícito, não afrontando, igualmente, o artigo 5º, inciso LVI, da Constituição Federal. Evidentemente, além de moralmente legítimo, o meio de prova deve mostrar-se idôneo a permitir o convencimento. Daí, documentos eletrônicos sujeitos a alteração ou a serem "fabricados" unilateralmente pela parte a quem aproveitam não podem ser dotados de força probante. Este não é o caso, como se viu acima, dos documentos eletrônicos "assinados" mediante uso da criptografia assimétrica. Sua utilização como meio de prova é, então, perfeitamente possível, em face do sistema jurídico já existente.

Este entendimento é o que mais se ajusta ao espírito do Código de 1973 que, segundo ensina Humberto Theodoro Junior, *"foi muito mais liberal do que o anterior e, em matéria de meios de prova, mostrou-se consentâneo com as tendências que dominam a ciência processual de nossos dias, onde, acima do formalismo, prevalece o anseio da justiça ideal, lastreada na busca da verdade material, na medida do possível"*[42].

As dificuldades que encontramos na plena equiparação do documento eletrônico ao documento tradicional residem na falta de alguma regulamentação, seja legislativa, seja meramente administrativa, de seu uso e aceitação por parte de entes públicos. Assim, atos notariais como a elaboração de instrumentos públicos em forma eletrônica, a autenticação de cópias físicas de documentos eletrônicos - ou vice-versa -, o *"reconhecimento"* das chaves públicas, a certificação da data dos documentos eletrônicos, ou outras participações possíveis que o tabelião possa ter na formação ou comprovação de documentos digitais dependerão de algum tipo de regulamentação, senão legislativa, ao menos administrativa[42-A].

Igualmente, o uso de documentos eletrônicos pela Administração Pública dependerá de algum tipo de previsão normativa prévia, dado o princípio da legalidade que orienta a atuação dos órgãos públicos[42-B].

Nenhum óbice, porém, existe a impedir o uso de documentos particulares eletrônicos, observadas as providências acima expostas, que permitam demonstrar a autenticidade da chave pública e a intenção das partes em atribuir eficácia à assinatura digital. Neste campo, a existência de prévia lei não se mostra um imperativo, mas, certamente, um

futuro tratamento legislativo será bem-vindo, para o fim de definir com clareza qual a eficácia e a validade de assinaturas e documentos eletrônicos, que requisitos eles deverão conter, ou quais os direitos e deveres daqueles que criam, certificam, ou se utilizam de chaves eletrônicas. Por isso, embora o Projeto de lei nacional acima mencionado tenha seus méritos pelo pioneirismo e iniciativa, é de se reconhecer sua carência no trato de vários aspectos juridicamente relevantes.

Além de permitir um regime uniforme e de normatizar uma série de novas situações que advirão da popularização dos documentos eletrônicos, uma futura lei ainda servirá para pôr abaixo eventuais resistências e desconfianças que ainda possam subsistir quanto ao seu uso e valor probante.

e) Considerações finais sobre a prova por documentos eletrônicos.

Diante de tudo o que foi acima exposto, claro está que existe, nos dias de hoje, técnica hábil a tornar o documento eletrônico algo no mínimo tão seguro quanto os documentos tradicionais. E, principalmente, o uso de documentos eletrônicos e assinaturas criptográficas pode ser plenamente recepcionado pela nossa ordem jurídica.

[...]

Hoje em dia, disseminou-se intenso comércio por meio da Internet, em que contratos são firmados mediante um simples clicar do *mouse*, considerado este ato como aceitação das cláusulas estabelecidas em uma página da *World Wide Web*. O usuário simplesmente preenche alguns campos com seus dados pessoais, escolhe o produto ou serviço que deseja e, ao final, *"aperta"* um botão virtual que remete todas estas informações à outra parte, manifestando, com este ato, a sua vontade.

É evidente que um contrato assim firmado é plenamente válido, condicionado apenas à observância das mesmas disposições que regem os contratos em geral e as relações de consumo. Discussões acerca do momento do seu perfazimento, da lei aplicável, do local do pagamento, da tributação, ou outras mais, certamente podem surgir no plano do direito material e devem ser motivo de estudo por parte dos civilistas, comercialistas ou tributaristas. Não é este o objetivo deste meu estudo e, por isso, restringir-me-ei a abordar o problema da *prova* destes contratos.

Ora, em nenhum momento, no perfazimento destes contratos, é exarado qualquer sinal que possa ser considerado como *assinatura*, ou seja, um identificador *único e exclusivo* de seu titular. Por isso, qualquer um poderia tê-lo enviado, que não a pessoa ali declarada. De outro lado, os termos em que o contrato é firmado também não estão documentalmente provados: os dizeres que contém uma página da WWW podem ser instantaneamente alterados; o que estava escrito ontem pode não ser o mesmo que ali encontramos hoje, sem que isto deixe vestígios materiais.

Assim, não se pode atribuir força documental a qualquer registro que tenha sido gerado no servidor que recebeu esta proposta. O registro, em poder de uma parte, e sem a inalterabilidade conferida pela assinatura criptográfica *da outra parte*, é amplamente suscetível a modificações. Além disso, não se tem a menor certeza acerca da identidade da pessoa com quem se contratou. Não se quer dizer com isso que tais contratos não existam, que sejam inválidos, nem que não possam ser provados. O que temos em mãos, porém, é um contrato cuja forma se assemelha à forma verbal (ou, mais próximos ainda, do contrato verbal firmado por telefone, em que os contratantes sequer se põem face à face). Por isso, tal contrato se perfaz do mesmo modo que um contrato verbal, e poderá ser provado por todos os meios admitidos em direito. O que não teremos, todavia, é a prova documental do negócio jurídico efetuado. Convém mencionar que aqui incluo os chamados *"sites seguros"*. Nestes, são utilizados processos criptográficos tão somente para conferir sigilo aos dados inseridos, de modo que as informações pessoais do usuário não possam ser interceptadas e lidas por um intruso. A criptografia aplicada nestas páginas eletrônicas serve apenas para dar privacidade à transmissão, mas não gera uma assinatura digital, que torne imutável o conteúdo do documento eletrônico, ou permita alguma conclusão sobre a autoria da mensagem.

Outro aparente “registro” merece ser aqui desnaturado como documento. O *software* de correio eletrônico mantém arquivados no computador do usuário todas as correspondências recebidas ou enviadas, ao menos até que sejam por ele voluntariamente apagadas. Como a maioria dos *softwares* de correio eletrônico não permite editar estes registros, isto pode dar ao usuário de computador menos experiente a falsa sensação de que são seguros ou não adulteráveis.

Igualmente, afirmo que se a correspondência recebida não estiver assinada eletronicamente, por processo criptográfico, difícil será emprestar-lhe a força de prova documental, ou mesmo atribuir-lhe qualquer força probante. Isto porque estes registros podem ser unilateralmente alterados de modo *extremamente fácil*.

Em primeiro lugar, há alguns *softwares* de correio eletrônico que editam seus registros. Basta que se utilize um destes programas, para que qualquer usuário iniciante altere todo o conteúdo, data, ou mesmo remetente da mensagem enviada ou recebida que esteja arquivada no seu próprio computador. Em segundo lugar, é possível editar os registros com um editor hexadecimal, caso o próprio programa não tenha função de edição. O editor hexadecimal é um tipo de programa de computador que acredito ser desconhecido pela maioria dos profissionais do Direito e, por isso, teço aqui algumas considerações a seu respeito, a fim de facilitar a compreensão da fragilidade dos registros. Lembro, porém, que qualquer profissional da área técnica, bem como alguns usuários mais experientes, conhecem este tipo de programa, comumente utilizado por programadores de computador. Um editor hexadecimal permite editar *qualquer* arquivo eletrônico, *byte* por *byte*. Assim, não deve o leitor se iludir com o fato de que o programa de correio eletrônico não edite seus próprios registros: um editor hexadecimal, nas mãos de quem saiba operá-lo, pode editá-los com a mesma facilidade com que um processador de textos altera seus documentos.

Assim, sem grande dificuldade, pode um missivista adulterar todo o conteúdo dos seus registros, incluindo-se, aqui, a indicação do remetente. Tanto se pode adulterar a mensagem recebida como se pode fraudar a autoria de uma mensagem contida nos registros. E tudo sem deixar marcas. E não se diga que poderíamos confrontar os registros dos dois contratantes, pois, diante da disparidade, não temos condições de dizer qual dos dois é o registro falseado, e qual é o verdadeiro, o que torna a constatação algo inócuo como meio de prova.

Concluo, pois, que sem o uso de assinatura criptográfica, nenhum valor probante têm os registros dos *e-mails* enviados ou recebidos arquivados no computador do usuário.

Menos sujeitos a adulterações tão simples, mas também não invioláveis, são os sistemas em que se tem cadastro de senhas de acesso. E, na Internet, tais sistemas têm proliferado bastante, para uso de serviços disponibilizados aos consumidores, entre os quais o próprio acesso ao provedor. Nem sempre estes sistemas são seguros. E, além disso, não vejo aqui, igualmente, a formação de uma prova eletrônica confiável, para ser exibida em juízo. Isto porque a senha não é de conhecimento exclusivo do seu titular. Alguém, que tenha - ou ilicitamente obtenha - acesso privilegiado ao sistema poderá se apropriar da senha alheia e utilizá-la indevidamente. Uma grande preocupação na Internet é a invasão de sistemas por *hackers*, que astuciosamente, e com boa experiência em informática, volta e meia logram descobrir a senha de acesso de algum usuário cadastrado, sem que este tenha minimamente contribuído para isso. Ou, se o próprio sistema autoriza a seus administradores ou operadores o acesso às senhas alheias, a idoneidade destes funcionários pode ser um ponto fraco na segurança.

Sobre tais problemas, são dignos de menção dois acórdãos que enfrentaram questões semelhantes:

No primeiro, apreciou-se ação de anulação de débito movida em face da TELESP, envolvendo dívidas contraídas mediante contrato de financiamento de contas telefônicas, conhecido por “Telecard”. Por este sistema, o usuário pode efetuar ligações para qualquer lugar do mundo, de qualquer linha telefônica, bastando indicar o número e senha do seu cartão de acesso ao sistema. Diante de número excessivo de ligações - que se constatou terem sido feitas a partir de telefones públicos - ingressou o usuário em juízo, negando tê-las feito. Decidindo pela procedência do pedido, a

sentença de primeiro grau foi mantida pelo E. Tribunal de Justiça de São Paulo, em acórdão da lavra do Des. Pereira Calças, que, entre outros fundamentos, asseverou que:

"Não há dúvida, como bem ressaltou o nobre sentenciante, que ao apelado competia zelar pelo sigilo de sua senha. O apelado sustenta que não foi ele o responsável pelo "vazamento" do número de sua senha, atribuindo o fato à falha do próprio sistema ou à possibilidade de em eventual cruzamento de linhas telefônicas, terceiro tê-lo ouvido quando fornecia sua senha à telefonista.

A prova produzida evidencia a possibilidade de ocorrer cruzamento de linhas telefônicas, bem como a possibilidade de funcionários da própria TELESP ou de empresas que trabalham para ela interceptarem ligações telefônicas e, desta forma, ter acesso à senha sigilosa do apelado"[47].

Um segundo acórdão que trago à apreciação foi proferido pelo E. Tribunal de Justiça de Pernambuco. Ali, correntista de instituição bancária, vítima do "conto do cartão", foi ludibriado por terceiro que dele obteve o cartão magnético e a respectiva senha. Entretanto, o gatuno logrou não apenas sacar o dinheiro que havia na conta corrente, como, via ligação telefônica, conseguiu transferir mais dinheiro da caderneta de poupança da vítima para a conta corrente, de onde pôde efetuar outras retiradas. Reconhecendo o direito do correntista ao ressarcimento, o acórdão, relatado pelo Des. Napoleão Tavares, tinha a seguinte ementa oficial:

"Sendo de pleno conhecimento do banco a prática corriqueira do "conto do cartão magnético", constitui negligência o atendimento, via telefônica, sem perfeita identificação do cliente, mediante rigorosa exigência do uso da senha pessoal.

Tratando-se de modalidade de atendimento visando a facilitar a operacionalidade do serviço, a empresa que o instituiu para melhorar o seu comércio há de suportar os riscos decorrentes dessa rendosa atividade"[48].

O que se pode extrair destes dois acórdãos é que, no primeiro, ao justificar o julgamento diante da mera *possibilidade* de que tenha havido o vazamento da senha, houve, implicitamente, reconhecimento de que o ônus da prova das ligações *continuava* a cargo da Telesp, não se reconhecendo como tal as declarações desta acerca de acesso supostamente feito com o cartão do usuário. Não vejo aqui inversão do ônus da prova em favor do consumidor[49], mas sim, numa leitura mais aberta do artigo 333 do CPC, a mera aplicação do princípio segundo o qual cada parte deve provar a existência dos fatos que lhe aproveitam, sendo indiferente a posição que ocupam no processo. Assim, por exemplo, a *existência* de um crédito deve ser provada pelo credor, independentemente da posição processual que ocupe: autor, face ao pedido de cobrança, ou réu, quanto à declaração de inexistência da obrigação. Havendo, então, a mera *possibilidade* de que o sistema possa ser quebrado, os registros por si não servem como prova, competindo ao credor demonstrar por outras vias que o acesso foi efetivamente feito pela parte contrária.

Do segundo julgado, por seu turno, pode-se extrair um importante princípio: diante de falhas das facilidades proporcionadas pela tecnologia, estas devem ser suportadas pelo operador do serviço, que deles se vale para expandir seu negócio. Por isso, concluo que a ele compete produzir prova cabal, desconsiderando-se como tal registros gerados por sistemas em que exista a *possibilidade concreta* de falha.

Enfim, nestas situações todas acima aludidas - páginas da *Web*, *e-mail*, ou sistemas controlados por senha -, é de se descartar que quaisquer registros possam ser considerados como *prova documental*. Pendendo controvérsia, competirá à parte que tem o ônus da prova demonstrar a verdade pelos meios de prova que dispuser; quando muito, e dependendo das peculiaridades do caso concreto, tais registros poderão ser considerados indícios ou começo de prova. Eventualmente, uma perícia pode demonstrar o grau de inviolabilidade do sistema trazendo mais elementos de convicção ao magistrado. Jamais, porém, podemos equipará-los à prova documental, nem, muito menos, havê-los por expressão absoluta e infalível da verdade.

Com relação a estes sistemas que utilizam *senhas de acesso,* anota Tito Livio Ferreira Gomide que:

"A aplicação dos códigos nos meios informatizados envolve, no mínimo, três fontes de conhecimento: 1) o criador do código ou conjunto de códigos do programa; 2) a máquina que contém o programa de leitura dos códigos; e 3) o operador que detém o código.

Todo código, portanto, depende de um criador, de um leitor e de um operador para poder ser utilizado.

O sigilo desse registro depende da confiança dessas três fontes de conhecimento, motivo da vulnerabilidade de sua segurança.

.....

As práticas fraudulentas consistem na 'fabricação' de dublês de cartões com tarjas magnéticas gravadas com o mesmo código eletrônico original ou a decifração das senhas 'secretas' por hackers, ou ainda através do roubo dos cartões (carteiros) e senhas ('conto do cartão')"[50].

Estas advertências, tão bem colocadas, não se aplicam, porém, ao sistema de assinatura por criptografia de chave pública. Isto porque, neste sistema, o próprio usuário cria o par de chaves e somente a ele compete manter em sigilo a chave privada. Criador e operador, então, se confundem na mesma pessoa do próprio titular da chave. E terceiros, para conferir a assinatura, só se utilizam da chave pública, sem jamais terem acesso à chave privada. Isto encerra uma vantagem e uma desvantagem. A vantagem é que ninguém mais tem acesso à sua chave privada. Só este fato permite perceber que a criptografia de chave pública chega a ser mais segura do que o mais desenvolvido dos sistemas, em que, em algum lugar, por mais protegida que esteja, a senha do usuário está cadastrada. A desvantagem é que não teremos a quem culpar, pela eventual negligência em manter a chave privada segura, já que a apropriação indevida desta chave pode ser considerado o maior risco que afeta a segurança do sistema. Diria, então, como importante recomendação, que toda a cautela possível deve ser tomada na proteção da chave privada pelo seu titular.

Seria o caso, então, para finalizar estas linhas, de fazermos uma distinção entre uma *"segurança técnica"* e uma *"segurança jurídica"*. Alguns métodos técnicos permitem que as partes - mas somente elas - saibam que estão verdadeiramente se comunicando com a pessoa declarada, desde que, evidentemente, um terceiro não tenha conseguido fraudar o sistema. A criptografia simétrica é uma delas. Senhas de acesso a sistemas também estão neste nível de segurança. A prática de enviar um retorno ao remetente do *e-mail* pode permitir conferir se ele é de fato a pessoa que pensamos ser. Uma coisa, porém, é a parte, no seu íntimo, saber que o seu interlocutor é de fato a pessoa que afirma ser; outra coisa é a confiabilidade destes interlocutores e a possibilidade de demonstrar esta certeza a um terceiro. Faria aqui, para melhor explicar, uma comparação com uma conversa telefônica entre dois contratantes. Imaginem que os dois sujeitos reconheceram um a voz do outro e cada qual anotou à mão os dizeres do outro interlocutor, ou a avença final a que chegaram. A certeza que se tem quanto à identidade do outro, ao reconhecer-lhe a voz, esgota-se no âmbito da relação pessoal que se estabelece, não se permitindo transferir a mesma certeza a um terceiro. E não há qualquer força probante nas anotações por eles tomadas, porque feitas unilateralmente. Vindo amanhã a juízo, estes dois interlocutores, um negando ter participado da conversa, ou então narrando versões díspares do seu teor e exibindo cada qual suas anotações manuscritas, o magistrado só terá uma conclusão: um dos dois está mentindo, o problema será saber qual!

Muitas empresas assumem o risco de realizar negócios desta maneira, por exemplo, em páginas da WWW, pois a redução de custos e a potencial expansão que a Internet proporciona deverão compensar eventuais prejuízos causados por pessoas maliciosas, fato cuja incidência deve ser bem reduzida em comparação com o número de transações firmadas e honradas. Para confirmar que o seu interlocutor é mesmo quem diz ser - principalmente no que diz respeito à titularidade do cartão de crédito! - pede-se a indicação de dados pessoais que um terceiro em tese não saberia informar. Esta cautela consiste apenas num potencial freio - diria eu, no nível de *segurança técnica* - a que criminosos tentem se fazer passar por outrem. Mas não podemos atribuir à correta indicação de tais dados qualquer certeza quanto à identidade da pessoa que

> efetua a transação. Impossível comparar esta conferência precária com a exclusividade proporcionada por uma assinatura, manual ou criptográfica. Não se pode, igualmente, considerar que exista prova documental destas transações, mesmo diante da amplitude que este estudo atribui ao conceito de documento e de assinatura, eis que ausentes os elementos autenticidade e integridade. Inexistente, pois, a *segurança jurídica*.
>
> **A *"segurança jurídica"* da comunicação, aqui entendida como uma certeza que possa ser demonstrável a um terceiro, só pode ser obtida com o uso de assinaturas geradas pela criptografia de chave pública, eis que este é o único método que impede a alteração unilateral do documento ou registro eletrônico e permite atribuir-lhe autenticidade. A um registro que seja tecnicamente possível, a uma parte, alterar, não se pode atribuir valor probante em face da outra parte, pois isto seria dar azo à autoprodução de prova.**
>
> Considerando, ainda, os princípios do Código de Defesa do Consumidor, entendo que em casos tais, em se tratando de relação de consumo, competirá ao fornecedor o ônus da prova. Eventuais disposições contratuais em contrário ferem o disposto nos incisos IV e VI, do artigo 51 desta lei, por colocar o consumidor em desvantagem exagerada, ou por representar uma disfarçada inversão do ônus da prova. Afinal, é praticamente impossível ao consumidor fazer prova de que não foi ele quem enviou a mensagem eletrônica, ou que o teor das comunicações mantidas não corresponde ao que se afirma. Recomenda-se, então, àqueles que pretendam negociar por meio da Internet, que usem métodos criptográficos de chave pública na comunicação; ou, então, que saibam o risco que estão assumindo, de não se conseguir fazer prova dos atos praticados *online*.[40] (grifos nosso)

O futuro legislativo que há treze anos escrevia o citado autor chegou, e **a segurança jurídica conferido por chaves públicas de criptografia** é exatamente aquilo a que se pretende a ICP-Brasil, cuja norma disciplinadora já foi aqui tratada. E este futuro veio acrescido da Lei 11.419/06, que em seu art. 11, à primeira leitura, parece não requerer maiores esforços para sua compreensão quando diz:

> Art. 11. **Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.**
>
> § 1º **Os extratos digitais e os documentos digitalizados e juntados aos autos pelos órgãos da Justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pelas procuradorias, pelas autoridades policiais, pelas repartições públicas em geral e por advogados públicos e privados têm a mesma força probante dos originais**, ressalvada a alegação motivada e fundamentada de adulteração antes ou durante o processo de digitalização.
>
> § 2º **A argüição de falsidade do documento original será processada eletronicamente na forma da lei processual em vigor**.
>
> § 3º Os originais dos documentos digitalizados, mencionados no § 2º deste artigo, **deverão ser preservados pelo seu detentor até o trânsito em julgado da sentença** ou, quando admitida, até o final do prazo para interposição de ação rescisória.
>
> § 4º (VETADO)

Obtido por meio eletrônico. Disponível em: <http://augustomarcacini.net/index.php/DireitoInformatica/DocumentoEletronico> Acesso em: 10 out. 2011.

> § 5º Os documentos cuja digitalização seja tecnicamente inviável devido ao grande volume ou por motivo de ilegibilidade deverão ser apresentados ao cartório ou secretaria no prazo de 10 (dez) dias contados do envio de petição eletrônica comunicando o fato, os quais serão devolvidos à parte após o trânsito em julgado.
>
> § 6º Os documentos digitalizados juntados em processo eletrônico somente estarão disponíveis para acesso por meio da rede externa para suas respectivas partes processuais e para o Ministério Público, respeitado o disposto em lei para as situações de sigilo e de segredo de justiça. (BRASIL, 2006)

Sandro D´Amato Nogueira (NOGUEIRA, 2009, p. 135) repisando o próprio texto da Lei 11.419/2006, corrobora a tese de que os documentos digitalizados, de fato, tem a mesma força probante dos originais, e que, não obstante a responsabilidade daqueles operadores que os inserirem no processo eletrônico, a argüição de falsidade será cabível e processada na forma da lei processual em vigor:

Carlos Henrique Abrão (2009, p. 129-130) ensina que a dinâmica do processo eletrônico exige um comportamento e responsabilidades maiores das partes, por conta das naturais exigências deste tipo de procedimento, como prévio cadastramento, utilização de senhas e inserção de documentos digitalizados, destacando:

> As partes devem estar subsumidas às responsabilidades que a elas confere o Código de Processo Civil, a partir do art. 14, de tal modo que, principalmente no processo eletrônico, sem meios considerados abusivos, ou resistências dirigidas à eternização do feito. [...] Rotula a legislação sobre o processo eletrônico a possibilidade de arguição de falsidade de documentos originais que serão digitalizados, preservando-se o conteúdo até final decisão.

Questão relevante traz Jose Carlos de Araújo Almeida Filho, ao afirmar que:

> Quando afirmamos haver senso e contrasenso no Processo Eletrônico, assim o fazemos porque, a partir do momento em que os documentos digitalizados são considerados originais para todos os fins e o parágrafo 1º do art. 11 permite a oposição – ou falsidade – de sua produção, não vimos, aqui, qualquer motivo para a guarda dos documentos.
>
> Uma vez produzido o documento eletrônico e inexistindo impugnação específica, o fenômeno que se opera é o da preclusão. (2010, p.216)

Ainda que não diretamente sobre o tema em si, posto que delimitado o tema em impugnação da prova documental no processo eletrônico partindo da premissa de que a mesma também se encontre em meio eletrônico, o mesmo doutrinador aproxima-se do que se pretende aqui discutir para acrescentar:

> Em termos processuais, admitimos diversos outros problemas, como, por exemplo, o incidente de falsidade a ser argüido nos autos do Processo Eletrônico. Já que os documentos ficarão em cartório e a parte é citada por

> meio eletrônico, a hipótese que se apresenta é a de impossibilidade de acesso total ao feito. Neste caso, parte do processo será visualizada no portal dos Tribunais e parte dele será verificada em cartório, autos com documentos em cartório, autos com documentos de forma eletrônica, disponibilizados a Internet e um incidente a ser processado analisando-se computador e meio físico. (ALMEIDA FILHO, 2010, p. 219)

J.E Carreira Alvim e Silvério Luiz Nery Cabral Júnior, (2008, p. 49-50), citando Augusto Marcacini e Livia Dias de Azevedo, ao analisarem o citado artigo 11 da Lei 11.419/06, afirmam:

> No fundo não existe diferença substancial entre "documentos produzidos eletronicamente! E "documentos digitalizados", pelo que a disposição contida no §1º do art. 11 apenas reforça o disposto no *caput*, cuidando apenas de relacionar os que mais comumente fazem essa juntada, o que teria sido dispensável, e de ressalvar a alegação de adulteração, antes ou durante o processo de digitalização, desde que motivada e fundamentada. Mesmo que não existisse essa ressalva, poderia a parte a quem pudesse prejudicar a produção de uma peça por meio eletrônico, opor-se dela, demonstrando, fundamentalmente, a sua adulteração. Embora fale em alegação motivada e fundamentada, uma coisa implica na outra, porque são expressões sinônimas, pois o que é motivado é fundamento e o que é fundamentado é motivado.
>
> [...]
>
> Registre-se, por oportuno, que, quando um documento é assinado eletronicamente pelo uso de criptografia assimétrica, arguição de falsidade só poderá ser baseada em "falsidade de assinatura", porquanto a adulteração do conteúdo do documento é inviável, vez que faz perder o vínculo entre este e a assinatura. Em tais circunstancias, o documento eletrônico com assinatura eletrônica é dotado de um maior grau de confiabilidade que o próprio documento tradicional, Isto porque o próprio *software* de criptografia, ao conferir a assinatura, acusa que o documento adulterado não corresponde a ela, enquanto o documento tradicional necessita de um exame pericial para constatar eventual alteração.
>
> A propósito de falsificação de assinatura digital, esclarece Marcacini:
>
> *A verdadeira assinatura digital, legitimamente gerada pelo seu titular, não tem como ser falsificada. No fundo, inexiste falsidade a ser apurada no próprio documento eletrônico; o problema em analise se resume exclusivamente na verificação da autenticidade da chave pública. Sabendo-se ser autêntica a chave publica, o próprio programa de computador permitirá conferir a autenticidade e integridade do documento eletrônico.*

Assim, afirma que incidente de falsidade surgirá no curso do processo eletrônico na forma dos arts. 390 a 395 do CPC, tanto para apuração da falsidade material quanto ideológica. Outrossim, destacam que se a argüição for da chave publica da assinatura digital, ter-se-ia a incidência do art. 389, II do mesmo diploma, como contestação de assinatura de documento.

Eis então que surge a verdadeira problemática do art. 11 da Lei citada. Isto porque, de pronto, **vê-se que os conceitos de documento eletrônico e documento digitalizado estejam ainda muito pouco compreendidos pelos operadores do Direito**. Muito certamente porque a

própria definição do *caput*, equivocadamente, não faz diferenciação entre documentos eletrônicos originais e cópias.

Ao afirmar que **os "documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais."** o artigo 11 do citado diploma acaba por misturar os conceitos daquilo que pretendia, ou deveria, esclarecer.

No item 2.4 deste trabalho, ao falar sobre o procedimento no processo eletrônico, viu-se que, via de regra, o procedimento mais comum no procedimento digital é o scaneamento de documentos impressos, ou seja, sua digitalização, e inserção nos autos eletrônicos mediante assinatura eletrônica ou digital (com ou sem certificado digital).

Não se tem dúvidas quando o documento produzido eletronicamente, como se refere o artigo 11 em apreço, é aquele meio físico (papel) convertido em meio eletrônico (arquivo com extensão .pdf), cuja impugnação e comprovação de autenticidade não parece apresentar qualquer problema, eis que nada mais é que uma cópia digital de um documento impresso. A simples apresentação do documento original em meio físico, seria suficiente à prova, quer de seu conteúdo, autenticidade ou mesmo assinatura.

Contudo, não há de ser este o espírito do legislador, posto que limitar o normativo legal a garantir previsão tão somente quanto à conversão do meio, de físico para digital, do documento apresentado, vai de encontro à própria finalidade da norma.

Decerto, por "**documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário"** há de se entender qualquer documento (conteúdo, narrativa, afirmação) produzido com suporte de meio eletrônico. Até mesmo porque, as peças processuais, por exemplo, iniciais, sentenças, decisões, petições, etc., hodiernamente são documentos eletrônicos, já que sequer são impressos para posterior digitalização, prática, como vista na introdução desta pesquisa, rechaçada pelo STJ:

> Carlos Leonardo Pires, responsável pelo processo eletrônico na STI. "**O ideal é que os documentos digitados no word ou outro editor de texto sejam gerados diretamente em arquivo PDF a partir do próprio documento eletrônico. O site do STJ traz orientação quanto a este procedimento**." (grifos nosso)[41]

[41] STJ. Obtido em meio eletrônico. Disponível em: <http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=101488> Acesso em: 21 out. 2011

Vincular a presunção de veracidade dos documentos eletrônicos apenas àqueles que, originários de meio físico, foram digitalizados e inseridos no processo digital, **seria negar a vigência da lei aos documentos originados em meio computacional**, como estes indicados pelo STJ, muito comuns na prática dos operadores dos sistemas processuais eletrônicos existentes, inclusive a autora desta pesquisa.

Como a maioria dos portais de processo digital exige requisitos máximos de tamanho dos arquivos que se pretende inserir e formar os autos eletrônicos, é muito mais simples, prático e rápido criar o documento a partir do próprio computador, através de programas geradores de arquivos extensão .pdf.

Nesse mister, crê-se que os documentos eletrônicos, quer originalmente produzidos, quer aqueles convertidos ao mundo digital, gozam da presunção de veracidade contida no art. 11 da Lei 11.419/06. E, mais, ousa-se discordar, ainda, de J.E Carreira Alvim e Silvério Luiz Nery Cabral Júnior, no que tange a afirmação de que a impugnação dos documentos assinados digitalmente, com certificado digital, estaria limitada à veracidade de sua assinatura.

Ora, se o arquivo é gerado em meio digital, a exemplo de uma petição inicial, digitada em qualquer editor de texto, convertida em arquivo .pdf no próprio computador onde fora escrita, é assinada digitalmente pelo advogado e inserida em um processo eletrônico qualquer, não pode ser impugnada quanto a seu conteúdo? Claro que sim. A bem da verdade, é muito pouco provável que aquela peça tenha sido produzida por outra pessoa, posto que seja dever do causídico guardar a sua assinatura digital com zelo e responsabilidade, mas sim, o conteúdo da peça pode ter sofrido adulteração.

Este raciocínio deve valer para qualquer documento eletrônico, ou seja, a sua impugnação – ainda que tornada mais difícil quando verificada a sua autenticidade por meio da criptografia de uma assinatura digital – permite a contestação de sua validade, conteúdo e assinatura, por ser este o espírito do legislador.

Luiz Guilherme Marinoni e Sérgio Cruz Arenhart, (MARINONI; ARENHART, 2009, p.545), não obstante dediquem-se a uma obra inteira sobre prova, afirmam que, de fato, há enorme carência de dispositivos que disciplinem a questão da força probante do documento eletrônico em si, e, até mesmo do próprio documento digitalizado.

As reais dúvidas acerca da impugnação da prova documental residem e resumem-se nas seguintes dúvidas:

a) O prazo da arguição prevista no artigo 11 da Lei do processo eletrônico seria o mesmo do art. 390?

b) O processamento incidental também se daria digitalmente? Em autos virtualmente apartados?

c) Como resolver a incompatibilidade do incidente de falsidade com o sistema dos Juizados Especiais que hoje atuam com PROJUDI, se a Lei 9.099/95 veda a complexidade de causa?

d) Em se tratando de arguição da autenticidade criptográfica, a quem cabe o ônus da prova?

A priori, não tendo a Lei do Processo Eletrônico fixado prazo diverso para a arguição de falsidade, e, ao contrário, afirmado que o processamento do incidente dar-se-á na forma da legislação processual em vigor, vence-se, facilmente o primeiro questionamento apresentado.

Quando ao processamento incidental da arguição de falsidade, crê-se não haver qualquer impedimento para que haja autuação em apartado, também eletronicamente, exceto se eventual contra prova tornar o incidente incompatível com o procedimento digital.

Atrito maior parece encontrar o artigo 11 da Lei 11.419/06 quando a falsidade suscitada der-se em autos eletrônicos que tramitem em seara de Juizados Especiais. Isto porque, a Lei 9.099/95, que rege aqueles juízos, em seu artigo 3º afirma que:

> Art. 3º. O Juizado Especial Cível tem competência para conciliação, processo e **julgamento das causas cíveis de menor complexidade**, assim consideradas:"
>
> I - as causas cujo valor não exceda a quarenta vezes o salário mínimo;
>
> II - as enumeradas no art. 275, inciso II, do Código de Processo Civil;
>
> III - a ação de despejo para uso próprio;
>
> IV - as ações possessórias sobre bens imóveis de valor não excedente ao fixado no inciso I deste artigo.

Logo, em principio, haveria vedação da alegação do incidente de falsidade junto aos feitos dos juizados especiais, conquanto a produção de prova pericial acabasse por tornar complexa a causa.

Todavia, em recentes julgados do STJ, firmou-se o entendimento de que a realização de perícia não afasta a competência dos Juizados Especiais em função de possível complexidade, como ora se observa:

> PROCESSO CIVIL. FORNECIMENTO DE MEDICAMENTOS. UNIÃO, ESTADO E MUNICÍPIO COMO LITISCONSORTES PASSIVOS. PRINCÍPIO FEDERATIVO E DA ESPECIALIDADE. VALOR DA CAUSA INFERIOR A 60 SALÁRIOS MÍNIMOS. COMPETÊNCIA ABSOLUTA.

> 1. Trata-se de ação para fornecimento de medicamentos ajuizada em face da União Federal, Estado de Santa Catarina e Município de Criciúma/SC. No apelo nobre, a municipalidade insurge-se contra a fixação da competência no âmbito do Juizado Especial Federal.
>
> 2. A competência do Juizado Especial Federal não se altera pelo fato de o Estado e o Município figurarem como litisconsortes passivos da União Federal. Prevalece, na espécie, o princípio federativo (que dá supremacia à posição da União em face de outras entidades) e o da especialidade (que confere preferência ao juízo especial sobre o comum). Precedentes.
>
> 3. Se o valor da ação ordinária é inferior ao limite de sessenta salários mínimos previstos no artigo 3º da Lei 10.259/2001, aliado à circunstância de a demanda não se encontrar no rol das exceções a essa regra, deve ser reconhecida a competência absoluta do Juizado Especial Federal**, sendo desinfluente o grau de complexidade da demanda ou o fato de ser necessária a realização de perícia técnica**.
>
> 4. Recurso especial não provido.
>
> (REsp 1205956/SC, Rel. Ministro CASTRO MEIRA, SEGUNDA TURMA, julgado em 23/11/2010, DJe 01/12/2010) – (grifo nosso)

> RECURSO ORDINÁRIO EM MANDADO DE SEGURANÇA. CONTROLE DE COMPETÊNCIA PELO TRIBUNAL DE JUSTIÇA. JUIZADOS ESPECIAIS CÍVEIS. MANDADO DE SEGURANÇA. CABIMENTO. LEI N. 9.099/95. NECESSIDADE DE PERÍCIA. COMPATIBILIDADE.
>
> 1. É possível a impetração de mandado de segurança com a finalidade de promover o controle de competência nos processos em trâmite nos juizados especiais.
>
> 2. **A necessidade de produção de prova pericial não influi na definição da competência dos juizados especiais cíveis estaduais**.
>
> 3. Recurso ordinário desprovido.
>
> (RMS 29.163/RJ, Rel. Ministro JOÃO OTÁVIO DE NORONHA, QUARTA TURMA, julgado em 20/04/2010, DJe 28/04/2010) – (grifo nosso)

Nesse sentir, a simples necessidade de produção da prova pericial não daria margem à impossibilidade de arguição da falsidade documental no processo eletrônico. Resta imaginar, contudo, se os magistrados destes juízos, habituados a feitos relativamente simples, assim prosseguiriam, especialmente se a impugnação fosse de um documento eletrônico em si, e não de mero documento digitalizado.

A facilidade encontrada nas respostas aos quesitos propostos até aqui não se mantém quando o enfrentamento diz respeito à impugnação do documento eletrônico por dúvidas no uso das chaves criptográficas. Mormente a pesquisa realizada aponte para que o documento eletrônico assinado digitalmente, com certificado digital, garanta a autenticidade de seu emitente, não há dispositivo legal que preveja ou determine qualquer obrigação às partes envolvidas neste sentido, nem, tampouco, de quem seria o ônus da comprovação.

As soluções talvez sejam as apontadas pelos textos dos Projetos de Lei 1.589/99, fundido ao PL 4.906/2001[42], respectivamente:

> **TÍTULO III - DOCUMENTOS ELETRÔNICOS**
> **Capítulo I - Da eficácia jurídica dos documentos eletrônicos**
> Art. 14 - Considera-se original o documento eletrônico assinado pelo seu autor mediante sistema criptográfico de chave pública.
> § 1º - Considera-se cópia o documento eletrônico resultante da digitalização de documento físico, bem como a materialização física de documento eletrônico original.
> § 2º - Presumem-se conformes ao original, as cópias mencionadas no parágrafo anterior, quando autenticadas pelo escrivão na forma dos arts. 33 e 34 desta lei.
> § 3º - A cópia não autenticada terá o mesmo valor probante do original, se a parte contra quem foi produzida não negar sua conformidade.
> Art. 15 - As declarações constantes do documento eletrônico, digitalmente assinado, presumem-se verdadeiras em relação ao signatário, desde que a assinatura digital:
> a) seja única e exclusiva para o documento assinado;
> b) seja passível de verificação;
> c) seja gerada sob o exclusivo controle do signatário;
> d) esteja de tal modo ligada ao documento eletrônico que, em caso de posterior alteração deste, a assinatura seja invalidada; e
> e) não tenha sido gerada posteriormente à expiração, revogação ou suspensão das chaves.
> Art. 16 - A certificação da chave pública, feita pelo tabelião na forma do Capítulo II do Título IV desta lei, faz presumir sua autenticidade.
> Art.17 - A certificação de chave pública, feita por particular, prevista no Capítulo I do Título IV desta lei, é considerada uma declaração deste de que a chave pública certificada pertence ao titular indicado e não gera presunção de autenticidade perante terceiros.
> Parágrafo único - Caso a chave pública certificada não seja autêntica, o particular, que não exerça a função de certificação de chaves como atividade econômica principal, ou de modo relacionado à sua atividade principal, somente responderá perante terceiros pelos danos causados quando agir com dolo ou fraude.
> Art. 18 - A autenticidade da chave pública poderá ser provada por todos os meios de direito, vedada a prova exclusivamente testemunhal.
> Art. 19 - Presume-se verdadeira, entre os signatários, a data do documento eletrônico, sendo lícito, porém, a qualquer deles, provar o contrário por todos os meios de direito.
> § 1º - Após expirada ou revogada a chave de algum dos signatários, compete à parte a quem o documento beneficiar a prova de que a assinatura foi gerada anteriormente à expiração ou revogação.
> § 2º - Entre os signatários, para os fins do parágrafo anterior, ou em relação a terceiros, considerar-se-á datado o documento particular na data:
> I - em que foi registrado;
> II - da sua apresentação em repartição pública ou em juízo;
> III - do ato ou fato que estabeleça, de modo certo, a anterioridade da formação do documento e respectivas assinaturas.
> Art. 20 - Aplicam-se ao documento eletrônico as demais disposições legais relativas à prova documental, que não colidam com as normas deste Título.
> **Capítulo II - Da falsidade dos documentos eletrônicos**
> Art. 21 - Considera-se falso o documento eletrônico quando assinado com chaves fraudulentamente geradas em nome de outrem.
> Art. 22 - O juiz apreciará livremente a fé que deva merecer o documento eletrônico, quando demonstrado ser possível alterá-lo sem invalidar a assinatura, gerar uma assinatura eletrônica idêntica à do titular da chave privada, derivar a chave privada a partir da chave pública, ou pairar razoável dúvida sobre a segurança do sistema criptográfico utilizado para gerar a assinatura.
> Art. 23 - Havendo impugnação do documento eletrônico, incumbe o ônus da prova:

[42] Obtido por meio eletrônico. Disponível em: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2685/Proposta_e_Estudo_CTS-FGV_Cibercrimes_final.pdf?sequence=1> Acesso em: 04 mar. 2011

> I - à parte que produziu o documento, quanto à autenticidade da chave pública e quanto à segurança do sistema criptográfico utilizado;
> II - à parte contrária à que produziu o documento, quando alegar apropriação e uso da chave privada por terceiro, ou revogação ou suspensão das chaves.
> Parágrafo único - Não sendo alegada questão técnica relevante, a ser dirimida por meio de perícia, poderá o juiz, ao apreciar a segurança do sistema criptográfico utilizado, valer-se de conhecimentos próprios, da experiência comum, ou de fatos notórios. (grifos do autor)

> Art. 8º O juiz apreciará livremente a fé que deva merecer o documento eletrônico, quando demonstrado ser possível alterá-lo sem invalidar a assinatura, gerar uma assinatura eletrônica idêntica à do titular da chave privada, derivar a chave privada a partir da chave pública, ou pairar razoável dúvida sobre a segurança do sistema criptográfico utilizado para gerar a assinatura.
>
> **Art. 9º Havendo impugnação de documento eletrônico, incumbe o ônus da prova:**
>
> **I - à parte que produziu a prova documental, quanto à autenticidade da chave pública e quanto à segurança do sistema criptográfico utilizado;**
>
> **II - à parte contrária à que produziu a prova documental, quando alegar apropriação e uso da chave privada por terceiro, ou revogação ou suspensão das chaves**. (grifos nosso)

Do quanto observado, vê-se que a impugnação da prova documental não pode ser compreendida apenas como uma contestação aos documentos digitalizados, postos que quanto a estes a simples guarda e exibição do meio físico que os contém são suficientes à contraprova, inclusive para fins de ação rescisória.

O grande cerne da questão, ainda sem solução aparente pelo legislador pátrio, diz respeito à impugnação do documento eletrônico, assim compreendido como aquele produzido em meio digital, conquanto mais difíceis sejam as definições que o compreende, bem como os pré-requisitos ao seu uso – com valor probante – nos autos do processo eletrônico, passando, então, necessariamente, pelo uso de assinaturas digitais criptografadas, a fim de que se possa garantir a integridade, autenticidade e validade daquele documento eletrônico.

4.2 EFEITOS DA IMPUGNAÇÃO PARA AS PARTES E ADVOGADO

No campo do processo eletrônico, dadas às participações de vários sujeitos em seu desenrolar, não é a clara a Lei 11.419/06 acerca das responsabilidades dos atores daqueles procedimentos digitais, no tocante aos efeitos da impugnação.

Isto porque, é preciso ter em mente, os diversos atores do processo eletrônico. Observe-se que, em um Juizado Especial Federal, em ação previdenciária de menor complexidade que tramite pelo sistema e-Proc, não necessariamente terá atos processuais praticados pelo advogado ou pela parte. Dadas as circunstâncias daquele tipo de lide.

É possível imaginar que a parte requerente seja intimada a colacionar aos autos algum documento, e, faltando-lhe conhecimento técnico, compareça à Secretaria do Juizado Federal e apresente uma cópia impressa daquele documento. Este será digitalizado, por meio de *sanner*, e inserido nos autos do processo eletrônico respectivo.

Impugnado pelo órgão previdenciário posteriormente, decerto, não seria o serventuário do foro responsabilizado pela falsidade – não que não seja isto impossível. O que se quer dizer é: o simples ato de inserir documentos em um processo eletrônico não implica necessariamente na imputação da responsabilidade por eventual falsidade a quem aquele ato praticou.

Se o advogado recebe um documento já digitalizado de seu cliente, logo meio físico eletrônico, sem assinatura digital do referido cliente, mas utiliza-o em processo daquela parte, deverá ser penalizado por eventual falsidade do documento? Não deveria, já que não produziu o referido documento.

Carlos Henrique Abrão (2010, p. 129-131) assim manifesta-se:

> Na dinâmica do processo eletrônico o papel das partes é fundamental para aglutinar o principal aspecto da formação da lide e os meios instrutórios destinados à solução do litígio.
>
> Denota-se, consequentemente, por meio desse prisma de visão, que jogam as partes um papel extremamente importante, desde o cadastramento, acesso ao sistema, senha, e principalmente no monitoramento do processo virtual e na inserção de elementos comprobatórios das peças discutidas.
>
> A esse respeito, a Lei 11.419/2006, de forma pontual, menciona a obrigatoriedade do desenvolvimento do sistema eletrônico, baseado no meio digital, colocado na rede mundial de computadores e com acesso junto às redes externas e internas.
>
> [...]
>
> As partes devem estar subsumidas às responsabilidades que a elas refere o Código de Processo Civil, a partir do art. 14, de tal modo que, principalmente no processo eletrônico, devem pautar a conduta mediante lealdade, veracidade, sem meios considerados abusivos, ou resistências dirigidas a eternizarão do feito.

> Bem se nota, na percepção traduzida, a obrigatoriedade de as partes adstringirem ao caminho processual da efetividade e instrumentalidade, e tal preceito também se aplica na formação do litisconsórcio ou na intervenção de terceiros.
>
> Precisamente, quando uma das partes fizer uso de meios inadequados ou argüir fatos absolutamente irrelevantes para o deslinde da causa, disso resulta conseqüência de responsabilidade processual inerente.
>
> Rotula a legislação sobre processo eletrônico a possibilidade da argüição de falsidade dos documentos originais que serão digitalizados, preservando-se seu conteúdo até final decisão.
>
> [...]
>
> **Consequentemente, as partes em litígio, no processo eletronico, também se sujeitam, naturalmente à eticidade e à transparência, condicionantes fundamentais para a validação e êxito do mecanismo digital.**
>
> **Qualquer violação dessa circunstância, ou a demonstração inequívoca de conduta incompatível, ou comportamento critico que prejudique a viabilidade do instrumento digital espelhada nos arts. 14 e 17 do CPC, ensejará reprimenda para evitar abuso**.

Não se olvida, obviamente, que a parte que der causa ao incidente deve ser processual e criminalmente responsabilizada. Porém, a Lei 11.419/06 foi omissa no que diz respeito a responsabilidade civil– e porque não criminal – decorrente da apuração de tal incidente de falsidade.

Faltou ao legislador, muito certamente por conta da tão citada dificuldade em compreender os mecanismos que envolvem todas essas evoluções tecnológicas, uma especial atenção aos sujeitos atores do processo eletrônico, a fim de, identificando as participações de cada um – parte, advogado, serventuário, auxiliares do juízo, membro do Ministério Público e magistrado – para daí, sim, poder especificar e determinar as responsabilidades de cada um, em eventual cometimento de infração nos autos digitais.

5 BREVES NOTAS SOBRE AS O ANTEPROJETO DO NOVO CPC E O TEMA

Tramita no Congresso Nacional o Anteprojeto do Novo Código de Processo Civil, o PL nº 8046/10. Sem dúvida uma legislação fruto dos anseios jurídicos de uma sociedade que, influenciada por esta Era da Informação – notadamente o próprio acompanhamento do Projeto através do e-democracia – preza e espera por uma tutela jurisdicional de entrega rápida e efetiva, com respeito às garantias constitucionais.

Importantes avanços na seara processual se avizinham, e o simples fato do projeto ter aberto oportunidade de discussões e debates públicos, como a Conferência estadual, realizada em Salvador, em 24 de outubro próximo passado[43], demonstra que a o Compêndio deverá traduzir as expectativas por inovações legais que permitam, de fato, um processo civil mais rápido, efetivo e eficaz.

Ao acessar os sítios da Câmara e Senado, vê-se que o tema processo eletrônico fez-se presente em quase todas as audiências e debates públicos sobre o Novo CPC. Sem dúvidas, a maior preocupação é quanto à unificação dos sistemas de procedimento digital, dando maior segurança aos usuários, o que, de fato, poderá ser resolvido antes mesmo da vigência da nova lei processual – e assim parece ser mais lógico – através da implantação do PJe do CNJ em todo país.

Noticia-se sobre o clamor ao Anteprojeto[44]:

> O ministro do Superior Tribunal de Justiça (STJ) Teori Zavascki e o advogado-geral da União substituto, Fernando Luiz Albuquerque Faria, **sugeriram que o projeto do novo Código de Processo Civil (PL 8046/10) avance na previsão do processo eletrônico**. Ambos participaram nesta quinta-feira de audiência pública na comissão especial que analisa o novo CPC e também apontaram avanços que o projeto pode fazer na cooperação internacional, nas ações coletivas e no incentivo à conciliação pelo Poder Público.
>
> **O ministro do STJ observou que o projeto ainda traz expressões como "datilografar" e "conferir página", o que mostra que o texto está ideologicamente vinculado ao papel, enquanto a realidade aponta cada vez mais para a informatização dos processos. "Um novo código só tem sentido se induzir mudanças de padrões culturais", ressaltou**.
>
> Já o advogado da União **reclamou da multiplicidade de sistemas de processo eletrônico existentes nos vários tribunais, o que dificulta a comunicação entre os órgãos da Justiça e as defensorias e procuradorias da União. "O novo CPC poderia de alguma forma tentar ajudar nessa dificuldade de comunicação**", disse.

---

[43] Mensagem eletrônica pessoal recebida pela autora.

[44] Obtido por meio eletrônico. Disponível em: <http://www2.camara.gov.br/agencia/noticias/DIREITO-E-JUSTICA/203681-AGU-E-STJ-SUGEREM-AVANCOS-NO-PROCESSO-ELETRONICO-NO-NOVO-CPC.html> Acesso em: 22 out. 2011

> O presidente da comissão especial, deputado Fabio Trad (PMDB-MS), **avaliou que as audiências vão ajudar a Câmara a aperfeiçoar o projeto e incorporar essa cultura do processo eletrônico**. O relator-geral da proposta, deputado Sérgio Barradas Carneiro (PT-BA), **também avaliou que a informatização do processo é uma tendência irreversível, mas disse que é preciso tomar cuidado na maneira de incluir esse ponto no texto, para que ele não fique defasado antes da sua aplicação, já que "essas tecnologias mudam a cada seis meses**". (grifos nossos)

Cumpre destacar que com respeito aos objetos desta pesquisa, os artigos do Anteprojeto[45] visualizados mais demonstram um retrocesso que um avanço:

> **Art. 435. A utilização de documentos eletrônicos no processo convencional dependerá de sua conversão à forma impressa e de verificação de autenticidade, na forma da lei.**
>
> **Art. 426. O juiz apreciará o valor probante do documento eletrônico não convertido, assegurado às partes o acesso a seu teor.**
>
> **Art. 427. Serão admitidos documentos eletrônicos produzidos e conservados com a legislação especifica.** (grifos nosso)

Crê-se, da leitura dos três artigos propostos que o legislador brasileiro continua a não compreender a dinâmica e acepções da ciência computacional, cujo entrelaçamento com o Direito não é mais mera modernidade dos jovens, mas sim uma necessidade decorrente das próprias relações humanas, modificadas por mundo tecnologicamente distinto e em plena evolução.

Diz-se isto porque condicionar a utilização de documentos eletrônicos à "sua forma impressa" parece ir pelo caminho da involução! Primeiramente, porque o dispositivo, novamente em crasso equívoco, dá entender que documento eletrônico é papel scaneado, ou seja, mais uma vez confunde documento eletrônico com documento digitalizado. Em segundo lugar, porque se não fez tal confusão, tornou impossível a própria realização da prova.

Note-se que converter, por exemplo, um documento eletrônico do tipo arquivo de voz ou música, para papel impresso é impossível. A não ser que se pretenda transcrever no papel as falas do áudio ou a letra da música. Pior, se for uma mídia de imagem? Como é que se translada para o papel uma imagem? Imprime-se todas as cenas? E as falas inerentes? Transcreve-se também? Não parece razoável.

---

[45] Obtido por meio eletrônico. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=490267> Acesso em: 29 out. 2011.

É preciso que o novo CPC inove, com a segurança que o documento e o processo eletrônico requerem, mas sem o apego ao físico, ao material, ao papel. O mundo mudou, a forma de pensá-lo, vivê-lo, senti-lo e legislá-lo também.

Urge que o Anteprojeto seja revisto para disciplinar corretamente o uso do documento eletrônico, a prova no processo digital, os efeitos da impugnação no curso da lide não física, a fim de que a celeridade processual experimentada com o advento da Lei 11.419/06 seja corretamente compreendida e legislada.

6 CONCLUSÃO

Pode-se inferir da pesquisa em apreço que a o Direito, por ser ciência social que disciplina as relações havidas em comunidade, é afetada diretamente pelas revoluções que a sociedade experimenta.

Neste sentido, as mudanças trazidas como conseqüência da Era Digital são marcantes e encontram-se em processo irreversível de diuturnas modificações, lançando, a cada dia, novos conceitos e vivências que precisam ser tuteladas, na medida em que os conflitos delas decorrentes importa à ciência jurídica.

Dentro deste rumo evolutivo, a informatização do judiciário é tema recorrente e ganhou macro dimensões com o advento da Lei 11.419/06. Contudo, viu-se que o aprimoramento técnico e pessoal das infraestruturas que compõem as unidades judiciárias do país deve ir além dos limites do processo eletrônico, eis que os serviços prestados pelas mesmas não devem limitar-se a um bem sucedido sistema informatizado de procedimento digital. Ao contrario, engloba atos outros que integram os serviços prestados à sociedade, tais como emissões de certidões *on line*; informações processuais seguras e atualizadas, via internet; dentre outros.

Restou comprovado que os significativos avanços da Lei do Processo Eletrônico implica em uma nova ordem de pensar o Direito, na qual os conhecimentos e habilidades dos operadores demandarão um convívio muito maior com os conhecimentos da ciência da informática. De certo, de aparente dificuldade operacional, os sistemas de processo digital hoje existentes podem ser utilizados por qualquer pessoa que se detenha ao mínimo esforço de aprender os passos para sua operacionalização.

Todavia, de suma importância a implantação de um sistema de processo eletrônico único – como tenciona o CNJ com o PJe – a fim de possibilitar a integração entre todos os tribunais do país, inclusive em grau de jurisdição superior; estabelecer regras claras quanto ao uso de assinatura digital com certificado criptografado, para que possa haver maior segurança no uso dos ditos sistemas; e facilitar a vida dos usuários deste procedimento, especialmente aqueles, como os advogados, que o fazem em unidades territoriais, ou mesmo, jurisdicionais diferentes.

Esta definição de um sistema único e suas garantias de segurança são, como visto, necessárias à produção de prova do documento eletrônico, quer no processo de autos físicos, quer no processo eletrônico.

A segurança das informações, a autenticidade de documentos, e autoria dos documentos eletrônicos perpassa, obrigatoriamente, pela assinatura digital, posto que, a alhures explicado, é ela a garantidora de um sistema eletrônico de processo civil menos sujeitos à intempéries ligadas à prova.

Destarte, a impugnação da prova documental no processo eletrônico é matéria a ser pensada não apenas no sentido da aferição da verdade processual decorrente, pura e simples, da digitalização de documentos em meio físico comum, ou seja, papel. Ao contrário, o normativo do artigo 11 da Lei 11.419/06 não diferencia a presunção de veracidade atribuída aos documentos eletrônicos originalmente produzidos em meio computacional, daqueles em suporte físico convertidos para suporte computacional.

Por tal razão, impugnar o documento eletrônico é medida cabível, valendo-se das regras do CPC já existentes, tanto no que diz respeito às provas digitalizadas – cuja apuração da verdade processual parece ser mais simples, graças à possibilidade de mera exibição do meio físico que a contiver – quanto a prova cujo meio é eletrônico na sua origem. Nesta, sem dúvidas, a assinatura digital fará diferença para uma apuração mais segura da falsidade apontada.

Por derradeiro demonstrou-se que o legislador ainda pode caminhar muito acerca do tema, delimitando a responsabilidade civil e penal de cada sujeito do processo eletrônico, em cada ato por ele praticado – se de mera inserção ou de produção intelectual.

O caminhar, com efeito, é para o futuro, esperando-se que o novo Código de Processo Civil, suprindo as lacunas apontadas, trilhe um caminho evolutivo, e não retrocedendo, arraigando-se a velhos conceitos e experiências.

REFERÊNCIAS

ABRÃO, Carlos Henrique. *Processo Eletrônico*. 2ª Edição. São Paulo. Editora Revista dos Tribunais. 2009.

ABRÃO, Carlos Henrique. *PROCESSO ELETRÔNICO: Processo Digital*. 3ª Edição. São Paulo. Editora Atlas. 2011.

ADONIAS, Antonio.**Documentos eletrônicos** [mensagem pessoal]. Mensagem recebida por <fabiani.borges@gmail.com> em 20 out. 2011.

ALMEIDA FILHO, José Carlos de Araújo. **Processo Eletrônico e Teoria Geral do Processo Eletrônico: a informatização Judicial no Brasil**. 3ª Edição. Rio de Janeiro. Editora Forense. 2010.

ALVIM, J.E. Carreira; JUNIOR, Silvério Luiz Nery Cabral. **Processo Judicial Eletrônico.** Curitiba. Editora Juruá. 2008.

ATHENIENSE, Alexandre Rodrigues. **Documentos eletrônicos no processo digital**. Disponivel em: <http://www.conteudojuridico.com.br/?artigos&ver=2.23320>. Acesso em: 30 out. 2011

ATHENIENSE, Alexandre. **Comentários à Lei 11.419/06 e as Práticas Processuais por Meio Eletrônico nos Tribunais Brasileiros**. Edição atualizada. Curitiba. Editora Juruá. 2010.

BAHIA. **Provimento n.º CGJ-03/2010**. http://www.tjba.jus.br/corregedoria/arquivos/PROVIMENTO%20CGJ%20032010.pdf. Acesso em: 20 ago. 2010.

BAHIA. **Provimento nº CGJ – 06/2011**. http://www5.tjba.jus.br/corregedoria/images/pdf/provimentocgj062011.pdf . Acesso em: 21 set. 2011

BAHIA. **Provimento Nº CGJ –11/2008-GSEC**. Disponível em < http://www5.tjba.jus.br/corregedoria/images/pdf/provimento200811.pdf>. Acesso em 26 out. 2011.

BARBOSA, Rui. **Obras completas de Rui Barbosa. Discursos Paralamentares.** Volume XIX. Tomo III. 1892. Disponível em: <http://www.casaruibarbosa.gov.br/rbonline/obrasCompletas.htm> Acesso em: 27 out. 2011.

BARBOSA, Rui. **Oração aos Moços**. São Paulo. Editora Martin Claret. 2003.

BRASIL. **Código Civil, Constituição Federal e Legislação Complementar**. Editora Saraiva. 2009.

BRASIL. **Código de Processo Civil, Constituição Federal e Legislação Complementar**. Editora Saraiva. 2009.

BRASIL. **Lei 11.419, de 19 de dezembro de 2006**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm>. Acesso em 18 de out 2010.

BRASIL. **Lei 8.245, de 18 de outubro de 1991**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8245.htm> . Acesso em: 20 ago. 2011.

BRASIL. **Lei 9.800, de 26 de maio de 1999**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9800.htm>. Acesso em: 05 abr. 2011.

BRASIL. **Medida Provisória Nº 2.200-2, de 24 de Agosto de 2001**. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm>. Acesso em 18 de out 2010.

BRASIL. **PL 2.126, de 24 de agosto de 2011**. Disponível em <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255> Acesso em: 26 out. 2011.

BRASIL. **Projetos de Lei 1.589/99 e PL 4.906/2001**. Disponível em: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2685/Proposta_e_Estudo_CTS-FGV_Cibercrimes_final.pdf?sequence=1> Acesso em: 04 mar. 2011

BRASIL. **PL 84, de 24 de fevereiro de 1999**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028> Acesso em: 26 out. 2011

BRASIL. *PLS* – **Projeto de Lei do Senado, Nº 166 de 2010**. Disponível em <www.senado.gov.br> Acesso em 18/08/2010.

BRASIL. Superior Tribunal de Justiça**. EDcl nos EDcl no REsp 1128778 / BA EMBARGOS DE DECLARAÇÃO NOS EMBARGOS DE DECLARAÇÃO NO RECURSO ESPECIAL 2009/0006764-9.** Recorrente: Banco Bradesco S/A. Recorrido: Ana Paula de Lima Bertolo Guimarães. Relator: Min. João Otávio de Noronha, Brasília, DJe 09 ago 2011. Disponível em: <www.stj.gov.br>. Acesso em: 22 out. 2011.

CANARIO, Pedro. **Adesão da advocacia ao certificação digital é baixa** (sic). Disponível em: <http://www.conjur.com.br/2011-set-24/advocacia-ainda-nao-preparada-processo-eletronico.> Acesso em: 29 set. 2011

CARNELUTTI, Francesco. **Instituições de Processo Civil.** Tradução Adrián Sotero de Witt Batista. São Paulo. Editora Classic Book. 2000.

CARVALHO, Paulo Roberto Lima de. **Prova Cibernética no Processo**. Curitiba. Editora Juruá. 2009.

CASTRO, Francisco Augusto Neves e. **Teoria das Provas e suas Aplicações aos Atos Civis.** 2ª ed., anotada por Pontes de Miranda. Campinas. Editora Servanda. 2000.

CERSOSIMO, Samuel. **Indisponibilidade do sistema de processo eletrônico e a devolução do prazo segundo decisão do TST**. Disponível em: <http://blog.viasdefato.com/2010/03/indisponibilidade-do-sistema-de.html> Acesso em: 27 out. 2011.

CHIOVENDA, Giuseppe. **Instituições de Direito Processual.** Vol. III. Campinas. Editora Bookseller. 1998.

CLEMENTINO, Edilberto Barbosa. **Processo Judicial Eletrônico**. Curitiba. Editora Juruá. 2007.

CNJ. **Processo Judicial eletrônico.** Disponível em: <http://www.cnj.jus.br/programas-de-a-a-z/sistemas> Acesso em: 26 out. 2011.

KLIPPEL, Rodrigo; BASTOS, Antonio Adonias. **Manual de Processo Civil.** Volume único. 2ª edição. Rio de Janeiro. Editora Lumen Juris. 2011.

LEAL, Sheila do Rocio Cercal Santos. Contratos Eletrônicos: **Validade Jurídica dos Contratos via Internet**. São Paulo: Atlas, 2007. 225 p.

LESSA, Breno Minucci. **A Invalidade das Provas Digitais no Processo Judiciário**. Disponivel em: <http://www.conteudojuridico.com.br/?artigos&ver=2.25613>. Acesso em: 28 out. 2011.

MARCACINI, Augusto Tavares Rosa**. O documento eletrônico como meio de prova.** Disponível em: <http://augustomarcacini.net/index.php/DireitoInformatica/DocumentoEletronico> Acesso em: 20 out. 2011.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. **Prova**. 1ª Edição. 2ª Tiragem. São Paulo. Editora Revista dos Tribunais. 2009.

MONTENEGRO FILHO, Misael. **Curso de Direito Processual Civil.** 5ª ed. v. I, São Paulo: Atlas, 2009. 570 p

NEVES, Daniel Amorim Assumpção. **Manual de direito processual civil**. Volume único. 2ª Edição. São Paulo. Editora Método. 2010.

NOGUEIRA, Sandro D´amatto. **Manual de Direito Eletrônico**. 1ª Edição. São Paulo. Editora BH. 2009.

NUCCI, Guilherme de Souza. **Provas no Processo Penal.** São Paulo. Editora Revista dos Tribunais, 2009.

PARENTONI, Leonardo Netto. D**ocumento Eletrônico: Aplicação e interpretação pelo Poder Judiciário**. Curitiba. Editora Juruá. 2009.

PECK, Patricia. **Documento Eletrônico e a Prova Eletrônica.** Disponível em: <http://uj.com.br/publicacoes/doutrinas/3410/DOCUMENTO_ELETRONICO_E_A_PROVA_ELETRONICA> Acesso em: 27 out. 2011.

PEREIRA, Robson. **Oração aos Moços e o processo judicial eletrônico**. Disponível em <http://www.conjur.com.br/2011-jul-04/letras-juricias-oracao-aos-mocos-processo-judicial-eletronico> Acesso em: 21 out. 2011.

PINHEIRO, Patrícia Peck. **Direito Digital**. 3ª Edição. São Paulo. Editora Saraiva. 2009.

STJ. **Balanço revela menos processos em tramitação, menos consumo de energia e mais área útil disponível no STJ**. Disponível em: <http://www.stj.jus.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=97958&tmp.area_anterior=44&tmp.argumento_pesquisa=eletr%F4nico> Acesso em: 20 abr. 2011.

STJ. **Informação veiculada em site da Justiça tem valor oficial**. Disponível em < http://www.stj.jus.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=102402> Acesso em: 29 jun. 2011.

STJ. *Processo* **eletrônico conquista magistrados e advogados, mas ainda tem desafios**. Disponível em: <http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=101488> Acesso em: 21 out. 2011

STJ. **REsp 1205956/SC, Rel. Ministro CASTRO MEIRA, SEGUNDA TURMA. Brasília. DJe 01 dez 2010**. Disponível em <www.stj.jus.br> Acesso em: 29 out. 2011.

STJ. Superior Tribunal de Justiça. **AgRg no Ag 1251998 / SP AGRAVO REGIMENTAL NO AGRAVO DE INSTRUMENTO 2009/0220086-7**. Agravante: Rosângela Nistal Lyra Vasconcellos. Agravado: Jayme Cuschnir e Outros. Relator: Min. LUIS FELIPE SALOMÃO, Brasília. DJe 19 nov 2010. Disponível em: <www.stj.gov.br>. Acesso em: 22 out. 2011.

STJ. Superior Tribunal de Justiça. **EDcl no AgRg no Ag 1329882/PR**. Embargante: Banco Nacional de Desenvolvimento Econômico e Social - BNDES. Embargado: Imcopa Importação Exportação e Indústrias de Óleos LTDA. e Outro. Relator: Ministro Sidnei Beneti. Brasília. DJe 01jul 201. Disponível em: <www.stj.gov.br>. Acesso em: 22 out. 2011.

STJ. Superior Tribunal de Justiça. **HC 149.250/SP**. Impetrante: Andrei Zenkner Schmidt e Outros. Impetrado: Tribunal Regional Federal da 3ª Região. Relator: Ministro Adilson Vieira Macabu (Desembargador Convocado do TJ/RJ). Brasília. DJe 05 set. 2011. Disponível em: <www.stj.gov.br>. Acesso em: 22 out. 2011.

ANEXO A – Processo Judicial Eletrônico do Conselho Nacional de Justiça

CONSELHO
NACIONAL
DE JUSTIÇA

PJe

PROCESSO JUDICIAL ELETRÔNICO

PJe – Processo Judicial Eletrônico

2010 Conselho Nacional de Justiça

EXPEDIENTE

Porta voz do CNJ	Pedro Del Picchia
Assessor-chefe da Comunicação Social do CNJ	Marcone Gonçalves
Comunicação Institucional do CNJ	Tarso Rocha
Revisão	Geysa Bigonha Maria Deusirene
Fotos	Gláucio Dettmar Luiz Silveira
Arte e Designer	Divanir Junior

Sumário

Apresentação

O **sistema Processo Judicial eletrônico (PJe)** é um *software* elaborado pelo Conselho Nacional de Justiça (CNJ) a partir da experiência e com a colaboração de diversos tribunais brasileiros.

O objetivo principal buscado pelo CNJ é elaborar e manter um sistema de processo judicial eletrônico capaz de permitir a prática de atos processuais pelos magistrados, servidores e demais participantes da relação processual diretamente no sistema, assim como o acompanhamento desse processo judicial, independentemente de o processo tramitar na Justiça Federal, na Justiça dos Estados, na Justiça Militar dos Estados e na Justiça do Trabalho.

Além desse grande objetivo, o CNJ pretende fazer convergir os esforços dos tribunais brasileiros para a adoção de uma solução única, gratuita para os próprios tribunais e atenta para requisitos importantes de segurança e de interoperabilidade, racionalizando gastos com elaboração e aquisição de *softwares* e permitindo o emprego desses valores financeiros e de pessoal em atividades mais dirigidas à finalidade do Judiciário: resolver os conflitos.

Neste material, você conhecerá um pouco mais do processo eletrônico, de como ele pode beneficiar a administração da Justiça, como ele está sendo elaborado no sistema PJe e como um tribunal pode se preparar para começar a utilizar essa ferramenta.

O PROCESSO ELETRÔNICO

O processo judicial eletrônico, tal como o processo judicial tradicional, em papel, é um instrumento utilizado para chegar a um fim: a decisão judicial definitiva capaz de resolver um conflito. A grande diferença entre um e outro é que o eletrônico tem a **potencialidade** de reduzir o tempo para se chegar à decisão.

A redução do tempo pode ocorrer de várias maneiras:

- extinguindo atividades antes existentes e desnecessárias em um cenário de processo eletrônico, tais como juntadas de petições, baixa de agravos de instrumento, juntadas de decisões proferidas por Cortes especiais ou pelo Supremo Tribunal Federal;
- suprimindo a própria necessidade de formação de autos de agravo em razão da disponibilidade inerente do processo eletrônico;
- eliminando a necessidade de contagens e prestação de informações gerenciais para órgãos de controle tais como as corregedorias e os conselhos;
- atribuindo ao computador tarefas repetitivas antes executadas por pessoas – e, portanto, propensas a erros –, tais como a contagem de prazos processuais e prescricionais;
- otimizando o próprio trabalho nos processos judicias, acrescentando funcionalidades antes inexistentes capazes de agilizar a apreciação de pedidos e peças processuais;
- deslocando a força de trabalho dedicada às atividades suprimidas para as remanescentes, aumentando a força de trabalho na área fim;
- automatizando passos que antes precisavam de uma intervenção humana;
- permitindo a execução de tarefas de forma paralela ou simultânea por várias pessoas.

Essas medidas têm como resultado a redução do tempo de atividades acessórias ao processo judicial, permitindo que sejam praticados mais atos tendentes à solução do processo e, portanto, agilizando a solução dos conflitos.

Uma comparação razoável seria imaginar o Judiciário como um veículo que tem que transportar uma carga de um ponto a outro. A carga seria a decisão judicial, o motor, os magistrados e servidores; e o tempo e o combustível, o custo do processo judicial. Em um processo tradicional, o Judiciário seria um caminhão pesado, gastando mais combustível e levando mais tempo para chegar ao destino porque seu motor tem que mover, além da carga "útil", a carga do próprio caminhão. No processo eletrônico, o Judiciário seria um veículo de passeio, com um motor mais leve, que consegue levar a carga ao destino mais rápido e com um custo menor.

Efeitos do processo eletrônico

Embora seja apenas um meio, o processo eletrônico traz algumas mudanças significativas na gestão dos tribunais. Há uma verdadeira revolução na forma de trabalhar o processo judicial. A essa revolução deve corresponder uma revisão das rotinas e práticas tradicionais, porquanto o que havia antes deve adaptar-se à nova realidade.

A primeira grande mudança é relativa à guarda do processo. No regime tradicional, o processo judicial fica nas mãos e sob a responsabilidade do diretor de secretaria, do escrivão, do magistrado e dos advogados. Com o processo eletrônico, essa responsabilidade recai sobre quem tem a atribuição de guardar os dados da instituição – a área de tecnologia da informação. O processo eletrônico passa a poder estar em todos os lugares, mas essa facilidade vem acompanhada da necessidade de ele não estar em qualquer lugar, mas apenas naqueles lugares apropriados – a tela do magistrado, do servidor, dos advogados e das partes. Isso faz com que a área de tecnologia da informação se torne **estratégica**, pareando-se, do ponto de vista organizacional, com as atividades das secretarias e dos cartórios judiciais.

A segunda grande mudança deve ocorrer na distribuição do trabalho em um órgão judiciário. Em varas de primeiro grau e em órgãos que processam feitos originários, boa parte do tempo do processo é despendido na secretaria, para a realização de atos processuais determinados pelos magistrados. Suprimidas as atividades mecânicas, haverá uma **atrofia** de secretarias e cartórios, ao que corresponderá uma redução do tempo necessário para que um processo volte aos gabinetes, que se verão repletos de processos em um curto espaço de tempo. Há a necessidade, portanto, de deslocar a força de trabalho das secretarias e cartórios para os gabinetes dos magistrados. Essa é uma mudança que demonstra de forma cristalina como o processo eletrônico pode levar a uma melhoria na atividade jurisdicional, já que é lá, no gabinete, que são produzidos os atos que justificam sua existência.

O terceiro grande impacto ocorre na cultura estabelecida quanto à tramitação do processo judicial. Embora ainda não tenham ocorrido mudanças legislativas a respeito, é certo que o processo eletrônico, em razão de sua ubiquidade, dispensa práticas até hoje justificáveis e presentes nos códigos de processo, como a obrigatoriedade de formação de instrumento em recursos. Mais que isso. Não há mais a necessidade de uma **tramitação linear** do processo, o qual, podendo estar em vários lugares ao mesmo tempo, retira qualquer justificativa para a concessão de prazos em dobro em determinadas situações. Não bastasse isso, como se verá adiante, o PJe inova substancialmente a própria forma de trabalho utilizada.

Finalmente, há o impacto do funcionamento ininterrupto do Judiciário, com possibilidade de peticionamento 24 horas, 7 dias por semana, permitindo uma melhor gerência de trabalho por parte dos atores externos e internos. Além disso, a disponibilidade possibilita que se trabalhe de qualquer lugar do mundo, a qualquer hora, o que também causará gigantescas modificações na forma como lidamos com o processo.

História do PJe

O projeto PJe – Processo Judicial Eletrônico – foi iniciado no Conselho Nacional de Justiça, em setembro de 2009. Esse começo, na verdade, foi uma retomada dos trabalhos realizados pelo CNJ junto com os cinco tribunais regionais federais e com o Conselho da Justiça Federal (CJF). Naquele momento, foram reunidas as experiências dos tribunais federais e, quando o projeto foi paralisado, o Tribunal Regional Federal da 5ª Região (TRF5) deu início, por conta própria, à execução.

O CNJ e os demais tribunais, ao terem conhecimento de tais circunstâncias, visitaram o TRF5 para conhecer os procedimentos e concluíram que aquele era o projeto que atendia às restrições mais críticas com grande potencial de sucesso, atentando especialmente para a necessidade de uso de *software* aberto, para a conveniência de o conhecimento ficar dentro do Judiciário e para o fato de se observar as demandas dos tribunais.

Após a celebração do convênio inicial com o CJF e com os cinco regionais federais, o sistema foi apresentado para a Justiça do Trabalho e para muitos tribunais de justiça. A Justiça do Trabalho aderiu em peso por meio de convênio firmado com o Conselho Superior da Justiça do Trabalho (CSJT) e com o Tribunal Superior do Trabalho (TST), os quais firmaram, por sua vez, convênios com todos os tribunais regionais do trabalho. Aderiram também 16 tribunais de justiça e o Tribunal de Justiça Militar de Minas Gerais.

O sistema foi instalado em abril em 2010 na Subseção Judiciária de Natal/RN, pertencente ao TRF5, sendo aperfeiçoado desde então, assim como instalado em outras seções judiciárias daquele tribunal. Em dezembro de 2010, será instalada a versão nacional no Tribunal de Justiça de Pernambuco e no Tribunal Regional Federal da 3ª Região, a partir do que será validada a versão a ser disponibilizada para os demais tribunais que aderiram ao projeto.

A gerência do projeto

O projeto é coordenado pela Comissão de Tecnologia da Informação e Infraestrutura do Conselho Nacional de Justiça, presidida pelo Ministro Cezar Peluso e integrada também pelos conselheiros Walter Nunes e Felipe Locke.

Na gestão direta, o projeto conta com um comitê formado por dois juízes auxiliares da Presidência do Conselho Nacional de Justiça e nove magistrados, três de cada um dos principais segmentos do Judiciário que fazem parte do projeto.

Sob esse comitê, há a gerência técnica do projeto, formada por três servidores do Judiciário capacitados em gestão de projetos, um grupo gerenciador de mudanças e o grupo de interoperabilidade. O grupo gerenciador de mudanças tem a responsabilidade de tratar das solicitações de mudanças a partir do momento da implantação da versão nacional. O grupo de interoperabilidade, por estabelecer as diretrizes de troca de informação entre o Judiciário e os outros participantes da administração da Justiça. Em razão disso, esse grupo é formado por representantes do Conselho Nacional do Ministério Público, do Conselho Federal da Ordem dos Advogados do Brasil, da Advocacia-Geral da União, da Defensoria Pública da União, de Procuradores de Estado e de Procuradores de Município.

O CRONOGRAMA

Além das versões preliminares que já foram instaladas no Tribunal Regional Federal da 5ª Região, o projeto tem quatro versões nacionais previstas para entrega em um ano:

Versão	Lançamento	Características gerais
1.0	dezembro/2010	Versão inicial, com possibilidade de tramitação de processos judiciais de qualuqer natureza, mas focado no processo civil, contemplando replicação de dados e distribuição objetiva dos processos judiciais
1.2	março/2011	Versão contemplando características específicas dos processos criminais e automatização de ritos processuais específicos decorrentes da definição de fluxos por classes
1.4	junho/2011	Inclusão de características de interoperabilidade com sistemas externos mais robustas, suprimindo-se a necessidade de os magistrados ou servidores fazerem uso de sistemas de terceiros para praticar atos de interesse do processo judicial
2.0	dezembro/2011	Revisão da forma de gravação de documentos processuais, permitindo um maior controle da atuação.

Os detalhes de cada uma das versões podem ser consultados pelos representantes dos tribunais participantes no portal do projeto no sítio de colaboração do Conselho Nacional de Justiça http://colaboracao.cnj.jus.br/projects/show/sisprocessual.

O QUE MUDA?

O sistema PJe trará uma verdadeira revolução ao Judiciário Brasileiro.

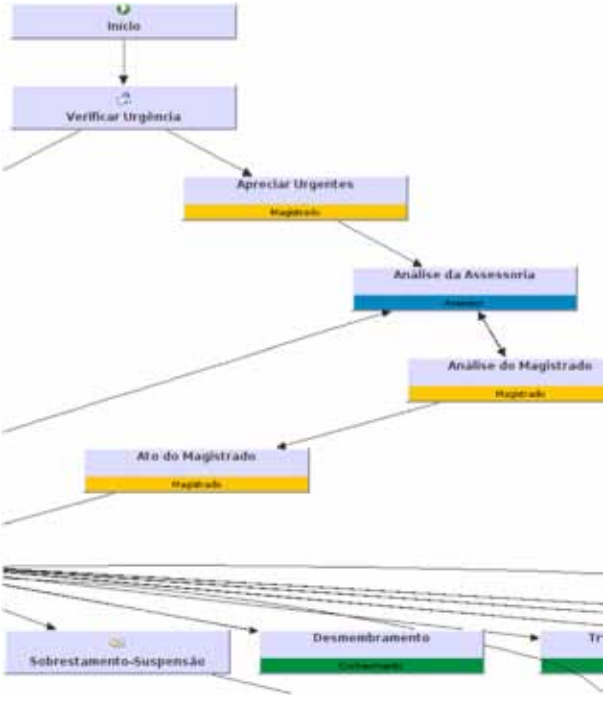
Neste tópico, apresentamos uma relação das grandes quebras de paradigma que ele acarretará.

FLUXOS

O PJe já está fazendo uso de fluxos para a definição de como o processo judicial deverá tramitar. É possível atribuir um fluxo diferente para cada uma das classes processuais existentes. Quanto mais específico o fluxo, mais fácil será automatizar tarefas de gabinete e secretaria.

À primeira vista, pode ser que pensemos que essa é uma característica dispensável. A experiência mostra, no entanto, que ela é essencial.

Com honrosas exceções, a grande maioria dos sistemas processuais trabalha em dois extremos no que concerne à tramitação ou ao acompanhamento da tramitação dos processos judiciais.

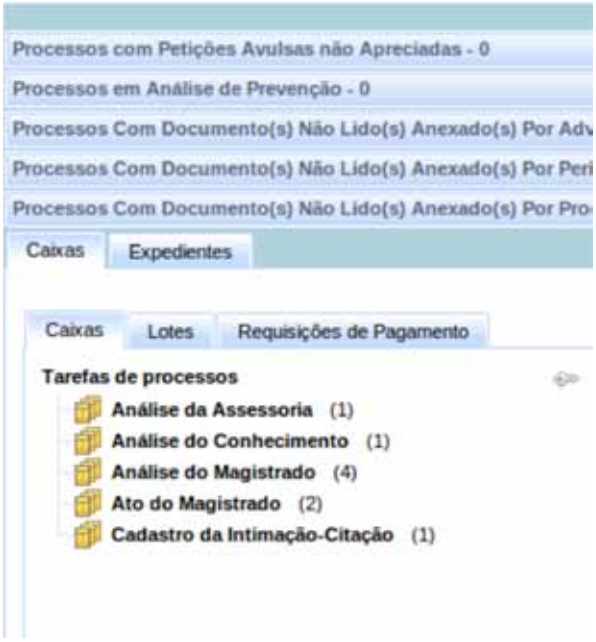


De um lado, temos o engessamento total: o sistema tem em seu código os passos passíveis de serem praticados e alteração dessa via reclama reescrever o programa em algum grau.

Do outro lado, temos a liberdade absoluta: o sistema permite que o usuário pratique qualquer ato. Não há limites e, em razão disso, surge o problema dos erros reiterados: sem freio, uma desatenção momentânea pode fazer com que um processo siga um tortuoso caminho, inclusive com a possibilidade da anulação da decisão. Mais que isso, a liberdade total não vem sem outro custo: uma imensa dificuldade em automatizar procedimentos, já que sempre é necessária uma intervenção humana para, fazendo uso da inteligência, informar à máquina qual deve ser o próximo passo.

O PJe, com seus fluxos configuráveis, fica entre esses dois extremos. Embora se possa definir caminhos mais rígidos se isso for **conveniente ou necessário**, a alteração dos fluxos não depende da reescrita do sistema ou do pessoal da TI, mas da atuação de alguém que conhece processo judicial, muito provavelmente um servidor especialista do tribunal. Além disso, esses caminhos rígidos podem levar à automatização de tarefas repetitivas. Finalmente, pode-se definir caminhos tão amplos que estaríamos simulando a situação da liberdade absoluta. Tudo depende de como se quer ver o sistema funcionar.

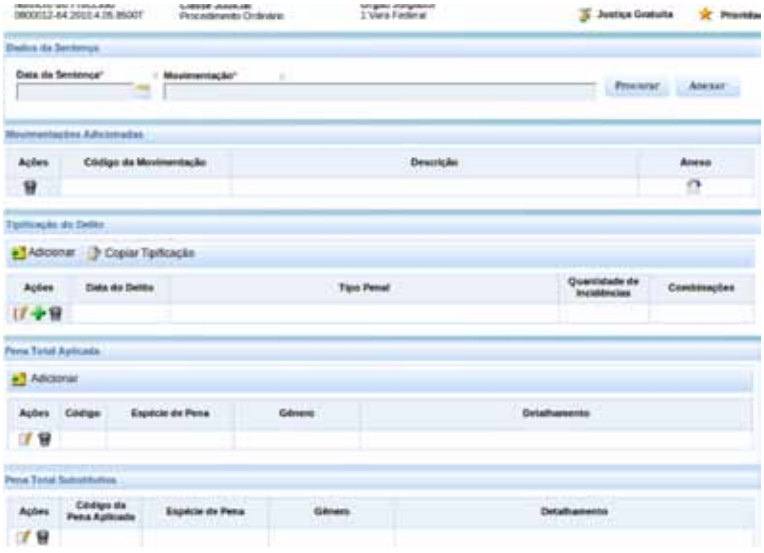
Atos ou movimentos?

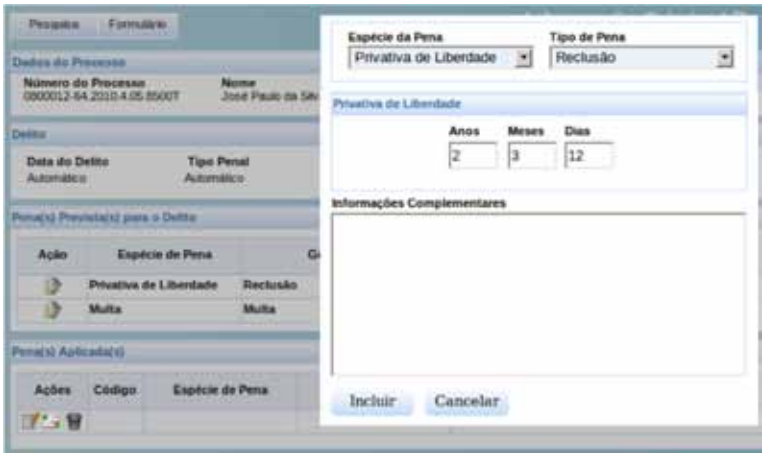


O PJe estimula, igualmente, uma significativa mudança na forma de se conduzir processos judiciais em secretaria.

Ordinariamente, o acompanhamento eletrônico da tramitação de processos judiciais é feito em um regime de pós-fato: pratica-se um ato e, então, registra-se que ele aconteceu por meio do lançamento de movimentações. No PJe, os fluxos permitem que essa lógica seja alterada: pratica-se o ato e lança-se a movimentação no mesmo momento. Em situações específicas, o magistrado e o servidor nem sequer perceberão que a movimentação foi lançada porque isso é feito independentemente de uma atuação dirigida ao lançamento.

Essa nova abordagem trará significativo benefício à tramitação de processos, visto que o tempo perdido com o lançamento de movimentações será aproveitado na prática dos próprios atos, reduzindo o custo do processo. Esses benefícios mais intensos à medida que, com a experiência, os fluxos processuais sejam otimizados.





O PJe também trata de forma inovadora o processo criminal. Partindo-se da constatação de que é indispensável agregar informações individualizadas sobre delitos e informações que interferem no curso do processo criminal, foi criado no CNJ grupo específico para tratar do tema, envolvendo magistrados e servidores, tanto da área judiciária quanto de tecnologia da informação.

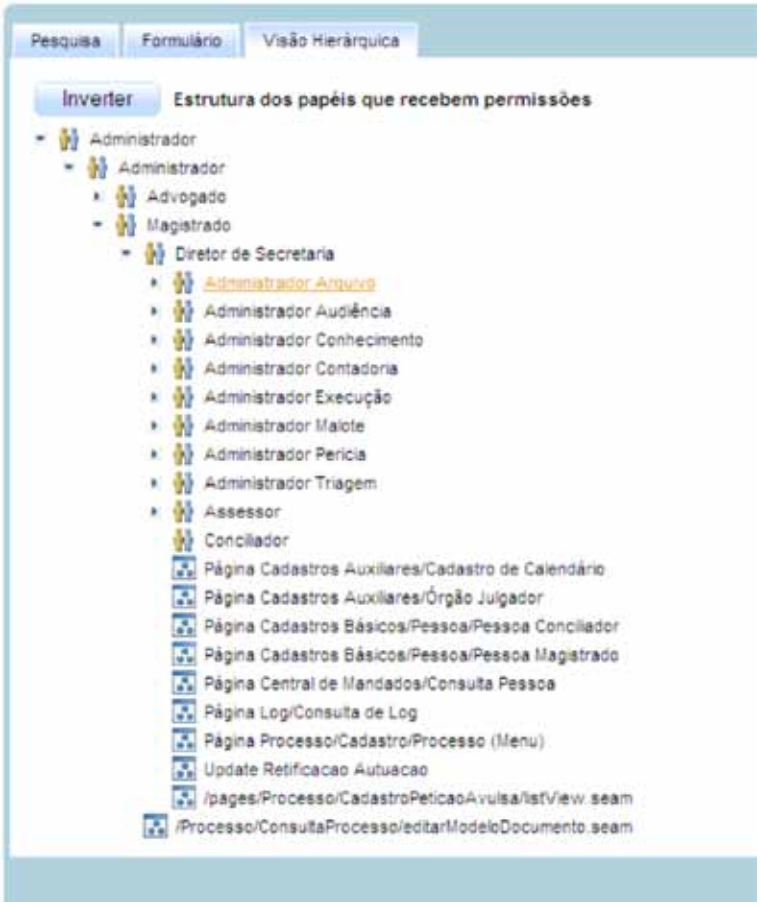
Como resultado, estão sendo elaboradas funcionalidades que primam por abranger todo o espectro do processo criminal, da tramitação do inquérito à reabilitação criminal, passando pelo acompanhamento da execução penal. As informações de prisão, soltura, condenação são armazenadas de forma individual – por réu – chegando-se ao detalhe de indicar a magistrados e servidores quais penas estão previstas para cada tipo penal.

Tudo isto permitirá um controle muito mais efetivo pelas partes, pelos procuradores e pelos magistrados, com verificação dos riscos de prescrição punitiva e executória, registro dos fatos de interesse para a execução criminal, contagens automáticas de prazos de cumprimento e outras facilidades que reduzirão o tempo de análise dos processos criminais.

Poderemos ainda expedir certidões nacionais e trocar informações com os órgãos de segurança pública de forma mais eficiente.

Segurança e liberdade

O Processo Judicial eletrônico traz para o processo eletrônico uma liberdade que era onipresente em sistemas de acompanhamento processual e que se perdeu com a implantação de sistemas de processo eletrônico: a de definir com precisão quais os poderes de um determinado usuário. A regra geral é que, nos novos sistemas, criavam-se "perfis" e se instaurava uma sistemática de "tudo ou nada": ou se atribui ou não se atribui um perfil.



No PJe, embora essa sistemática de perfis possa ser mantida, os administradores de uma comarca ou subseção e os administradores de Órgãos judiciários podem definir com extrema precisão o que pode ou não ser acessado por um usuário. Assim, ele pode atribuir um perfil pré-definido, mas também pode acrescentar recursos àquele usuário específico, sem precisar entrar em contato com a TI para alterar o perfil – procedimento que, inclusive, pode ter impacto negativo em outras unidades judiciárias.

Tem-se, portanto, mais liberdade para definição dos poderes de cada usuário da unidade, o que contribui para a segurança do trâmite do processo judicial, porquanto o magistrado, o escrivão ou o diretor de secretaria poderão delegar poderes somente àqueles que efetivamente têm a responsabilidade para os exercer, sem serem obrigados a escolher entre um perfil poderoso, mas que não poderia ser dado a um determinado usuário, e um perfil débil, que não trará as funcionalidades necessárias para um adequado andamento da vara.

Ser um ou ser muitos, eis a questão

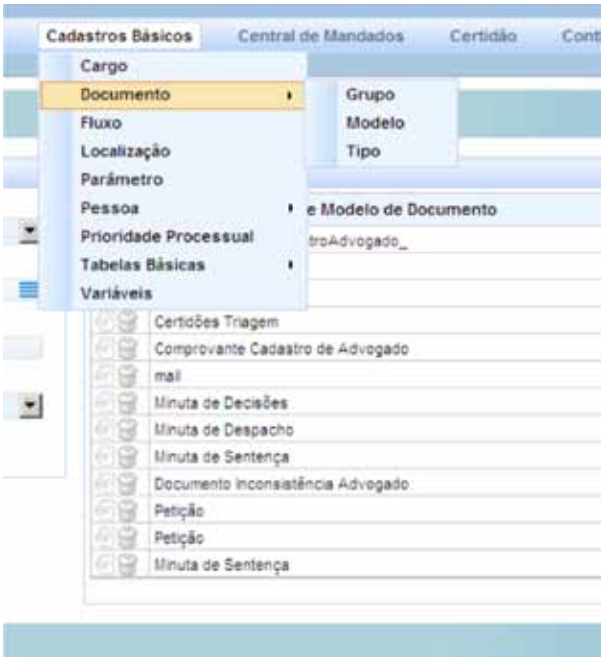
Além da facilidade de definir os perfis, é possível no PJe atribuir mais de um perfil a um mesmo usuário, inclusive em localidades ou órgãos diferentes.

Ao lado da possibilidade de se utilizar perfis padronizados sem a necessidade de modificação para usuário idêntico, a ideia é permitir a otimização dos recursos humanos, com a possibilidade de um mesmo servidor do Judiciário atuar em órgãos ou varas diversas sem a necessidade de deslocamento físico ou de nova lotação.

Com isso, aquelas varas ou secretarias assoberbadas poderão receber auxílio momentâneo de servidores lotados em varas que estão com demanda aquém de sua capacidade regular.

Modelos de documentos

A utilização de modelos de documentos pessoais ou de um determinado Órgão é prática amplamente difundida no Judiciário. Essa reutilização estimula a existência de padrões, reduz a possibilidade de erros e agiliza o tempo de aprendizagem de novos integrantes das equipes.

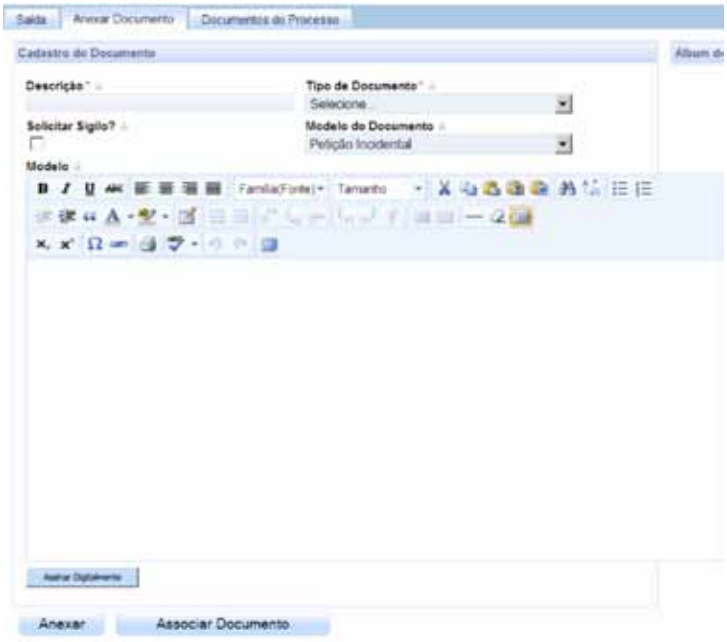


O PJe não poderia, em razão disso, deixar de prever a utilização de modelos de documentos. Avança-se já na versão inicial, permitindo-se a classificação de modelos, o que viabiliza a automatização dos fluxos processuais. Admite-se ainda que os atores externos, notadamente os advogados de escritórios pessoais ou de menor porte, mantenham seus modelos mais comuns no sistema, colaborando-se assim com a agilidade do processo.

Nas versões futuras, essa sistemática estará melhorada com a adoção de taxonomia mais estável de tipos de documentos e com a possibilidade de estruturação dos documentos apresentados pelas partes e produzidos no próprio sistema, por elas ou pelos servidores do Judiciário

Produção de documentos no sistema, e não para o sistema

O PJe estimula o advogado e os demais participantes do processo judicial a elaborem seus documentos **no próprio sistema**, utilizando editor de texto integrado ao navegador Web.



Esse estímulo tem várias razões de ser: não se obriga o advogado nem o tribunal a adquirir processadores de texto proprietários com alto custo para as organizações; os documentos produzidos têm reduzido tamanho de armazenamento e transmissão, permitindo manter a infraestrutura de comunicação mais modesta e garantindo maior velocidade para acesso ao conteúdo; os documentos são facilmente indexáveis por ferramentas automáticas, facilitando pesquisas rápidas em seus metadados e conteúdos.

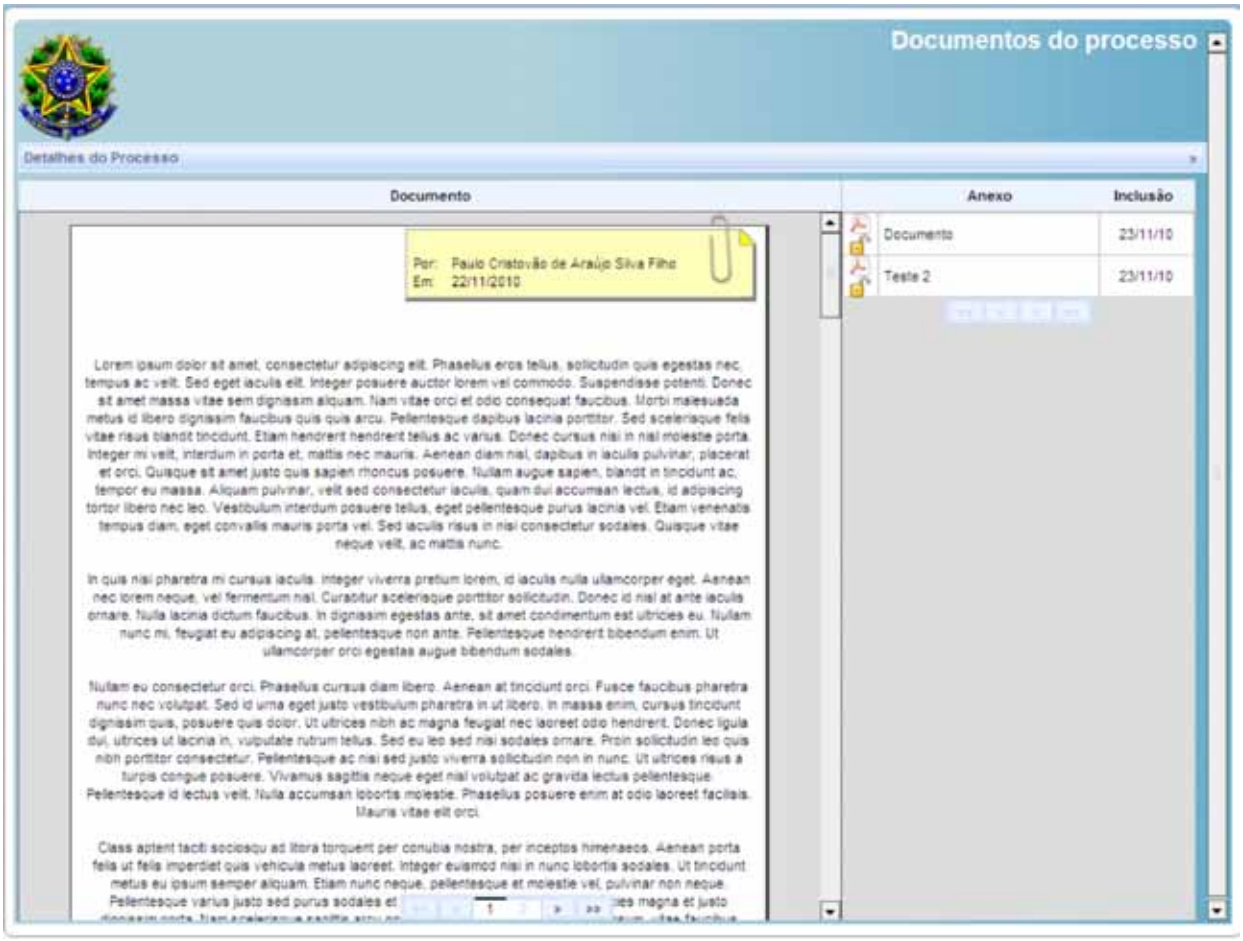
É claro que os editores utilizados têm alguns recursos a menos que aqueles constantes em processadores de texto, mas é certo que essas limitações têm pouco ou nenhum impacto sobre a produção de um documento jurídico, como são aqueles com os quais tratamos. Mais à frente, os benefícios decorrentes disso surgirão na forma de jurisprudências mais selecionadas, facilidade de uso e visualização.

A VISUALIZAÇÃO DO PROCESSO

Um dos grandes calcanhares dos sistemas processuais eletrônicos é a visualização do processo. Sair de um encarte de peças processuais sequenciais para uma sequência de cliques e janelas múltiplas é doloroso para quem lida tradicionalmente com processos judiciais.

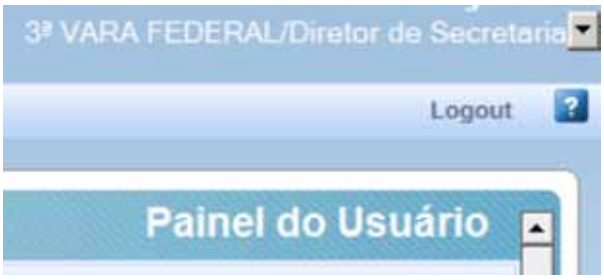
No PJe, isso é facilitado pelo uso de um novo visualizador capaz de mostrar as peças sequencialmente, sem a necessidade de abrir novas janelas e com a apresentação simultânea de alguns metadados sobre a peça sob visualização. Essa nova forma de ver o processo, combinada com o uso de dois monitores nos computadores de quem vai operar o sistema, permitirá ganho significativo de produtividade, chegando próximo ao uso direto dos autos.

Mais à frente, com a inclusão de marcadores personalizados nos documentos, esse ganho se tornará ainda maior, muito provavelmente tornando o processo eletrônico substancialmente mais fácil de examinar que os processos tradicionais.



Ajuda em contexto e editável

Ajudar o usuário a entender como funciona um sistema é um dos grandes desafios de quem o elabora. No PJe, isso pode ser feito de forma colaborativa e de modo muito mais intuitivo em razão da ajuda contextual e da utilização do formato ***wiki*** na produção da ajuda.



Essas expressões significam que, ao clicar na ajuda, o usuário não se deparará com um índice da ajuda, mas com o texto relativo especificamente à página que estava aberta no momento em que ele clicou. Além disso, o próprio texto da ajuda não é estável, e sim **editável por usuários selecionados pelo tribunal**, de modo que ela ganha o dinamismo próprio das ferramentas colaborativas hoje amplamente conhecidas. Se encontrada uma dúvida não esclarecida, o editor da ajuda pode, desde logo, modificar o texto para que todos, e não apenas aquele que perguntou, tomem conhecimento da solução.

Pesquisa textual

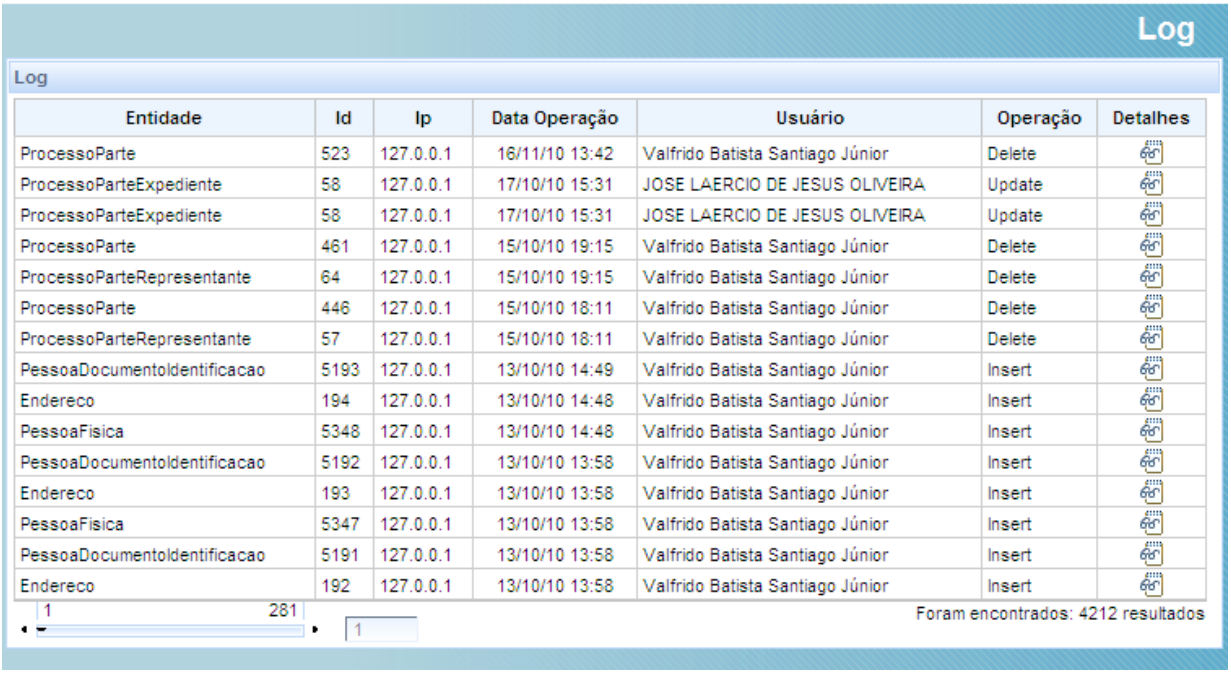
O PJe também inova no que concerne à pesquisa de dados. Em vez de extensos formulários, o usuário pode usar um campo de pesquisa que funciona da maneira já consagrada nas ferramentas de busca da internet.

Tudo aquilo que for indexável e acessível ao usuário ficará acessível de forma rápida e eficiente. E isso não prejudica a pesquisa tradicional com a aplicação de filtros em telas de trabalho.

Registro das alterações

Já obedecendo a requisito previsto no MoReq-Jus aprovado pela Resolução n. 91, o PJe armazena registros de todas as alterações ocorridas no sistema para eventual necessidade de posterior auditoria.

A medida, em vez de ser mero preciosismo, é imprescindível em um momento em que o processo sai do campo físico, no qual temos a sensação de segurança quanto à imutabilidade dos atos processuais, para o campo do virtual, no qual a sensação mais comum é a de imaterialidade.



Log

Log

Entidade	Id	Ip	Data Operação	Usuário	Operação	Detalhes
ProcessoParte	523	127.0.0.1	16/11/10 13:42	Valfrido Batista Santiago Júnior	Delete	
ProcessoParteExpediente	58	127.0.0.1	17/10/10 15:31	JOSE LAERCIO DE JESUS OLIVEIRA	Update	
ProcessoParteExpediente	58	127.0.0.1	17/10/10 15:31	JOSE LAERCIO DE JESUS OLIVEIRA	Update	
ProcessoParte	461	127.0.0.1	15/10/10 19:15	Valfrido Batista Santiago Júnior	Delete	
ProcessoParteRepresentante	64	127.0.0.1	15/10/10 19:15	Valfrido Batista Santiago Júnior	Delete	
ProcessoParte	446	127.0.0.1	15/10/10 18:11	Valfrido Batista Santiago Júnior	Delete	
ProcessoParteRepresentante	57	127.0.0.1	15/10/10 18:11	Valfrido Batista Santiago Júnior	Delete	
PessoaDocumentoIdentificacao	5193	127.0.0.1	13/10/10 14:49	Valfrido Batista Santiago Júnior	Insert	
Endereco	194	127.0.0.1	13/10/10 14:48	Valfrido Batista Santiago Júnior	Insert	
PessoaFisica	5348	127.0.0.1	13/10/10 14:48	Valfrido Batista Santiago Júnior	Insert	
PessoaDocumentoIdentificacao	5192	127.0.0.1	13/10/10 13:58	Valfrido Batista Santiago Júnior	Insert	
Endereco	193	127.0.0.1	13/10/10 13:58	Valfrido Batista Santiago Júnior	Insert	
PessoaFisica	5347	127.0.0.1	13/10/10 13:58	Valfrido Batista Santiago Júnior	Insert	
PessoaDocumentoIdentificacao	5191	127.0.0.1	13/10/10 13:58	Valfrido Batista Santiago Júnior	Insert	
Endereco	192	127.0.0.1	13/10/10 13:58	Valfrido Batista Santiago Júnior	Insert	

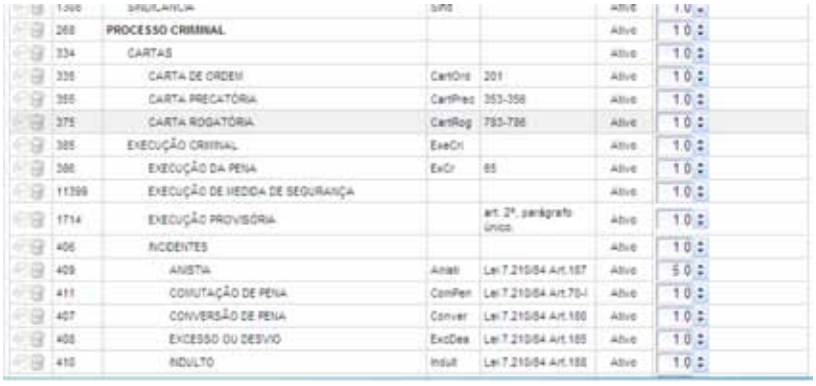
1 281

Foram encontrados: 4212 resultados

1

Tabelas unificadas

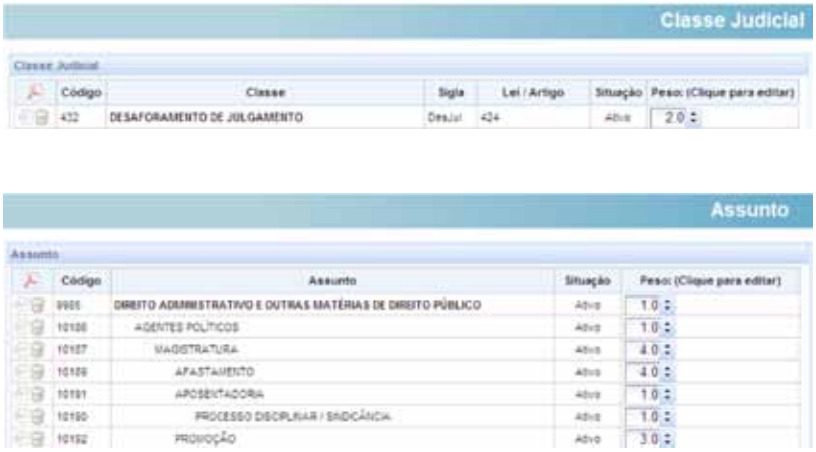
O PJe também já trará consigo as tabelas unificadas nacionais. As alterações futuras dessas tabelas serão acompanhadas da atualização do PJe, evitando o retrabalho que hoje existe quando elas são republicadas.



268	PROCESSO CRIMINAL			Ativo	1.0	
334	CARTAS			Ativo	1.0	
336	CARTA DE ORDEM	CartOrd	201	Ativo	1.0	
355	CARTA PRECATÓRIA	CartPrec	353-358	Ativo	1.0	
375	CARTA ROGATÓRIA	CartRog	783-786	Ativo	1.0	
385	EXECUÇÃO CRIMINAL	ExeCri		Ativo	1.0	
386	EXECUÇÃO DA PENA	ExCr	65	Ativo	1.0	
11399	EXECUÇÃO DE MEDIDA DE SEGURANÇA			Ativo	1.0	
1714	EXECUÇÃO PROVISÓRIA		art. 2º, parágrafo único	Ativo	1.0	
406	INCIDENTES			Ativo	1.0	
409	ANISTIA	Anist	Lei 7.210/84 Art.187	Ativo	5.0	
411	COMUTAÇÃO DE PENA	ComPen	Lei 7.210/84 Art.70-I	Ativo	1.0	
407	CONVERSÃO DE PENA	Conver	Lei 7.210/84 Art.180	Ativo	1.0	
408	EXCESSO OU DESVIO	ExcDes	Lei 7.210/84 Art.185	Ativo	1.0	
410	INDULTO	Indult	Lei 7.210/84 Art.188	Ativo	1.0	

Distribuição mais transparente e justa

A distribuição dos processos judiciais é até hoje um grande problema dos tribunais brasileiros. Há uma sensação de falta de transparência que, infelizmente, colabora para formar uma imagem negativa do Poder Judiciário. Do lado interno, muitos magistrados têm a sensação de injustiça na distribuição do trabalho.



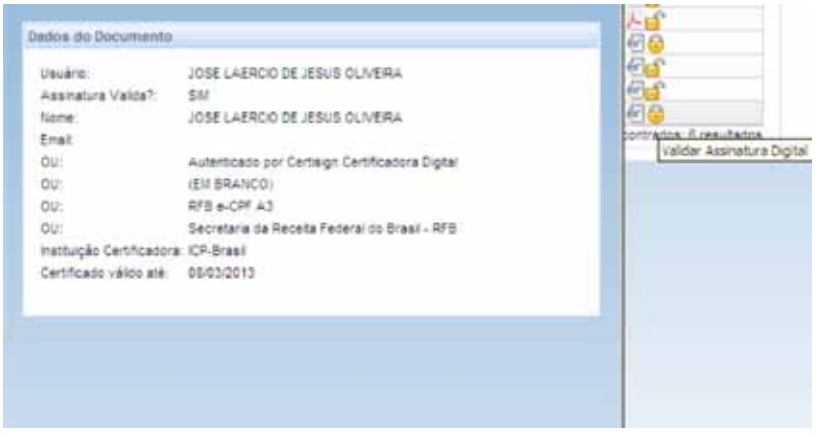
No PJe, a distribuição recebeu uma especial atenção. Embora seja possível manter o modelo atual mais comum, fundado na igualdade de processos entre classes processuais, a distribuição será regida por um conjunto de fatores que levarão a medir o verdadeiro trabalho decorrente do processo. Esses fatores podem ser trabalhados pelas corregedorias e presidências de modo a deixar claros os critérios adotados, e justa a distribuição da carga de trabalho, sem que isso afete o princípio do Juiz Natural e a obrigação legal de sorteio dos processos entre os igualmente competentes.

O trabalho foi realizado com a participação de representantes especialistas na área de distribuição de diversos tribunais brasileiros e contempla praticamente todas as hipóteses possíveis, tornando objetiva a distribuição.

Finalmente, a sistemática é cercada de cuidados que permitirão demonstrar para os jurisdicionados a retidão na distribuição dos processos.

Uso de assinatura digital com certificado

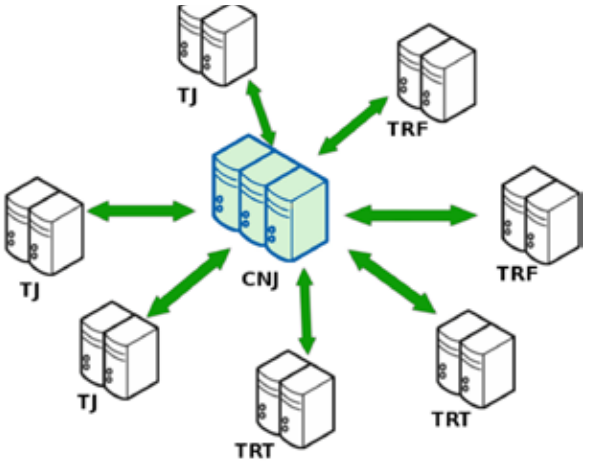
O PJe trabalhará desde o início com o uso de assinaturas digitais com base em certificados da estrutura do ICP-Brasil. Trata-se de medida também prevista no modelo de requisitos de sistemas judiciários que assegurará características importantes para a segurança do processo judicial eletrônico.



Mais adiante, esse recurso permitirá que o advogado, entregando documentos eletrônicos assinados, possa repassar a tarefa de protocolo para seus auxiliares, reduzindo, assim, a necessidade de interação direta com o sistema.

Replicação automática de informações de gestão

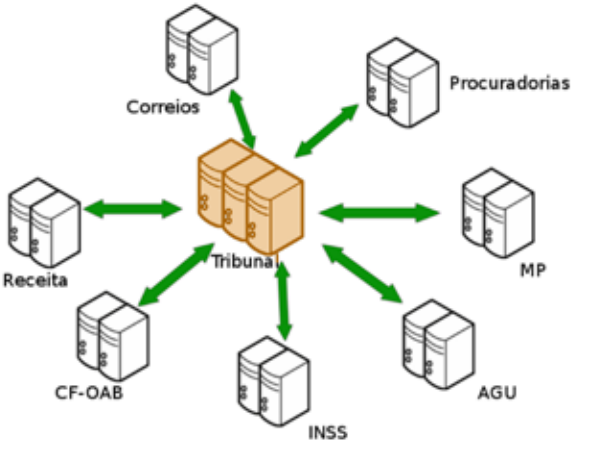
O Conselho Nacional de Justiça e os demais conselhos solicitam periodicamente informações aos tribunais. Essas informações são utilizadas para a tomada de decisões estratégicas de gestão e de política legislativa no Poder Judiciário. Embora extremamente importantes, a produção das informações consomem muitos recursos dos tribunais, que alocam servidores e outros recursos para essas atividades. Essa, inclusive, é uma das mais recorrentes reclamações dos magistrados.



No PJe, a maior parte das informações serão replicadas automaticamente, sem necessidade de alocação de recursos dos tribunais, o que liberará os recursos e pessoal para outras atividades mais vinculadas ao fim do Poder Judiciário. Além disso, essa replicação automatizada permitirá a concretização de serviços essenciais para nosso sistema atual, tais como a emissão de certidões negativas e a verificação de prevenção nacional.

Integração com terceiros

O PJe também permitirá a integração dos tribunais com sistemas de terceiros colaboradores do Judiciário e, mais adiante, com sistemas de escritórios de advocacia. As procuradorias e escritórios de advocacia poderão, em razão disso, trabalhar em seus próprios sistemas. A comunicação entre esses sistemas e o dos tribunais será feita exclusivamente pelos computadores.



Isso tem por efeito direto uma melhor aceitação do sistema pelos atores externos, com a redução do impacto sobre suas atividades, além do efeito indireto de reduzir as demandas de infraestrutura para tratamento das solicitações nos sítios de internet dos tribunais.

O sistema já está integrado com a Secretaria da Receita Federal do Brasil – o que facilita o cadastramento das partes e evita a multiplicação de homônimos – e com o Conselho Federal da Ordem dos Advogados do Brasil – que valida o cadastro de advogados no sistema.

Pretende-se, nas versões futuras, concluir a integração com as procuradorias, com o Ministério Público e com os Correios, além de outros órgãos que têm intensa ligação com o Judiciário.

Preparação do tribunal

A instalação de novo sistema processual não é algo simples. Como se viu no transcorrer do texto, há muitas mudanças e o ser humano naturalmente é avesso a elas. Além disso, é imprescindível a preparação da infraestrutura do tribunal para receber o sistema a fim de evitar surpresas no futuro.

Em razão disso, apresentamos a seguir um guia rápido, mas não exaustivo, do que deve ser feito. Ele deve ser complementado considerando as características próprias de cada tribunal.

Escolha da estratégia de implantação

O primeiro passo para a instalação do sistema é escolher uma estratégia de implantação. A instalação em múltiplas frentes tem a desvantagem de potencializar o efeito de problemas simples, já que este se reproduzirá em vários pontos ao mesmo tempo. Por outro lado, instalar em apenas um ponto pode ocultar a emergência de desafios que seriam localizados em outras varas.

O ideal é partir para a implantação em sistema de piloto, após breve homologação e treinamento dos usuários da unidade piloto, que também deverá ser escolhida entre as que têm maior tendência de colaborar com a implantação. Essa boa vontade é imprescindível para que a comunicação seja estabelecida e as soluções para os inevitáveis problemas sejam alcançadas.

Do ponto de vista da competência, a utilização em piloto reclama delimitação clara para evitar confusões com os atores externos. Além disso, é fundamental ter planos de contingência para os casos em que seja impossível o tratamento dos casos via sistema.

Preparação dos recursos humanos

Para a instalação de novo sistema, o primeiro passo é preparar os recursos humanos. São os servidores do Judiciário que darão vida ao sistema e, na falta deles e da sua boa vontade, qualquer iniciativa fracassará.

É necessário, portanto, que sejam abertas duas frentes para essa preparação: treinamento do pessoal da área de tecnologia da informação e treinamento de servidores da área fim quanto à configuração e uso do sistema.

O pessoal da área de TI deve estar preparado para instalar e manter o sistema, assim como encontrar, reparar e reportar erros. Nesse ponto, a comunicação é o grande fator determinante. O CNJ ofertou e prosseguirá oferecendo cursos para que o pessoal de TI se prepare para o uso do sistema. Além dessa capacitação, é importante que ao menos dois servidores de TI acompanhem a configuração do sistema para tirarem dúvidas dos servidores da área judiciária e busquem neles o esclarecimento daquelas relativas ao que se quer na configuração.

Na área judiciária, devem ser preparados servidores para as seguintes áreas: administração do sistema; administração de órgão julgador e uso em geral. A configuração da administração do sistema, por ocasião da instalação do PJe pelo CNJ, deve ser acompanhada pelos servidores da área responsável, o que dará uma substancial base de conhecimento. A administração de órgão julgador deverá ser preparada para multiplicadores, preferencialmente a começar pelos órgãos que funcionarem como piloto. Igual estratégia deve ser adotada quanto aos usuários.

Preparação do ambiente de tecnologia da informação

Um ambiente de tecnologia da informação adequadamente preparado tem significativo impacto sobre as impressões a respeito do sistema. Falhas, quedas e indisponibilidades podem dar a impressão de que um sistema é instável ou imprestável.

A equipe de tecnologia da informação do tribunal deve, portanto, preparar o ambiente de execução, tanto do ponto de vista de quem provê o sistema quanto de quem o utiliza.

Em razão disso, a Diretoria de Tecnologia de Informação do Conselho Nacional de Justiça, juntamente com os servidores líderes técnicos do projeto elaboraram as seguintes características para uma **instalação ótima do sistema**, sem embargo de ele poder funcionar em contextos mais modestos.

Ambientes dos usuários

Recurso	Descrição
Microcomputadores	• Processador de 2 núcleos com 2.0 GHz/núcleo; • 2GB de memória RAM; • 2 adaptadores de vídeo (para utilização de dois monitores) 2 monitores de vídeo com resolução mínima de 1024x768; • Leitora de cartão inteligente (smartcard) ou entrada USB para token criptográfico, conforme o hardware de certificados dos magistrados, servidores e auxiliares; • Navegadores: Mozilla Firefox 3.5 ou superior; Microsoft Internet Explorer 8.0 ou superior; quanto aos demais, recomenda-se testar a versão mais recente. O uso em sistemas operacionais outros que não o MS Windows será liberado na versão 1.2.
Scanners	A quantidade de scanners e sua configuração devem ser estudadas de acordo com a demanda prevista de documentos a serem digitalizados nos ambientes dos tribunais.
Sala de atendimento	Instalação de sala para autoatendimento dos advogados que praticarão atos diretamente nas dependências do órgão julgador, inclusive com equipamentos para digitalização. Este equipamento deverá ter tanto a leitura de cartão inteligente quanto a entrada USB para token criptográfico
Links de comunicação	Recomenda-se a adoção, por ambiente, de link de 2Mbps, conforme a Resolução 90 do CNJ
Certificados A3 ICP-Br	Os usuários do sistema obrigatoriamente devem utilizar certificados ICP-Brasil A3 para assinaturas de documentos no sistema. Os certificados têm validade de 3 anos.

Ambiente dos equipamentos servidores

Recurso	Descrição
Servidores de aplicação	2 servidores de aplicação, cada um com a seguinte configuração; • 2 processadores quad-core com 2.0GHz/núcleo; • 32 GB de memória RAM; • 75 GB de espaço em disco, preferencialmente em RAID 1 ou 5; • 2 interfaces SAN HBA de 8Gbps; • 2 interfaces de rede de 1Gbps; • Sistema operacional linux ou unix-like; • Java Runtime Environment versão 1.6;• JBoss Application Server versão 5.0.1.GA e • Certificado A1 ICP-Brasil
Servidores de banco de dados	2 servidores de bancos de dados, configurados como master e slave, instalados, cada um, com a seguinte configuração:; • 2 processadores quad-core com 2.0GHz/núcleo; • 32 GB de memória RAM; • 75 GB de espaço em disco do sistema operacional, preferencialmente em RAID 1 ou 5; • 2 x 2 TB de espaço em disco para os arquivos do sistema gerenciador de banco de dados, um para cada banco de dados do PJe, preferencialmente em RAID 5; • 2 interfaces SAN HBA de 8Gbps; • 2 interfaces de rede de 1Gbps; • Sistema operacional linux ou unix-like; • Java Runtime Environment versão 1.; • PostgreSQL 8.4.1 ou, na versão de março, Oracle 11g
Links entre os equipamentos servidores	O ideal é que os equipamentos servidores estejam interligados em rede de altíssima velocidade, se possível por meio de barramento de fibra ótica.

Observações:

Os servidores de aplicação podem ser máquinas virtuais

Sugere-se não virtualizar os servidores de bancos de dados

As interfaces SAN somente são necessárias caso sejam utilizados ***storages***

O espaço em disco indicado para os sistemas de bancos de dados pode ser suprido por ***storages*** de alta performance ligados em SAN ou em serviços de CAS transparentes para os CDBs

O espaço em disco indicado para armazenamento do banco de dados de arquivos binários pode ser suprido por ***storages*** ligados em rede TCP

CONCILIANDO

a gente se entende

Semana Nacional da Conciliação. De 29 de novembro a 3 de dezembro de 2010, a justiça brasileira precisa de você. Conciliar economiza tempo, dinheiro e promove a paz social. Participe. www.cnj.jus.br/conciliacao

CNJ CONSELHO NACIONAL DE JUSTIÇA

O Brasil faz a justiça

4º ENCONTRO NACIONAL DO JUDICIÁRIO

O BRASIL FAZ A JUSTIÇA

CNJ CONSELHO NACIONAL DE JUSTIÇA

www.cnj.jus.br

ANEXO B – Glossário ICP-BRASIL.

Infra-Estrutura de Chaves Públicas Brasileira

GLOSSÁRIO ICP-BRASIL

Versão 1.2

03.10.2007

PALAVRA CHAVE	DESCRIÇÃO
ABNT (Associação Brasileira de Normas Técnicas)	Fundada em 1940, é o órgão responsável pela normalização técnica no país, fornecendo a base necessária ao desenvolvimento tecnológico brasileiro.
Aceitação do Certificado Digital	Demonstração da concordância de uma pessoa física ou jurídica quanto à correção e adequação do conteúdo e de todo o processo de emissão de um certificado digital, feita pelo indivíduo ou entidade que o solicitou. O certificado é considerado aceito a partir de sua primeira utilização, ou após haver decorrido o prazo pré-estipulado para sua rejeição. A aceitação do certificado será declarada pelo titular.
Acesso	Estabelecimento de conexão entre um indivíduo ou entidade e um sistema de comunicação ou de informações. A partir do Acesso podem ocorrer a transferência de dados e a ativação de processos computacionais.
Acesso Físico	Habilidade de obter acesso a um ambiente físico. Os sistemas de controle de Acesso Físico possibilitam a integração de funcionalidades, com leitores biométricos, alarmes de incêndio, emissão de crachás para visitantes, etc.
Acesso lógico	O Controle de Acesso Lógico permite que os sistemas de Tecnologia da Informação verifiquem a identidade dos usuários que tentam utilizar seus serviços. Como exemplo mais comum, temos o *logon* de um usuário em um computador.
Acesso Remoto	Habilidade de obter acesso a um computador ou uma rede a distância. As conexões *dial-up, wireless*, DSL são exemplos de possibilidades de Acesso Remoto.
AES (Advanced Encryption Standard)	O Padrão de Cifração Avançada (AES) é uma cifra de bloco adotada como padrão de cifração pelo governo dos Estados Unidos. O AES é um dos algoritmos mais populares usados na criptografia de chave simétrica. AES tem um tamanho de bloco fixo de 128 bits e uma chave com tamanho de 128, 192 ou 256 bits.
Agente de Registro	Responsável pela execução das atividades inerentes à AR. É a pessoa que realiza a autenticação da identidade de um individuo ou de uma organização e validação das solicitações de emissão e revogação de certificados nas Autoridades de Registro.
Agentes Causadores de Eventos	É uma pessoa, organização, dispositivo ou aplicação que causa um evento registrado pelo conjunto de sistemas de auditoria.
Algoritmo	Série de etapas utilizadas para completar uma tarefa, procedimento ou fórmula na solução de um problema. Usado como "chaves" para criptografia de dados.
Algoritmo Assimétrico	É um algoritmo de criptografia que usa duas chaves: uma chave pública e uma chave privada, onde a chave pública pode ser distribuída abertamente enquanto a chave privada é mantida secreta. Os algoritmos assimétricos são capazes de muitas operações, incluindo criptografia, assinaturas digitais e acordo de chave.

PALAVRA CHAVE	DESCRIÇÃO
Algoritmo Criptográfico	Processo matemático especificamente definido para cifrar e decifrar mensagens e informações, normalmente com a utilização de chaves.
Algoritmo Simétrico	Algoritmo de criptografia que usa somente uma chave, tanto para cifrar como para decifrar. Esta chave deve ser mantida secreta para garantir a confidencialidade da mensagem. Também conhecido como algoritmo de chave secreta.
Alvará	Documento eletrônico assinado digitalmente pela Entidade Auditora para uma Autoridade de Carimbo do Tempo, através de um sistema de auditoria e sincronismo. Consiste em um certificado de atributo no qual estarão expressos os dados referentes ao sincronismo e o parecer do auditor sobre a exatidão do relógio da entidade auditada.
Ambiente Físico	É aquele composto por todo ativo permanente das entidades integrantes da ICP-Brasil.
Ambiente Lógico	É aquele composto por todo ativo de informação das entidades integrantes da ICP-Brasil.
Análise de Risco	Identificação e avaliação dos riscos (vulnerabilidades e impactos) a que os ativos da informação estão sujeitos.
Aplicações do Certificado	Os certificados da ICP-Brasil são utilizados, de acordo com o seu tipo, em aplicações como: i. **Tipo A**: confirmação da identidade na *web*, correio eletrônico, transações *on-line*, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos com verificação da integridade de suas informações. ii. **tipo S**: cifração de documentos, bases de dados, mensagens e outras informações eletrônicas.
Applet	*Applet* é um software aplicativo que é executado no contexto de outro programa.
Arquivo dedicado *(Dedicated File – DF)*	Um DF corresponde a um arquivo que contém informações de controle sobre outros arquivos e, opcionalmente, sobre a memória disponível para alocação. Um DF também pode corresponder a um diretório que permite que outros arquivos e/ou diretórios (EF e DF) possam estar contidos, vinculados ou agrupados [ISO/IEC 7816-4].
Arquivo elementar *(Elementary File – EF)*	Um EF corresponde a um conjunto de unidades de dados ou registros que compartilham o mesmo identificador de arquivo. Por exemplo, dados necessários para uma aplicação são armazenados em EF. Um EF não pode ser “pai” (pertencer a um nível hierárquico superior na árvore de arquivos e diretórios) de outro arquivo [ISO/IEC 7816-4].
Arquivo “Pai”	Corresponde ao arquivo dedicado (DF) imediatamente precedente a um dado arquivo dentro da hierarquia [ISO/IEC 7816-4].
Arquivamento de Chave	É o armazenamento da chave privada para seu uso futuro, após o período de

PALAVRA CHAVE	DESCRIÇÃO
privada	validade do certificado correspondente. Só se aplica a chaves privadas de certificados de sigilo. As chaves privadas de assinatura digital só poderão ser utilizadas durante o período de validade dos respectivos certificados, sendo portanto proibido seu armazenamento.
Arquivamento de chave Pública	É o armazenamento da chave pública, por um período mínimo de 30 anos, para uso futuro, após o período de validade do certificado correspondente com o objetivo de verificar as assinaturas geradas durante o prazo de validade dos respectivos certificados. Só se aplica a chaves públicas de certificados de assinatura. As chaves publicas de sigilo só poderão ser utilizadas durante o período de validade dos respectivos certificados, sendo portanto proibido seu armazenamento.
ASN.1	*Abstract Syntax Notation 1* é uma notação formal usada para descrever os dados transmitidos por protocolos de telecomunicações, não obstante a representação física destes dados, o que quer que a aplicação faça, seja complexo ou muito simples.
Assinatura Digital	Código anexado ou logicamente associado a uma mensagem eletrônica que permite de forma única e exclusiva a comprovação da autoria de um determinado conjunto de dados (um arquivo, um *e-mail* ou uma transação). A assinatura digital comprova que a pessoa criou ou concorda com um documento assinado digitalmente, como a assinatura de próprio punho comprova a autoria de um documento escrito. A verificação da origem do dado é feita com a chave pública do remetente.
Ataque	i. Ato de tentar desviar dos controles de segurança de um programa, sistema ou rede de computadores. Um ataque pode ser ativo, tendo por resultado a alteração dos dados; ou passivo, tendo por resultado a liberação dos dados. ii. Tentativa de criptoanálise. O fato de um ataque estar acontecendo não significa necessariamente que ele terá sucesso. O nível de sucesso depende da vulnerabilidade do sistema ou da atividade e da eficácia de contra-medidas existentes.
Ativação de Chave	Método pelo qual a chave criptográfica fica pronta para exercer suas funções. A ativação da chave se dá por meio de um módulo criptográfico, após a identificação dos operadores responsáveis. A identificação pode ocorrer através de uma senha ou outro dispositivo de controle de acesso como um *token, smart card*, biometria.
Ativo de Informação	É o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos de uma organização.
Ativo de Processamento	É patrimônio composto por todos os elementos de *hardware* e *software* necessários para a execução dos sistemas e processos das entidades, tanto os produzidos internamente quanto os adquiridos

PALAVRA CHAVE	DESCRIÇÃO
Atribuição de Chaves *(Key Establishment)*	Processo ou protocolo que possibilita atribuir uma chave criptográfica simétrica compartilhada a parceiros legítimos A atribuição de chaves pode ser realizada por um processo automático (protocolo de negociação de chaves ou protocolo de transporte de chaves), método manual ou uma combinação dos anteriores.
Auditor	Profissional que realiza a avaliação dos controles e processos das entidades auditadas. Deve ser idôneo, dotado de capacidades e conhecimentos técnicos específicos e realizar o seu trabalho com observância de princípios, métodos e técnicas geralmente aceitos. Não deve possuir nenhum dos impedimentos ou suspeições estabelecidos nas normas da ICP-Brasil e no Código de Processo Civil.
Auditor Independente	É aquele auditor que não está vinculado aos quadros do ITI nem da entidade auditada. Trabalha para uma empresa de auditoria independente.
Auditoria	Procedimento utilizado para verificar se todos os controles, equipamentos e dispositivos estão preparados e são adequados às regras, normas, objetivos e funções. Inclui o registro e análise de todas as atividades importantes para detectar vulnerabilidades, determinar se houve violação ou abusos em um sistema de informações com vista a possibilitar ao auditor formar uma opinião e emitir um parecer sobre a matéria analisada.
Auditoria de Conformidade	Avaliação da adequação dos processos, procedimentos e atividades das unidades auditadas com a legislação e os regulamentos aplicáveis. Verificam-se todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo o controle dos processos de solicitação, identificação, autenticação, geração, publicação, distribuição, renovação e revogação de certificados.
Auditoria Independente	Auditoria realizada por Empresa de Auditoria Especializada e Independente.
Auditoria Operacional	Auditoria de conformidade realizada após o processo de credenciamento. Realizada anualmente ou a qualquer momento, se houver suspeitas de irregularidades.
Auditoria Pré-operacional	Auditoria de conformidade realizada antes do processo de credenciamento.
Autenticação	Processo de confirmação da identidade de uma pessoa física (Autenticação de um Individuo) ou jurídica (Autenticação da Identidade de uma Organização) através das documentações apresentadas pelo solicitante e da confirmação dos dados da solicitação. Executado por Agentes de Registro, como parte do processo de aprovação de uma solicitação de certificado digital.
Autenticação do Agente de Registro	Verificação da identidade de um Agente de Registro, em um sistema computadorizado, como um pré-requisito para permitir o acesso aos recursos de um sistema. Na ICP-Brasil a autenticação do Agente deve se dar com o uso de certificado que tenha requisito de segurança, no mínimo, equivalente ao de um certificado A3.
Autenticação e Sincronização de	Atividade periodicamente realizada pela EAT que resulta na habilitação ou não de um SAS ou de um SCT para operar sincronizado com a Hora Legal

PALAVRA CHAVE	DESCRIÇÃO
Relógio (ASR)	Brasileira. Essas operações devem ser efetuadas por intermédio de um conjunto de protocolos que garantam que o resultado final seja isento de fraudes.
Autenticidade	Qualidade de um documento ser o que diz ser, independente de se tratar de minuta, original ou cópia e que é livre de adulterações ou qualquer outro tipo de corrupção.
Auto-assinatura digital	É a assinatura feita usando a chave privada correspondente à chave pública associada ao certificado digital.
Auto-teste	A estratégia de auto-teste foi proposta inicialmente para ser utilizada em classes de sistemas orientados a objetos. Nesta estratégia, é incorporada uma especificação de testes à classe, além do acréscimo de funções BIT (do inglês *Built-in Test*) que criam capacidades de observação e controle do estado da classe. A idéia principal é a incorporação ao componente da capacidade de gerar casos de testes automaticamente, ou da inclusão de casos de teste já prontos. Esses casos de teste podem ser executados pelo cliente ou pelo próprio componente.
Autoridade Certificadora (AC)	É a entidade subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Cabe também à AC emitir listas de certificados revogados (LCR) e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação (DPC). Desempenha como função essencial a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada). Na hierarquia dos Serviços de Certificação Pública, as AC estão subordinadas à Autoridade Certificadora de nível hierarquicamente superior.
Autoridade Certificadora Raiz (AC Raiz)	Primeira AC da cadeia de certificação da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) cujo certificado é auto-assinado, podendo ser verificado através de mecanismos e procedimentos específicos, sem vínculos com este. Executora das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Compete-lhe emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu; gerenciar a lista de certificados emitidos, revogados e vencidos e executar atividades de fiscalização e auditoria das AC, das AR e dos PSS habilitados na ICP-Brasil, em conformidade com as diretrizes e normas técnicas estabelecidas pelo CG da ICP-Brasil e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.
Autoridade de Carimbo de Tempo (ACT)	A autoridade na qual os usuários de serviços de carimbo do tempo (isto é, os subscritores e as terceiras partes) confiam para emitir carimbos do tempo.
Autoridade de Registro (AR)	Entidade responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC que tem por objetivo o recebimento,

PALAVRA CHAVE	DESCRIÇÃO
	validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.
Autoridade Gestora de Políticas da ICP-Brasil	Vide Comitê Gestor da ICP-Brasil
Autorização	Concessão de direito ou permissão que inclui a capacidade de acessar informações e recursos específicos em um sistema computacional ou permissão de acesso a ambientes físicos.
Autorização de Auditoria Independente	Constitui ato declaratório do Diretor de Auditoria, Fiscalização e Normalização do ITI que permite ao Auditor Independente prestar serviços de auditoria, no âmbito da ICP-Brasil, em conformidade com as normas estabelecidas por este Comitê Gestor.
Avaliação de Conformidade	Conjunto de ensaios com o objetivo de verificar se os padrões e especificações técnicas mínimas aplicáveis a um determinado sistema ou equipamento de certificação digital estão atendidos.
Backup	Vide Cópia de Segurança
Banco de dados	Basicamente é um conjunto de informações relacionadas que são reunidas de forma organizada e categorizada, assim como os "arquivos tradicionais em forma de fichas", porém armazenados em meio magnético (disco de computadores) e que são "Gerenciados" por "Sistemas Especializados", ou, os chamados "Sistemas Gerenciadores de Banco de Dados" (ex: *MYSQL, SQL Server, Oracle, DB2, IMS/DLI, ADABAS*, etc.), que permitem armazenagem, atualização e recuperação dessas informações de forma eficiente (fácil, rápida e precisa) independente do volume.
BASE64	É um método para codificação de dados para transferência na internet (*Content Transfer Enconding*).
BER (Basic Encoding Rules)	Regras para codificação de objetos ASN.1 em uma seqüência de *bytes*.
Biometria	Ciência que utiliza propriedades físicas e biológicas únicas e exclusivas para identificar indivíduos. São exemplos de identificação biométrica as impressões digitais, o escaneamento de retina e o reconhecimento de voz.
Bit (Binary digit)	É a menor unidade de informação possível dentro de um computador. Pode assumir os valores de 0 ou 1.
Bloco	Seqüência de bits de comprimento fixo.
Buffer	É uma região de memória temporária utilizada para escrita e leitura de dados. Os dados podem ser originados de dispositivos (ou processos) externos ou internos ao sistema. Os *buffers* podem ser implementados em software (mais usado) ou hardware. Normalmente são utilizados quando existe uma diferença entre a taxa em que os dados são recebidos e a taxa em que eles podem ser

PALAVRA CHAVE	DESCRIÇÃO
	processados, ou no caso em que essas taxas são variáveis.
***Bureau International des Poids et Mesures* (BIPM)**	Organização central do Sistema Internacional de Metrologia localizada na França e responsável pela geração do UTC.
Cache	É um bloco de memória para o armazenamento temporário de dados que possuem uma grande probabilidade de serem utilizados novamente.
Cadastro de Auditoria Independente	Registro cadastral oficial do ITI das empresas de auditoria especializada e independente. Para almejar o cadastro a empresa deverá apresentar ao ITI rol de documentos previstos na resolução 44 do CG da ICP-Brasil. O cadastro terá validade de 5 anos sendo possível renovações.
Cadeia de AC	São as interligações hierárquicas existentes entre as diversas Autoridades Certificadoras participantes da ICP-Brasil.
Cadeia de Certificação	Uma série hierárquica de certificados assinados por sucessivas autoridades certificadoras.
Carimbo de Tempo	Documento eletrônico emitido pela ACT, que serve como evidência de que uma informação digital existia numa determinada data e hora no passado.
Cartão Inteligente	Vide *Smart Card*
Cavalo-de-Tróia	É um programa no qual um código malicioso ou prejudicial está contido dentro de uma programação ou dados aparentemente inofensivos de modo a poder obter o controle e causar danos.
CBC (Cipher Block Chaining)	É um modo de operação de uma cifra de bloco (ver cifra de bloco), em que o texto plano primeiro é submetido a uma operação binária de XOR com o criptograma resultante do bloco anterior. Algum valor conhecido é usado para o primeiro bloco (normalmente chamado de vetor de inicialização**,** esse valor deve ser único para cada mensagem, mas não precisa ser secreto – pode ser enviado junto com o criptograma, para permitir a decifração). O resultado é então cifrado usando a chave simétrica. Assim, blocos de entrada idênticos em texto claro irão produzir criptogramas diferentes.
Certificação de Data e Hora	Vide *Time-stamping*
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.
Certificado de Atributo	Estrutura de dados contendo um conjunto de atributos (características e informações) sobre a entidade final, que é assinada digitalmente com a chave privada da entidade que o emitiu. Pode possuir um período de validade, durante o qual os atributos incluídos no certificado são considerados válidos.
Certificado Auto-	Certificado assinado com a chave privada da própria entidade que o gerou. O

PALAVRA CHAVE	DESCRIÇÃO
assinado	único certificado auto-assinado da ICP-Brasil é o da Autoridade Certificadora Raiz.
Certificado de Calibração	Documento emitido pelo Observatório Nacional atestando que o equipamento usado para emitir carimbos de tempo (SCT) está dentro dos padrões de sincronismo esperados e está apto a entrar em funcionamento.
Certificado de Assinatura Digital (A1, A2, A3 e A4)	São os certificados usados para confirmação da identidade na *web*, correio eletrônico, transações *on-line,* redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos com verificação da integridade de suas informações.
Certificado de Especificações	Documento com as descrições dos requisitos atendidos pelo SCT, no qual o seu fabricante declara responsabilidade sobre estas características. Cada certificado é restrito a um SCT.
Certificado de Sigilo (S1, S2, S3 e S4)	São os certificados usados para cifração de documentos, bases de dados, mensagens e outras informações eletrônicas.
Certificado digital	É um conjunto de dados de computador, gerados por uma Autoridade Certificadora, em observância à Recomendação Internacional ITU-T X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação.
Certificado do Tipo A1 e S1	É o certificado em que a geração das chaves criptográficas é feita por software e seu armazenamento pode ser feito em hardware ou repositório protegido por senha, cifrado por *software.* Sua validade máxima é de um ano, sendo a freqüência de publicação da LCR no máximo de 48 horas e o prazo máximo admitido para conclusão do processo de revogação de 72 horas.
Certificado do Tipo A2 e S2	É o certificado em que a geração das chaves criptográficas é feita em software e as mesmas são armazenadas em Cartão Inteligente ou *Token,* ambos sem capacidade de geração de chave e protegidos por senha. As chaves criptográficas têm no mínimo 1024 bits. A validade máxima do certificado é de dois anos, sendo a freqüência de publicação da LCR no máximo de 36 horas e o prazo máximo admitido para conclusão do processo de revogação de 54 horas.
Certificado do Tipo A3 e S3	É o certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão Inteligente ou *Token*, ambos com capacidade de geração de chaves e protegidos por senha, ou *hardware* criptográfico aprovado pela ICP-Brasil. As chaves criptográficas têm no mínimo 1024 bits. A validade máxima do certificado é de três anos, sendo a freqüência de publicação da LCR no máximo de 24 horas e o prazo máximo admitido para conclusão do processo de revogação de 36 horas.
Certificado do Tipo A4 e S4	É o certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão Inteligente ou *Token*, ambos com capacidade de geração de chaves e protegidos por senha, ou *hardware* criptográfico aprovado pela ICP-Brasil. As chaves criptográficas têm no mínimo 2048 bits. A validade máxima do certificado é de três anos, sendo a freqüência

PALAVRA CHAVE	DESCRIÇÃO
	de publicação da LCR no máximo de 12 horas e o prazo máximo admitido para conclusão do processo de revogação de 18 horas.
Certificado Expirado	Certificado cuja data de validade foi ultrapassada.
Certificado Válido	É um certificado que está dentro do prazo de validade, não tendo sido revogado e sendo possível validar toda a cadeia do certificado até uma AC Raiz aceita pelo usuário que recebe e valida o certificado.
CFB (Ciphertext Feedback)	É um modo de operação para uma cifra de bloco (ver Cifra de Bloco), no qual a saída do sistema é retro-alimentada no mecanismo. Depois que cada bloco é cifrado, parte dele sofre um deslocamento em um registrador. O conteúdo desse registrador é cifrado usando a chave do usuário e a saída sofre uma nova operação binária de XOR com os dados de entrada, para produzir o criptograma. Nesse modo, podemos trabalhar com blocos de mensagens menores do que o tamanho nativo do algoritmo. Dependendo do sistema externo onde está inserido o sistema criptográfico, isso pode trazer vantagens, pois evita a utilização de *buffers* para armazenar temporariamente elementos da mensagem até completar o tamanho de bloco do algoritmo. Efetivamente, o que se irá obter é uma conversão do algoritmo, que opera em forma nativa como cifrador de blocos, em um sistema de cifração seqüencial. Esse método é auto-sincronizável e permite que o usuário decifre apenas uma parte de uma grande base de dados, se começar a partir de uma distância fixa dos dados desejados.
Chave Criptográfica	É o valor numérico ou código usado com um algoritmo criptográfico para transformar, validar, autenticar, cifrar e decifrar dados.
Chave Criptográfica em Texto Claro	Representa uma chave criptográfica não cifrada.
Chave Criptográfica Secreta	Vide Chave Privada e Chave Simétrica
Chave de Sessão	Chave para sistemas criptográficos simétricos. Utilizada pela duração de uma mensagem ou sessão de comunicação. O protocolo SSL (*Secure Sockets Layer)* utiliza as chaves de sessão para manter a segurança das comunicações via internet.
Chave Privada	Uma das chave de um par de chaves criptográficas (a outra é uma chave pública) em um sistema de criptografia assimétrica. É mantida secreta pelo seu dono (detentor de um certificado digital) e usada para criar assinaturas digitais e para decifrar mensagens ou arquivos cifrados com a chave pública correspondente.
Chave Pública	Uma das chaves de um par de chaves criptográficas (a outra é uma chave privada) em um sistema de criptografia assimétrica. É divulgada pelo seu dono e usada para verificar a assinatura digital criada com a chave privada correspondente. Dependendo do algoritmo, a chave pública também é usada para cifrar mensagens ou arquivos que possam, então, ser decifrados com a chave privada correspondente.

PALAVRA CHAVE	DESCRIÇÃO
Chave Simétrica	Chave criptográfica gerada por um algoritmo simétrico (Ver Algoritmo Simétrico).
Chaves Assimétricas	Chaves criptográficas geradas por um algoritmo assimétrico (Ver Algoritmo Assimétrico).
Ciclo de Vida do Certificado	Período de tempo que se inicia com a solicitação do certificado e termina com sua expiração ou revogação.
Cifra de Bloco	Algoritmo criptográfico simétrico, no qual a mensagem é dividida em blocos e cada bloco é cifrado separadamente.
Cifrar	i. É o processo de transformação de dados ou informação para uma forma ininteligível usando um algoritmo criptográfico e uma chave criptográfica. Os dados não podem ser recuperados sem usar o processo inverso de decifração. ii. Processo de conversação de dados em "código ilegível" de forma a impedir que pessoas não autorizadas tenham acesso à informação.
Classificação da Informação	Ato ou efeito de analisar e identificar o conteúdo de documentos, atribuindo um grau de sigilo que define as condições de acesso aos mesmos, conforme normas e legislação em vigor.
CMM-SEI (Capability Maturity Model do Software Engineering Institute)	Modelo para avaliação da maturidade dos processos de software de uma organização e para identificação das práticas-chave que são requeridas para aumentar a maturidade desses processos. O CMM prevê cinco níveis de maturidade: inicial, repetível, definido, gerenciado e otimizado. O modelo foi proposto por Watts S. Humphrey, a partir das propostas de Philip B. Crosby, e vem sendo aperfeiçoado pelo *Software Engineering Institute* - SEI da Carnegie Mellon University.
CMPV (Cryptographic Module Validation Program)	Programa de testes para módulos criptográficos criado pelo *NIST (National Institute of Standards and Technology*, do governo dos Estados Unidos, e pelo CSE (*Communications Security Establishment*) do governo do Canadá, em 1995. Utiliza-se de laboratórios independentes credenciados. Fabricantes interessados nos testes de validação podem selecionar qualquer um dos laboratórios credenciados. Para as validações, são utilizados os requisitos definidos no padrão FIPS 140-2.
CN (Common Name)	Atributo especificado dentro do campo Assunto - Nome Distinto (*Distinguished Name*) - de um certificado. Por exemplo, para certificados de servidor o nome do *"host"* DNS do site a ser certificado; para um Certificado de Assinatura de Software, o nome comum é o nome da organização e em certificados de assinante, o nome comum é normalmente composto pelo prenome e sobrenome do titular.
Co-assinatura	A co-assinatura (*co-sign)* é aquela gerada independente das outras assinaturas.
Código de Autenticação	Corresponde a um verificador criptográfico de integridade e autenticidade que é comumente referenciado como MAC (*Message Authentication Code*).

PALAVRA CHAVE	DESCRIÇÃO
Comitê Gestor da ICP-Brasil	Autoridade gestora de políticas da ICP-Brasil que tem suas competências definidas na Medida Provisória 2.200-2. É responsável, dentre outras coisas, por estabelecer a política e as normas de certificação, fiscaliza a atuação da Autoridade Certificadora Raiz, cuja atividade é exercida pelo Instituto Nacional de Tecnologia da Informação.
Commom Criteria (CC)	É um padrão internacional (ISO/IEC 15408) para a segurança do computador. CC fornece a garantia que o processo da especificação, da execução e da avaliação de um produto de segurança do computador foi conduzido de modo rigoroso e padronizado.
Compensação (*Offset*)	Correção necessária no relógio local para fazer com que indique o mesmo tempo indicado pelo relógio de referência.
Comprometimento	Violação concreta ou suspeita de violação de uma política de segurança de um sistema, onde possa ter ocorrido divulgação não autorizada ou perda do controle sobre informações sigilosas.
Confiança	É a suposição de que uma entidade se comportará substancialmente como esperado no desempenho de uma função específica.
Confidencial	Tipo de classificação de informação, que se for divulgada ou usada sem autorização, trará sérios prejuízos para uma organização.
Confidencialidade	Propriedade de certos dados ou informações que não podem ser disponibilizadas ou divulgadas sem autorização para pessoas, entidades ou processos. Assegurar a confidencialidade de documentos é assegurar que apenas pessoas autorizadas tenham acesso à informação.
Confirmação da Identidade	Vide Autenticação da Identidade
Consulta *On-line* de Situação do Certificado	Vide OCSP
Conta	Permissão para acesso a um serviço. A permissão é obtida após o registro de dados específicos do usuário, no servidor, que definem o ambiente de trabalho desse usuário. O registro pode incluir configurações de tela, configurações de aplicativos e conexões de rede. O que o usuário vê na tela, além de quais arquivos, aplicativos e diretórios ele tem acesso é determinado pela maneira com que foi configurada a conta do usuário.
Contexto Seguro de Execução	Estrutura de dados existente durante a execução da biblioteca criptográfica onde as chaves criptográficas estão protegidas contra divulgação, modificação e substituição não autorizada.
Contingência	Situação excepcional decorrente de um desastre.
Contra-assinatura	A contra-assinatura (*countersign*) é aquela realizada sobre uma assinatura já existente. Na especificação CMS a contra-assinatura é adicionada na forma de um atributo não autenticado (*countersignature attribute*) no bloco de informações (*signerInfo)* relacionado à assinatura já existente.

PALAVRA CHAVE	DESCRIÇÃO
Controle “n de m”	Forma de controle múltiplo onde “n” pessoas de um grupo de “m”, são requeridas para utilização de uma chave privada.
Controle de Acesso	i. Conjunto de componentes dedicados a proteger a rede, aplicações *Web* e instalações físicas de uma AC contra o acesso não autorizado, permitindo que somente organizações ou indivíduos previamente identificados e autorizados possam utilizá-las. ii. Restrições ao acesso às informações de um sistema, exercidas pela gerência de segurança da entidade detentora daquele sistema.
Controles	i. Procedimentos usados para controlar o sistema de tal maneira que ele esteja de acordo com critérios especificados. ii. Qualquer ação, procedimento, técnica ou qualquer outra medida que reduza a vulnerabilidade de uma ameaça a um sistema.
Cópia de Segurança	São as cópias feitas de um arquivo ou de um documento que deverão ser guardadas sob condições especiais para a preservação de sua integridade no que diz respeito tanto à forma quanto ao conteúdo, de maneira a permitir o resgate de programas ou informações importantes em caso de falha ou perda dos originais.
COTEC	O Comitê Técnico - COTEC - presta suporte técnico e assistência ao Comitê Gestor da ICP-Brasil, sendo responsável por manifestar previamente sobre as matérias apreciadas e decididas pelo comitê Gestor.
Credenciamento	Entende-se como o processo em que o ITI avalia e aprova os documentos legais, técnicos, as práticas e os procedimentos das entidades que desejam ingressar na ICP-Brasil. Aplica-se a Autoridades Certificadoras, Autoridades de Registro e Prestadores de Serviços de Suporte. Quando aprovados, os credenciamentos são publicados no Diário Oficial da União.
CryptoAPI	*Cryptographic Application Programming Interface* (também conhecida como *CryptoAPI, Microsoft Cryptography API*, ou simplesmente *CAPI*) é uma interface de programação para aplicações incluída com o sistema operacional *Microsoft Windows* que provê serviços para habilitar desenvolvedores para aplicações de segurança baseadas em *Windows* usando criptografia. É um conjunto de bibliotecas dinamicamente ligadas que provê um nível de abstração que isola programadores do código usado para cifrar dados.
Criptografar	Ver Cifrar
Criptografia	i. Disciplina de criptologia que trata dos princípios, dos meios e dos métodos de transformação de documentos com o objetivo de mascarar seu conteúdo, impedir modificações, uso não autorizado e dar segurança à confidência e autenticação de dados. ii. Ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, através de um processo de cifragem, e para restaurar informações cifradas para sua forma original, inteligível, através de um processo de decifragem. A criptografia também se preocupa com as técnicas de criptoanálise, que dizem respeito à formas de recuperar aquela informação sem se ter os parâmetros completos para a decifragem.

PALAVRA CHAVE	DESCRIÇÃO
Criptografia Assimétrica	É um tipo de criptografia que usa um par de chaves criptográficas distintas (privada e pública) e matematicamente relacionadas. A chave pública está disponível para todos que queiram cifrar informações para o dono da chave privada ou para verificação de uma assinatura digital criada com a chave privada correspondente; a chave privada é mantida em segredo pelo seu dono e pode decifrar informações ou gerar assinaturas digitais.
Criptografia de Chaves Públicas	Ver Criptografia Assimétrica
CSP (Cryptographic Service Provider)	É uma biblioteca de software que implementa a *Cryptographic Application Programming Interface (CAPI)*. CSP's implementam funções de codificação e decodificação, que os programas de aplicação de computador podem usar para, por exemplo, autenticação segura de usuário ou para o email seguro. CSP's são executados basicamente como um tipo especial de DLL com limitações especiais no carregamento e no uso.
Curvas Elípticas	A criptografia de curvas elípticas (ECC) é uma abordagem de criptografia de chave pública baseada na estrutura algébrica de curvas algébricas de campos finitos. As curvas elípticas são usadas também em diversos algoritmos do fatoração de inteiro que tem aplicações em criptografia.
Custódia	Consiste na responsabilidade jurídica de guarda e proteção de um ativo, independente de vínculo de propriedade. A custódia, entretanto, não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros.
Dados	Informações representadas em forma digital, incluindo voz, texto, *fac-símile*, imagens e vídeo.
Dados de Ativação	Valores de dados, que não sejam chaves criptográficas, necessários para operar módulos criptográficos e que necessitam ser protegidos (ex.: PIN, *passphrase* ou uma chave compartilhada manualmente).
Data de validade do Certificado	A hora e a data de quando termina o período operacional de um certificado digital. Não tem relação com a revogação antes da hora e data anteriormente prevista.
Datação de Registros	É o serviço de certificação da hora e do dia em que foi assinado um documento eletrônico, com identidade do autor.
Decifrar	Processo que transforma dados previamente cifrados e ininteligíveis de volta à sua forma legível.
Declaração das Práticas de Carimbo de Tempo (DPCT)	Declaração das práticas e dos procedimentos empregados pela ACT para emi-tir Carimbos do Tempo.
Declaração de Praticas de Certificação (DPC)	Documento, periodicamente revisado e republicado, que descreve as práticas e os procedimentos empregados pela Autoridade Certificadora na execução de seus serviços. É a declaração a respeito dos detalhes do sistema de credenciamento, as práticas, atividades e políticas que fundamentam a emissão de certificados e outros serviços relacionados. É utilizado pelas

PALAVRA CHAVE	DESCRIÇÃO
	Autoridades Certificadoras para garantir a emissão correta dos certificados e pelos solicitantes e partes confiantes para avaliar a adequação dos padrões de segurança empregados às necessidades de segurança de suas aplicações.
Decriptografar	Ver Decifrar
DER (Distinguished Encoding Rules)	Regras para codificação de objetos ASN.1 em uma seqüência de *bytes*. Corresponde a um caso especial de BER.
DES (Data Encryption Standard)	Algoritmo simétrico de criptografia de dados que utiliza um sistema de cifragem em blocos. Foi criado pela IBM em 1977 e apesar de permitir cerca de 72 quadrilhões de combinações (2^{56}), seu tamanho de chave (56 bits) é considerado pequeno, tendo sido quebrado por "força bruta" em 1997 em um desafio lançado na internet. Está definido no documento de padronização FIPS 46-1.
Desastre	i. É um evento súbito e inesperado cujo impacto resulta em perdas significativas para a organização. ii. Uma circunstância em que um negócio é julgado incapaz de funcionar em conseqüência de alguma ocorrência natural ou criada.
Desativação de Chave	Contrário de ativação de chave (ver Ativação de Chave).
Destruição de Chave	Refere-se à destruição física da mídia armazenadora e/ou lógica (sobrescrever os espaços onde a chave estiver armazenada) da chave criptográfica.
Diffie-Hellman	*Diffie-Hellman* é um método de criptografia desenvolvido por Whitfield Diffie e Martin Hellman e publicado em 1976. O algoritmo *Diffie-Hellman* permite que haja a troca de chaves públicas entre duas ou mais partes, permitindo que as pessoas que recebem a chave pública usem essa chave para cifrar o conteúdo de uma mensagem que será enviada à parte que forneceu a chave pública. Esse texto cifrado não poderá ser aberto por indivíduos que possuam a chave pública e sim, apenas pela parte que enviou a chave pública, pois a mesma possui a chave privada que se encontra em seu poder. Tendo posse dessa chave a mensagem cifrada poderá ser aberta.
Direito de Acesso	É o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo.
Diretório	Unidade lógica de armazenamento que permite agrupar arquivos em pastas hierárquicas e subpastas.
Disponibilidade	É a razão entre o tempo durante o qual o sistema está acessível e operacional e o tempo decorrido. No âmbito da ICP-Brasil a disponibilidade das informações publicadas pelas AC em serviço de diretório ou página *web* deve ser de 99% do mês, 24 horas por dia e 7 dias por semana.
DMZ (Demilitarized Zone)	Uma área na rede de uma empresa que é acessível à rede pública (internet), mas não faz parte da sua rede interna. Geralmente, esses servidores possuem números de IP acessíveis pela rede externa, o que os torna alvos de ataques. Para assegurar que os riscos são minimizados, um sistema de detecção e

PALAVRA CHAVE	DESCRIÇÃO
	prevenção de intrusos deve ser implementado nessa DMZ.
DN (Distinguished Name)	Conjunto de dados que identifica de modo inequívoco uma entidade ou indivíduo pertencente ao mundo físico no mundo digital (por exemplo: país=BR, estado=Rio de Janeiro, nome organizacional=Sua Empresa S.A., nome comum=José da Silva).
DNS (Domain Name Service)	É um serviço e protocolo da família TCP/IP para o armazenamento e consulta às informações sobre recursos da rede. A implementação é distribuída entre diferentes servidores e trata principalmente da conversão de nomes internet em seus números IP correspondentes.
Documentação técnica	Conjunto de documentos técnicos que acompanham o objeto de homologação e que a parte interessada deve depositar no LSITEC-LEA para servir ao processo de homologação. A documentação técnica deve apresentar uma descrição técnica sobre o objeto de homologação que satisfaça aos requisitos definidos no MCT.
Documento	Unidade de registro de informações, qualquer que seja o suporte.
Documento digital	Unidade de registro de informações, codificada por meio de dígitos binários.
Documento Eletrônico	Unidade de registro de informações, acessível por meio de um equipamento eletrônico.
Drift	Variação no *skew* (segunda derivada do *offset*) apresentada por alguns relógios.
DSA (Digital Signature Algarithm)	Algoritmo unicamente destinado a assinaturas digitais, foi proposto pelo NIST em agosto de 1991, para utilização no seu padrão DSS (*Digital Signature Standard)*. Adotado como padrão final em dezembro de 1994, trata de uma variação dos algoritmos de assinatura ElGamal e Schnorr. Foi inventado pela NSA e patenteado pelo governo americano.
ECB (Electronic Code Book)	É um modo de operação de uma cifra de bloco (ver cifra de bloco), com a característica que cada bloco possível de “texto claro” tem um valor correspondente definido da mensagem cifrada e vice-versa. Ou seja o mesmo valor de “texto claro” resultará sempre no mesmo valor da mensagem cifrada. ECB é usado quando um volume de “texto claro” é dividido em diversos blocos dos dados, onde cada um é então cifrado independentemente de outros blocos. De fato, ECB tem a capacidade de suportar uma chave separada de cifração para cada tipo do bloco.
e-PING	Padrões de Interoperabilidade de Governo Eletrônico: define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de Serviços de Governo Eletrônico, estabelecendo as condições de interação com os demais poderes e esferas de governo e com a sociedade em geral. As áreas cobertas pela e-PING, estão segmentadas em: " Interconexão; " Segurança; " Meios de Acesso; " Organização e Intercâmbio de Informações; " Áreas e Assuntos de Integração para Governo Eletrônico.
Elemento de Dado	No contexto da norma ISO/IEC 7816-4 referente ao cartão inteligente, um

PALAVRA CHAVE	DESCRIÇÃO
	elemento de dado corresponde a um item de informação para o qual é associado um nome, uma descrição de conteúdo lógico, um formato e uma codificação [ISO/IEC 7816-4].
Emitir Certificado Digital	É a atividade de geração de um Certificado Digital, a inclusão neste dos dados de identificação do seu emissor (Autoridade Certificadora), do titular e da sua assinatura digital e subseqüente notificação ao seu solicitante, observados os dispostos nos documentos públicos das AC denominados Práticas de Certificação - PC e Declaração de Práticas de Certificação – DPC.
Empresa de Auditoria Especializada e Independente	Vide Empresa de Auditoria Independente
Empresa de Auditoria Independente	São empresas de Auditoria Independentes, autorizadas pelo ITI para atuar na ICP-Brasil e que podem ser contratadas pelas autoridades certificadoras para realizar auditorias operacionais em entidades a elas subordinadas.
Encadeamento	Ato de associar um carimbo de tempo a outro.
Encriptar	Ver Cifrar
Engenharia Social	É o termo utilizado para a obtenção de informações importantes de uma organização, através de seus usuários e colaboradores, ou de uma pessoa física. Essas informações podem ser obtidas pela ingenuidade ou confiança. Os ataques desta natureza podem ser realizados através de telefonemas, envio de mensagens por correio eletrônico, salas de bate-papo e até mesmo pessoalmente.
Ensaio	Procedimento técnico realizado em conformidade com as normas aplicáveis, que objetiva analisar um ou mais requisitos técnicos de um dado sistema ou equipamento.
Entidade de Auditoria de Tempo (EAT)	Entidade que realiza as atividades de autenticação e sincronismo de Servidores de Carimbo do Tempo (SCT), instalados nas ACT. Na estrutura de carimbo do tempo da ICP-Brasil, a EAT é o próprio Observatório Nacional.
Entidades Operacionalmente Vinculadas	Entidade relacionada a outra: i. como matriz, subsidiária, sócia, *joint-venture,* contratada ou agente, ii. como membro de uma comunidade de interesses registrada, ou iii. como entidade que mantém relacionamento com uma entidade principal, que mantém negócios ou registros capazes de fornecer comprovação adequada da identidade da afiliada. No caso da ICP-Brasil, diz-se que uma AR ou PSS está operacionalmente vinculada a uma AC, por exemplo.
Entidade Usuária Externa	Um indivíduo ou processo que realiza acesso a um módulo criptográfico independentemente do papel assumido.
Enveloped Data	Consiste em conteúdo cifrado de todos os tipos e chaves cifradas de sessão do tipo *"content-encryption"* para um ou mais recipientes. As mensagens *"enveloped"* mantêm os conteúdos do segredo da mensagem e reservam-nos

PALAVRA CHAVE	DESCRIÇÃO
	somente a pessoas ou entidades para recuperar os conteúdos. *Cryptographic message syntax (CMS)* pode ser usado para codificar mensagens *"enveloped".*
Equipamento de Certificação Digital	Todo e qualquer aparelho, dispositivo ou elemento físico que compõe meio necessário ou suficiente à realização de Certificação Digital
Erro	Diferença de tempo medida pelo Observatório Nacional entre o SAS e o SCT da ACT.
Erro Máximo Acumulado	Erro máximo que pode ser acumulado pelo relógio interno do SCT, entre duas ASR.
Estabilidade	Capacidade de um oscilador em manter a mesma freqüência em um determinado intervalo de tempo.
***Escrow* de Chave Privada**	Vide Recuperação de Chave
Evento	São ocorrências de significância, eletrônicas ou manuais, que devem ser registradas para análises e auditorias posteriores. Na ICP-Brasil, há diversos tipos de eventos que devem obrigatoriamente ser registrados, como: iniciação e desligamento do sistema de certificação; tentativas de criar, remover, definir senhas ou mudar os privilégios de sistema dos operadores da AC etc.
Exatidão	Afastamento máximo tolerado entre o valor indicado por um sistema de medição e o valor verdadeiro do tempo.
Expoente Privado	Representa o expoente na definição de chave privada: par (d, n) onde "d" é o expoente privado e "n" é o módulo público (produto de dois fatores primos privados).
Expoente Público	Representa o expoente na definição de chave pública: par (e, n) onde "e" é o expoente público e "n" é o módulo público (produto de dois fatores primos privados).
Exportação de certificado digital	É a atividade de copiar um Certificado Digital instalado em determinado computador ou hardware, para um disquete, CD, etc, permitindo a sua instalação em outro(s) computador(es) ou hardware.
Exportação de chaves criptográficas	Processo de retirada de chave criptográfica do módulo criptográfico. A exportação pode ser realizada de forma manual ou automática.
Exportação de chaves criptográficas de forma automática	Processo de retirada de chave criptográfica de um módulo criptográfico que utiliza uma mídia eletrônica ou meio de comunicação eletrônico.
Exportação de chaves criptográficas de forma manual	Processo de retirada de chave criptográfica do módulo criptográfico que utiliza métodos manuais. Ex: apresentação do valor da chave um *display.*
***FIPS (Federal Information Processing Standards*)**	Correspondem aos padrões e diretrizes desenvolvidos e publicados pelo NIST (*National Institute of Standards and Technology*) para uso de sistemas computacionais no âmbito governamental federal norte-americano. O NIST

PALAVRA CHAVE	DESCRIÇÃO
	desenvolve os padrões e diretrizes FIPS quando há requisitos obrigatórios do governo federal, tais como, segurança e interoperabilidade e não há padrões ou soluções industriais aceitáveis.
FIPS 140 Federal Information Processing Standards)	O *Federal Information Processing Standards* 140 é um padrão do governo dos Estados Unidos para implementações de módulos de criptografia - ou seja, hardware e software para cifrar e decifrar dados ou realizar outras operações criptográficas (como geração ou verificação de assinaturas digitais). Encontra-se atualmente na versão 2, estando em elaboração, pelo NIST, a versão 3.
Firewall	É um conjunto formado por Hardware, Software e uma política de acesso instalado entre redes, com o propósito de segurança. A função do *firewall* é controlar o tráfego entre duas ou mais redes, com o objetivo de fornecer segurança, prevenir ou reduzir ataques ou invasões às bases de dados corporativas, a uma (ou algumas) das redes, que normalmente têm informações e recursos que não devem estar disponíveis aos usuários da(s) outra(s) rede(s).
Firmware	Programas e componentes de dados de um módulo que estão armazenados em uma porção de hardware (ROM, PROM, EPROM, EEPROM ou FLASH, por exemplo) que não podem ser dinamicamente escritos ou modificados durante a execução.
Fonte Confiável de Tempo (FCT)	É a denominação dada ao Relógio Atômico localizado no Observatório Nacional.
Fronteira criptográfica (*Cryptographic Boundary*)	A fronteira criptográfica é um perímetro explicitamente definido que estabelece os limites físicos de um módulo criptográfico.
Geração de Par de Chaves	Processo de criação de um par de chaves (chave privada e chave pública), sendo normalmente executado na solicitação de um certificado digital.
Gerador de Números Aleatórios	Vide *RNG*
Gerador de Números Pseudo-aleatórios	Vide *PRNG*
Gerenciamento de Certificado	É a forma como uma AC, baseada em suas DPC, PC e PS, atua na emissão, renovação e revogação de certificados, bem como na emissão e publicação da sua LCR.
Gerenciamento de Risco	Processo que visa a proteção dos ativos das entidades integrantes da ICP-Brasil, por meio da eliminação, redução ou transferência dos riscos, conforme seja econômica e estrategicamente mais viável.
Hacker	Pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros.
Handle	i. Um dispositivo, unido a um objeto, que seja anexado para mover ou usar o

PALAVRA CHAVE	DESCRIÇÃO
	objeto. ii. um tipo do ponteiro inteligente, uma referência a uma posição na memória de computador.
Hardware	i. Conjunto dos componentes físicos necessários à operação de um sistema computacional. ii. Equipamento mecânico e eletrônico, combinado com *software* (programas, instruções, etc.) na implementação de um sistema de processamento de informações eletrônicas.
Hardware Secure Module (HSM)	É um dispositivo baseado em *hardware* que gera, guarda e protege chaves criptográficas, além de ter a capacidade de executar operações criptográficas, como assinatura digital.
Hash	É o resultado da ação de algoritmos que fazem o mapeamento de uma seqüência de bits de tamanho arbitrário para uma seqüência de bits de tamanho fixo menor - conhecido como resultado *hash* - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado *hash* (resistência à colisão) e que o processo reverso também não seja realizável (dado um *hash*, não é possível recuperar a mensagem que o gerou).
Hibernação	Um mode de *"power-saving"* que conserve a bateria do computador, mas permite uma reativação mais rápida da operação do que desligando o computador e então voltando a ligá-lo. Quando o modo de hibernação é ativado, todas as aplicações atuais que estão na memória estão conservadas no disco e o computador é desligado. Ao retomar a operação, pressionando uma tecla ou clicando o *mouse*, as aplicações são lidas do disco e voltam ao mesmo estado anterior.
Hierarquia do Certificado	Uma estrutura de certificados digitais que permite a indivíduos verificarem a validade de um certificado. O certificado é emitido e assinado por uma Autoridade Certificadora que está numa posição superior na hierarquia dos certificados. A validade de um certificado específico é determinada, entre outras coisas, pela validade correspondente ao certificado da AC que fez a assinatura.
Homologação	Processo que consiste no conjunto de atos, realizados de acordo com um Regulamento e com as demais normas editadas ou adotadas pela ICP-Brasil, que, se plenamente atendido, resultará na expedição de ato pelo qual, na forma e nas hipóteses previstas, a entidade responsável pela condução do referido processo reconhecerá o laudo de conformidade.
HSM (Hardware Security Modules)	Vide Módulo de Segurança Criptográfica
IDEA (International Data Encryption Algorithm)	Algoritmo criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM Systec. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Mas, na maioria dos microprocessadores, uma implementação por soft*ware* do IDEA é mais rápida do que uma implementação por *software* do DES. O IDEA é o programa para criptografia de *e-mail* pessoal mais disseminado no mundo. Seu tamanho de chave é de 128 bits.

PALAVRA CHAVE	DESCRIÇÃO
Identificação	Vide Autenticação
Identificador de Registro	Valor associado a um registro que pode ser usado para referenciar aquele registro. Diversos registros poderiam ter o mesmo identificador dentro de um EF [ISO/IEC 7816-4].
Importação de Certificado Digital	É a atividade de copiar um Certificado Digital a partir de um disquete, CD, *smart card,* para um computador ou hardware, permitindo a sua instalação e uso posterior, por exemplo, para assinatura digital de *e-mails.*
Importação de chaves criptográficas	Processo de inserção de chave criptográfica no módulo criptográfico. A importação pode ser realizada de forma manual ou automática.
Importação de chaves criptográficas de forma automática	Processo de inserção de chave criptográfica de um módulo criptográfico que utiliza uma mídia eletrônica ou meio de comunicação eletrônico.
Importação de chaves criptográficas de forma manual	Processo de inserção de chave criptográfica de um módulo criptográfico que utiliza métodos manuais. Ex: digitação em um teclado, por uma entidade usuária externa, do valor da chave.
Incerteza	Dispersão dos valores que podem ser atribuídos a um mensurando, como resultado de uma sincronização.
Incidente de Segurança	É qualquer evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo das entidades integrantes da ICP-Brasil.
Infra-estrutura de chaves públicas brasileira (ICP-Brasil)	É um conjunto de técnicas, arquitetura, organização, práticas e procedimentos, implementados pelas organizações governamentais e privadas brasileiras que suportam, em conjunto, a implementação e a operação de um sistema de certificação. Tem como objetivo estabelecer os fundamentos técnicos e metodológicos de uma sistema de certificação digital baseado em criptografia de chave pública, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. A ICP-Brasil foi criada pela Medida Provisória 2200-2, de 24.08.2001 e está regulamentada pelas Resoluções do Comitê-Gestor da ICP-Brasil, disponíveis no sítio www.iti.gov.br.
Instituto Nacional de Tecnologia da Informação (ITI)	É uma autarquia federal vinculada à Casa Civil da Presidência da República, é a Autoridade Certificadora Raiz da ICP-Brasil. É a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.
Integridade	Garantia oferecida ao usuário de que documento eletrônico, mensagem ou conjunto de dados não foi alterada, nem intencionalmente, nem acidentalmente por pessoas não autorizadas durante sua transferência entre sistemas ou computadores.
Interface	Representa um ponto lógico de entrada e saída de dados, que provê acesso

PALAVRA CHAVE	DESCRIÇÃO
	aos serviços disponíveis pelos softwares.
Intimação	Ato pelo qual se dá conhecimento do procedimento de fiscalização para que a entidade fiscalizada faça ou deixe de fazer alguma coisa.
Irretratabilidade	Consiste basicamente em um mecanismo para garantir que o emissor da mensagem ou participante de um processo não negue posteriormente a autoria.
ISO (International Standards Organization)	É a organização que cria padrões internacionais para diversas áreas, incluindo computadores. Congrega em torno de 90 países.
ITU (International Telecommunication Union)	É uma organização internacional que faz parte do Sistema das Nações Unidas. Responsável pelo estabelecimento de normas e padrões em telecomunicações e seus serviços.
Key Containers	Uma parte do *key database* (banco de dados que contém as chaves criptográficas para um *CSP* específico) que contém todos os pares de chaves (pares de chaves para troca e assinatura) que pertencem a um usuário específico. Cada recipiente tem um nome único que é usado ao chamar funções de contexto para obter um *handle* ao *container*.
Key Zeroization	Um método de apagar chaves criptográficas armazenadas eletronicamente, alterando ou suprimindo os índices de armazenamento das chaves para impedir a recuperação das informações.
Laboratório de Ensaio e Auditoria (LEA)	São entidades, formalmente vinculadas ao ITI, aptas a realizar os ensaios exigidos nas avaliações de conformidade e a emitir os correspondentes laudos de conformidade, na forma prevista na resolução nº 36 do CG da ICP-Brasil, que embasarão a tomada de decisão por parte do ITI quanto à homologação ou não de um dado sistema ou equipamento avaliado.
Laudo de Conformidade	Documento emitido ao final da avaliação de conformidade, na forma prevista na resolução nº 36 do CG da ICP-Brasil , que atestará se um dado sistema ou equipamento, devidamente identificado, está ou não em conformidade com as normas editadas ou adotadas pela ICP-Brasil.
Leap second	Segundo adicionado ao UTC para compensar o atraso da rotação da Terra e manter o UTC em sincronismo com o tempo solar.
Leitora de Cartão Inteligente	Hardware instalado no computador, utilizando de interface serial ou usb, que serve para efetuar leituras de *smart cards.*
Lista de Certificados Revogados (LCR)	Lista assinada digitalmente por uma Autoridade Certificadora, publicada periodicamente, contendo certificados que foram revogados antes de suas respectivas datas de expiração. A lista, geralmente, indica o nome de quem a emite, a data de emissão e a data da próxima emissão programada, além dos números de série dos certificados revogados e a data da revogação.
Lista de Controle de Acesso	Lista de indivíduos ou entidades com permissão de acesso a certas áreas específicas de um servidor, rede, aplicação de internet ou instalações físicas.
Log	Conjunto de registros que lista as atividades realizadas por uma máquina ou

PALAVRA CHAVE	DESCRIÇÃO
	usuário específico. Um único registro é conhecido como 'registro de log'. Em termos de segurança, os *logs* são usados para identificar e investigar as atividades suspeitas e estudar as tentativas (ou os sucessos) dos ataques, para conhecimento dos mecanismos usados e aprimoramento do nível de eficiência da segurança.
Login	É o processo de identificação e autenticação ao qual o usuário é submetido antes de integrar ao sistema, software ou aplicativo.
Logoff	É o processo de encerramento da sessão de trabalho pelo usuário.
MAC (Message Authentication Code)	É uma pequena parte de informação usada para autenticar uma mensagem. Um algoritmo MAC aceita como entrada uma chave secreta e uma mensagem de comprimento indefinido para ser autenticado e envia como saída um MAC (conhecido às vezes como *tag)*. O valor do MAC protege a integridade de uma mensagem assim como sua autenticidade, permitindo que os verificadores (quem possuem também a chave secreta) detectem todas as mudanças no conteúdo da mensagem.
MD5 *(Message Digest 5)*	É uma função de *hash* - espalhamento unidirecional - inventada por Ron Rivest. Este algoritmo produz um valor *hash* de 128 bits, para uma mensagem de entrada de tamanho arbitrário. Foi inicialmente proposto em 1991, após alguns ataques de criptoanálise terem sido descobertos contra a função *hashing* prévia: a MD4. O algoritmo foi projetado para ser rápido, simples e seguro. Seus detalhes são públicos e têm sido analisados pela comunidade de criptografia. Foi descoberta uma fraqueza em parte do MD5, mas até agora ela não afetou a segurança global do algoritmo. Entretanto, o fato dele produzir uma valor *hash* de somente 128 bits é o que causa maior preocupação.
Mídia	Base física (*hardware*) ou lógica (*software*) sobre a qual a informação é registrada, podendo ser exportada para outra mídia ou permanecer armazenada nela própria.
Mídia Armazenadora	Vide Mídia.
MIME (Multipurpose Internet Mail Extensions)	É um padrão da internet que estende o formato de *e-mail* para suportar: texto em conjunto de caracteres além do tipo *US-ASCII*; anexos do tipo *não-texto*; corpos de mensagem do tipo *multi-part* e informação de cabeçalho em conjunto de caracteres do tipo *não-ASCII.* Os tipos de conteúdo definidos por padrões MIME são também de importância além do *e-mail*, como em protocolos de comunicação como o HTTP para a internet.
Mitigação	Os esforços da mitigação tentam impedir que perigos se tornem desastres completamente, ou reduzem os efeitos dos desastres quando ocorrem. A mitigação focaliza em medidas a longo prazo para se reduzir ou eliminar riscos. A implementação de estratégias de mitigação pode ser considerada uma parte do processo da recuperação se aplicado após a ocorrência de um desastre.
Módulo Criptográfico	Software ou hardware que fornece serviços criptográficos, como cifração,

PALAVRA CHAVE	DESCRIÇÃO
	decifração, geração de chaves, geração de números aleatórios.
Módulo criptográfico mono-CI	Módulo criptográfico com um único circuito integrado protegido por um invólucro.
Módulo criptográfico multi-CI	Módulo criptográfico com vários circuitos integrados protegidos por um invólucro.
Módulo criptográfico multiaplicação	Faz referência a um módulo criptográfico que suporta mais que uma aplicação. Exemplo: módulo criptográfico contendo aplicação ICP e aplicação EMV.
Módulo de Segurança Criptográfica (MSC)	É um *hardware* com capacidade de processamento, que gera chaves criptográficas e assina documentos, sendo usado para para assinar os certificados digitais em Autoridades Certificadoras, oferecendo grande velocidade e segurança.
Multi-threaded	Característica dos sistemas operativos modernos que permite repartir a utilização do processador entre várias tarefas simultaneamente.
Não-repúdio	Não-Repúdio, ou não recusa, é a garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica, não poderá posteriormente negar sua autoria, visto que somente aquela chave privada poderia ter gerado aquela assinatura digital. Deste modo, a menos de um uso indevido do certificado digital, fato que não exime de responsabilidade, o autor não pode negar a autoria da transação. Transações digitais estão sujeitas a fraude, quando sistemas de computador são acessados indevidamente ou infectados por cavalos-de-tróia ou vírus. Assim os participantes podem, potencialmente, alegar fraude para repudiar uma transação.
Navegador de internet ou *Browser*	Aplicativo utilizado para visualizar arquivos HTML, VRML, textos, arquivos de áudio, animação, videoclipes e/ou correio eletrônico pela internet. Entre os principais navegadores disponíveis no mercado estão: Microsoft Internet Explorer, Netscape Navigator, Opera, Mozilla, etc.
NBR (Norma Brasileira Regulamentadora)	É a sigla de Norma Brasileira aprovada pela ABNT, de caráter voluntário e fundamentada no consenso de um grupo de representantes da comunidade científica. Suas disposições abrangem diversos temas e são obrigatórias quando em condições estabelecidas pelo poder público competente.
Negociação de chaves (*Key Agreement*)	Processo ou protocolo que possibilita atribuir uma chave criptográfica simétrica compartilhada aos parceiros legítimos em função de valores secretos escolhidos por cada um dos parceiros, de forma que nenhuma outra entidade possa determinar o valor da chave criptográfica. Exemplo clássico de negociação de chaves é o algoritmo *Diffie-Hellman*.
No-breaks	Equipamento que tem como função suprir a energia de um circuito, por um tempo determinado, na ausência da fonte de energia principal da rede elétrica.
Nome Significativo	É aquele que possibilita determinar a identidade da pessoa ou organização a que se refere.
Número de Série do	Um valor que identifica de forma unívoca um certificado emitido por uma

PALAVRA CHAVE	DESCRIÇÃO
Certificado	Autoridade Certificadora.
Número de Identificação Pessoal (*Personal Identification Number* - PIN)	Código alfanumérico ou senha usada para autenticar uma identidade.
Número de Registro	No contexto do sistema de arquivos de cartões inteligentes, representa um número seqüencial atribuído a cada registro, que serve para identificar unicamente o registro dentro de seu EF [ISO/IEC 7816-4].
***Object Identifier* (OID)**	Um OID – *Object Identifier* - é um número único que identifica uma classe de objetos ou um atributo em um diretório ou combinação de diretórios. OIDs são definidos por entidades emissoras e formam uma hierarquia. Um OID é representado por um conjunto de números decimais separados por pontos (ex.: 1.2.3.4). OIDs são usados extensivamente em certificados de formato X.509, como por exemplo, para designar algoritmos criptográficos empregados, políticas de certificação e campos de extensão. Praticamente toda implementação de ICP usando este formato requer o registro de novos OIDs, em particular uma que designe a política de certificação que estabelece seu regime regulatório básico. É crucial que os OIDs sejam obtidos dos legítimos responsáveis pelos arcos, para se evitar incompatibilidades e colisões. Nos certificados da ICP-Brasil os OIDs utilizados para identificar as Políticas de Certificados e Declaração de Práticas de Certificação das Autoridades Certificadoras são atribuídos pelo ITI, durante o processo de auditoria da AC e obedecem a seguinte lógica: **2.16.76.1.1.n –** OID para Declarações de Práticas de Certificação **2.16.76.1.2.n –** OID para Políticas de Certificados **2.16.76.1.3.n e 2.16.76.1.4.n –** OID usados para permitir a inclusão no certificado de outros dados de pessoas físicas e jurídicas, como CNPJ, CPF, título de eleitor, categoria profissional etc.
Objeto de Dado	No contexto do padrão ISO/IEC 7816-4 para cartões inteligentes, um objeto de dado consiste em um conjunto de caracteres (*tag*), um comprimento e um valor (um elemento de dado, por exemplo). Nesta parte do padrão ISO/IEC 7816, objetos de dados são referenciados como BER-TLV, COMPACT-TLV e SIMPLE-TLV [ISO/IEC 7816-4].
Observatório Nacional (ON)	Vinculado ao Ministério da Ciência e Tecnologia, integrante do Sistema Nacional de Metrologia – Sinmetro, o ON é o responsável legal pela geração, conservação e disseminação da Hora Legal Brasileira, com rastreabilidade metrológica ao BIPM. Mantém e opera o Relógio Atômico, que é a Fonte Confiável do Tempo (FCT), a partir da qual se determina a Hora Legal Brasileira.
Octeto	Conjunto de 8 bits compreendendo um *byte*.
OCSP (On-line Certificate Status Protocol)	O Protocolo *On-line* para verificação de Estado de Certificados, OCSP é um dos dois esquemas comuns para verificar se um certificado digital não se encontra revogado. O outro método é a LCR (ver LCR).

PALAVRA CHAVE	DESCRIÇÃO
	Através do OCSP, qualquer aplicação pode fazer consultas a um serviço que checa, diretamente no Banco de Dados da Autoridade Certificadora, o status de um determinado certificado. As respostas emitidas por este serviço são individuais (uma para cada certificado) e são assinadas digitalmente, a fim de garantir sua confiabilidade. Dessa maneira, a lacuna entre o momento da revogação e a emissão da próxima LCR deixa de existir, já que, uma vez que seja marcado como revogado no banco de dados da AC, a próxima resposta OCSP já apresentará este status, eliminando a possibilidade de um acesso não-autorizado desta natureza.
Off-Line	Fora de linha, desligado. Quando não existe nenhum contato do computador com uma rede.
Oficial de Segurança	Papel de acesso que quando assumido por uma entidade usuária externa permite realizar serviços relacionados à iniciação do sistema de arquivos do módulo, gerenciamento do módulo, reinicialização do módulo, sobrescrita do valor de chaves criptográficas (*key zeroization*) e destruição do módulo.
On-Line	Significa "estar em linha", estar ligado em determinado momento à rede ou a um outro computador.
Operação Criptográfica	Operação que manipula uma chave criptográfica.
Operador	Um indivíduo ou processo que realiza operações no módulo criptográfico.
OpenSSL	É uma implementação de código aberto dos protocolos SSL e TLS. A biblioteca (escrita na linguagem C) implementa as funções básicas de criptografia e disponibiliza várias funções utilitárias. O *OpenSSL* está disponível para a maioria dos sistemas do tipo Unix, incluindo Linux, Mac OS X e para as quatro versões do BSD de código aberto e também para o *Microsoft Windows.*
Par de chaves	Chaves privada e pública de um sistema criptográfico assimétrico. A chave privada e sua chave pública são matematicamente relacionadas e possuem certas propriedades, entre elas a de que é impossível a dedução da chave privada a partir da chave pública conhecida. A chave pública pode ser usada para verificação de uma assinatura digital que a chave privada correspondente tenha criado ou a chave privada pode decifrar a uma mensagem cifrada a partir da sua correspondente chave pública. A chave privada deve ser de conhecimento exclusivo do titular do certificado.
Parâmetros críticos de segurança (PCS)	Representam informações sensíveis e relacionadas à segurança, tais como, chaves criptográficas assimétricas privadas, chaves simétricas de caráter secreto, chaves de sessão e dados de autenticação (senhas e PIN, por exemplo), cuja leitura ou modificação podem comprometer a segurança de um módulo criptográfico.
PEM (Privacy Enhanced Mail)	É um padrão da internet que fornece troca segura no correio eletrônico. O PEM emprega um conjunto de técnicas de criptografia para permitir a confidencialidade, a autenticação do remetente e a integridade da mensagem.

PALAVRA CHAVE	DESCRIÇÃO
	Os aspectos da integridade da mensagem permitem que o usuário assegure de que uma mensagem não seja modificada durante o transporte do remetente. A autenticação do remetente permite que um usuário verifique que a mensagem PEM que receberam é verdadeiramente da pessoa que reivindica tê-la emitido. A característica da confidencialidade permite que uma mensagem seja mantida secreta das pessoas a quem a mensagem não foi dirigida.
PI (Parte Interessada)	É a parte interessada (empresa) que deseja fazer a homologação junto ao LSITEC-LEA.
PIN (Personal Identification Number)	É uma seqüência de números e/ou letras (senha) usadas para liberar o acesso à chave privada, ou outros dados armazenados na mídia, somente para pessoas autorizadas.
PKCS (Public Key Cryptographic Standard)	Padrões de criptografia de chave pública. São especificações produzidas pelos Laboratórios RSA em cooperação com desenvolvedores de sistemas seguros de todo o mundo com a finalidade de acelerar a distribuição da criptografia de chave pública.
PKCS#1	Especificação de padrão de dados para o protocolo RSA, incluindo o padrão para criptografia e assinatura digital RSA e o padrão para estocagem de chaves públicas e privadas.
PKCS#5	Especificação de um padrão para derivação de chaves e mecanismos de cifração baseado em senhas. Descreve um método para cifrar um vetor de bytes utilizando uma chave secreta calculada a partir de uma senha (*Password-Based Encryption* ou PBE). É destinado á proteção de chaves privadas em situações que exijam a sua transferência. Isto pode ser necessário, por exemplo, quando as chaves são geradas pela CA e não pelo usuário; ou quando o usuário necessita transferir a chave para outra máquina. A cifragem utilizada está baseada no DES.
PKCS#10	Especificação de um padrão para codificar requisições de certificados, incluindo o nome da pessoa que requisita o certificado e sua chave pública.
PKCS#7 (CMS)	O padrão CMS descreve uma sintaxe genérica para dados que podem ser submetidos a funções criptográficas, tais como assinatura e envelopagem digital. Permite recursividade, com aninhamento de envelopes e *wrappers*. Permite também a associação de atributos arbitrários, como por exemplo selo temporal ou contra-assinatura, à mensagem no processo de autenticação por assinatura. Casos particulares oferecem meios de disseminação de certificados e CRLs. O padrão CMS pode dar suporte a uma variedade de arquiteturas de gerenciamento de chaves baseadas em ICP, como aquela proposta para o padrão PEM na RFC 1422. Entretanto, topologias, modelos de confiança e políticas de certificação para ICPs estão fora do seu escopo. Valores produzidos pelo padrão estão destinados à codificação DER, ou seja, para transmissão e armazenagem na forma de cadeias de octetos de comprimento não necessariamente conhecidos de antemão. Na ICP-Brasil, é largamente utilizado na assinatura digital.

PALAVRA CHAVE	DESCRIÇÃO
PKCS#8	Especificação de um padrão para chaves privadas: o valor da chave, o algoritmo correspondente e um conjunto de atributos associados. Define também em uma sintaxe para chaves cifradas recorrendo às técnicas PBE definidas no PKCS#5.
PKCS#11	Este padrão descreve a interface de programação chamada *"Cryptoki"* utilizada para operações criptográficas em hardwares: *tokens, smart cards*. É comum utilizar o PKCS#11 para prover o suporte aos *tokens* como as aplicações de SSL e S/MIME.
PKCS#12	Descreve uma sintaxe para a transferência de informação de identificação pessoal, incluindo chaves privadas, certificados, chaves secretas e extensões. É uma norma muito útil uma vez que é utilizada por diversas aplicações (ex. IE e Mozilla) para importar e exportar este tipo de informação. Suporta a transferência de informação pessoal em diferentes condições de manutenção da privacidade e integridade. O grau de segurança mais elevado prevê a utilização de assinaturas digitais e cifras assimétricas para proteção da informação.
PKI (Public Key Infrastrusture)	Infra-estrutura de chaves públicas. A ICP-Brasil é um exemplo de PKI.
Plano de Auditoria	Roteiro que descreve, pelo menos, como a auditoria pretende proceder à verificação da Política de Certificação, PC, da Declaração de Práticas de Certificação, DPC e da Política de Segurança, PS e recomendar providências quanto às observações levantadas.
Plano de Contingência	É um plano para situações de emergência, que visa a garantir a disponibilidade dos recursos e serviços críticos e facilitar a continuidade de operações de uma organização. Deve ser regularmente atualizado e testado, para ter eficácia caso necessária sua utilização. Sinônimo de plano de desastre e plano de emergência.
Plano de Continuidade de Negócios	Plano cujo objetivo é manter em funcionamento os serviços e processos críticos das entidades integrantes da ICP-Brasil, na eventualidade da ocorrência de desastres, atentados, falhas e intempéries.
Plano de Desenvolvimento e Implantação dos Trabalhos de Auditoria	Plano elaborado pela Empresa de Auditoria Independente, que especifica de maneira clara e objetiva cada etapa do trabalho, procedimentos e técnicas a serem adotadas em cada atividade, prazo de execução e pontos de homologação, bem como tabelas indicativas do número de horas de auditoria e o número de auditores a serem alocados nos serviços que serão realizados em entidades da ICP-Brasil.
Plano de Recuperação de Desastres	Conjunto de procedimentos alternativos, a serem adotados após um desastre, visando a reativação dos processos operacionais que tenham sido paralisados, total ou parcialmente, ainda que com alguma degradação.
Política de Carimbo de Tempo (PCT)	Conjunto de normas que indicam a aplicabilidade de um carimbo de tempo para uma determinada comunidade e/ou classe de aplicação com requisitos comuns de segurança.

PALAVRA CHAVE	DESCRIÇÃO
Política de Certificação (PC)	Documento que descreve os requisitos, procedimentos e nível de segurança adotados para a emissão, revogação e gerenciamento do ciclo de vida de um Certificado Digital.
Política de Segurança (PS)	É um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades.
Precisão	Ver Exatidão.
Prestador de Serviço de Certificação	As Autoridades Certificadoras, as Autoridades de Registro e os prestadores de serviço suporte credenciados junto à ICP-Brasil.
Prestador de Serviços de Suporte	Aquele que desempenha as atividades descritas na PC, PCT, DPC ou DPCT da AC ou ACT responsável por esses documentos. São empresas contratadas por uma AC, ACT ou AR para realizar atividades de: disponibilização de infra-estrutura física e lógica; disponibilização de recursos humanos especializados; disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.
Privacidade de documentos eletrônicos	Vide Confidencialidade de Documentos Eletrônicos
PRNG (Pseudo Random Number Generator)	Um gerador de número pseudo-aleatório é um algoritmo que gera uma seqüência de números, os quais são aproximadamente independentes um dos outros. A saída da maioria dos geradores de números aleatórios não é verdadeiramente aleatória; ela somente aproxima algumas das propriedades dos números aleatórios. Enquanto números verdadeiramente aleatórios podem ser gerados usando hardware para geração de número aleatório, número pseudo aleatórios são uma parte crítica da computação moderna, da criptografia até o método de *Monte Carlo* passando por sistemas de simulação. Uma cuidadosa análise matemática é necessária para assegurar que a geração dos números seja suficientemente "aleatória".
Procedimento de Fiscalização	As ações que objetivam a verificação do cumprimento das normas que regem a ICP-Brasil por parte das entidades credenciadas.
Protocolo	Uma descrição das regras que dois computadores devem obedecer ao estabelecer uma comunicação. Um conjunto de regras padronizadas que especifica o formato, a sincronização, o seqüenciamento, a transmissão de dados, incluindo inicialização, verificação, coleta de dados, endereçamento e verificação e correção de erros em comunicação de dados.
PSC (Provedor de Serviços Criptográficos)	Vide *CSP (Cryptographic Service Provider)*
Proxy	É um servidor que age como um intermediário entre uma estação de trabalho e a internet para segurança, controle administrativo e serviço de *cache*. Um servidor (programa) *proxy* (ou com capacidades de *proxy*) recebe pedidos de computadores ligados à sua rede e, caso necessário, efetua esses mesmos pedidos ao exterior dessa rede, usando como identificação o seu próprio numero IP e não o numero IP do computador que requisitou o serviço. Útil

PALAVRA CHAVE	DESCRIÇÃO
	quando não se dispõe de números IP registrados numa rede interna ou por questões de segurança.
PUK (Personal Identification Number Umblocking Key)	É uma chave para desbloqueio do número de identificação pessoal (PIN), o qual normalmente fica bloqueado após várias tentativas inválidas. Como o PIN, a senha PUK deve ser guardada de forma segura, pois ambas permitem, em dispositivos como *tokens* e *smart cards*, o acesso à chave privada de um titular de certificado.
Rastreabilidade	Relacionamento do resultado de uma medição de sincronismo com um valor de referência previamente estabelecido como padrão. A rastreabilidade se evidencia por intermédio de uma seqüência contínua de medidas, devidamente registradas e armazenadas e permite a verificação, direta ou indireta, do relacionamento entre o tempo informado e a fonte confiável de tempo.
Recuperação de Chave	Processo no qual uma chave privada pode ser recuperada, a partir de dados armazenados por uma empresa ou órgão governamental. Na ICP-Brasil é proibida a recuperação de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.
Rede	Um grupo de computadores inter-conectados, controlados individualmente, junto com o hardware e o software usado para conectá-los. Uma rede permite que usuários compartilhem dados e dispositivos periféricos como impressoras e mídia de armazenamento, troquem informações por meio do correio eletrônico e assim por diante.
Rede de Sincronismo Autenticado (ReTemp/HLB)	Rede criada e mantida pelo Observatório Nacional, que permite a rastreabilidade e a autenticação do tempo, nos equipamentos que a compõem, em relação à Hora Legal Brasileira e à UTC.
Rede Local	Um grupo de computadores conectados com a finalidade de compartilhar recursos. Os computadores em uma rede local são normalmente ligados por um único cabo de transmissão e localizados dentro de uma pequena área, como um único prédio ou seção de um prédio.
Redundância	i. Componentes de um sistema de computador que são instalados para fazer *backup*. Utilizados para garantir a operação ininterrupta de um sistema em caso de falha. ii. Diz-se de um segundo dispositivo que esteja imediatamente disponível para uso quando de uma falha de um dispositivo primário de um sistema de computador.
Registro	Cadeia de octetos que pode ser manuseada como um todo pelo cartão inteligente e referenciada por um número de registro ou por um identificador de registro [ISO/IEC 7816-4].
Relatório de auditoria	Documento que traduz a forma como foi desenvolvido o trabalho de auditoria e que exprime de forma clara, concisa e exata, uma opinião sobre os resultados a que o auditor chegou, devendo conter, sempre que for caso, as alegações, as respostas ou as observações dos responsáveis e, ainda, conclusões e recomendações.

PALAVRA CHAVE	DESCRIÇÃO
Relatório de Fiscalização	Documento pelo qual o servidor responsável pela fiscalização descreve o que constatou na entidade fiscalizada
Relying Party	Vide Terceira Parte
RNG (Random Number Generator)	Quando um número aleatório é gerado por um programa, este número não é exatamente aleatório (por isto que números aleatórios gerados por programas são mais corretamente classificados como pseudo-aleatórios). Portanto, em sistemas onde são geradas chaves criptográficas importantes, é necessário existir um circuito chamado *Random Number Generator* (RNG) que garanta que os números gerados são realmente ao acaso e não baseados no relógio de tempo real do computador.
Realimentação de dados de autenticação *(Echo)*	Exibição visível de caracteres no momento da inserção de uma senha.
Renovação de Certificados	É o processo para obter um certificado novo antes que o certificado existente tenha expirado. Na ICP-Brasil, é obrigatória a geração de novas chaves criptográficas para cada certificado emitido.
Repositório	É um sistema confiável e acessível *on-line,* mantido por uma Autoridade Certificadora, para publicar sua Declaração de Práticas de Certificação (DPC), Políticas de Certificado (PC), Política de Segurança (PS), Lista de Certificados Revogados (LCR) e endereços das instalações técnicas das AR vinculadas.
Resolução (*Resolution*)	Menor diferença entre indicações de um dispositivo mostrador que pode ser significativamente percebida. A resolução de um relógio é o menor incremento de tempo que o mesmo pode indicar.
Retardo (*Delay*)	Tempo de propagação na internet entre o SCT e o SAS.
Revogação de Certificados	Encerramento da validade de um certificado digital antes do prazo previsto. Pode ocorrer por iniciativa do usuário, da Autoridade de Registro, da Autoridade Certificadora ou da Autoridade Certificadora Raiz.
RFC (Request for Comments)	Os RFC são documentos técnicos ou informativos que discutem os mais diversos aspectos relacionados à internet. Os assuntos variam desde especificações, padrões e normas técnicas até questões históricas acerca da rede mundial de computadores. Os RFC são documentos públicos, qualquer pessoa tem acesso a eles, podendo ler, comentar, enviar sugestões e relatar experiências sobre o assunto. Pode-se pesquisar os RFC no *site*: http://www.faqs.org/rfcs.
Risco ou Ameaça	i. É a probabilidade da concretização de um evento que possa causar perdas significativas por causar danos a um ou mais aos ativos da organização. ii. É um fator externo que pode vir a atacar um ativo causando um desastre ou perda significativa.
Roteador	Sistema computacional que usa uma ou mais métricas para determinar o caminho otimizado pelo qual o tráfego da rede deve ser encaminhado – por meio de seus endereços – de uma rede local ou remota para outra.
Roteamento	Processo de seleção de rotas para uma mensagem.

PALAVRA CHAVE	DESCRIÇÃO
RSA (Rivest Shamir and Adleman)	O RSA é um algoritmo assimétrico que possui esse nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. É, atualmente, o algoritmo de chave pública mais amplamente utilizado, sendo capaz de fornecer assinaturas digitais e cifrar textos.
Sala-cofre	Área de Segurança restrita, formada por cofre com proteção eletromagnética, física e contra fogo, afim de proteger as chaves privativas que assinam os Certificados Digitais.
***Secure Messaging* (Transferência Segura de Mensagens por Meios Eletrônicos)**	Qualquer método de entrega de uma mensagem segura, incluindo *TLS* (segurança da camada de transporte), SMTP sobre SSL e HTTPS.
Segundo de Transição *(leap second)*	Ajuste ao UTC por meio da subtração ou adição de um segundo no último segundo de um mês do UTC. A primeira escolha é o fim de dezembro e de junho e a segunda escolha é o fim de março e de setembro.
Segurança Física	O principal objetivo da implantação de controles de segurança física é restringir o acesso às áreas críticas da organização, prevenindo os acessos não autorizados que podem acarretar danos a equipamentos, acessos indevidos à informação, roubos de equipamentos, entre outros. Os controles de acesso físico devem ser implementados em conjunto com os controles de acesso lógico. A falta de implementação desses dois controles em conjunto, seria o mesmo que restringir o acesso às informações através de senhas, mas deixar os servidores desprotegidos fisicamente, vulneráveis a roubo, por exemplo.
Selo Cronológico Digital	Serviço que registra, no mínimo, a data e a hora correta de um ato, além da identidade da pessoa ou equipamento que enviou ou recebeu o selo cronológico. O Selo Cronológico Digital cria uma confirmação assinada digitalmente e à prova de fraude sobre a existência de uma transação ou documento específico.
Selo de Homologação	Selo conferido aos sistemas e equipamentos homologados pelo ITI.
Semente (de chave criptográfica)	Um valor secreto usado para inicializar uma função ou uma operação criptográfica.
Senha	Um conjunto de caracteres, conhecidos apenas pelo usuário, que fornecem acesso ao arquivo, computador ou programa. Senhas são geralmente usadas em conjunto com o nome do usuário que o autentica e o garante autorização ao acesso.
Senha Forte	Inverso de Senha Fraca ou Óbvia
Senha Fraca ou Óbvia	É aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena, tal como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, seqüências numéricas simples, palavras com significado, dentre outras

PALAVRA CHAVE	DESCRIÇÃO
Serviço Criptográfico ICP (ou Aplicação ICP)	Aplicação de infra-estrutura de chaves públicas contextualizada para o âmbito da ICP-Brasil.
Servidor de Aplicativos	Sistema que realiza a interface entre o subscritor e o SCT. Encaminha as solicitações de carimbo de tempo ao SCT e em seguida devolve ao subscritor os carimbos de tempo ou mensagens de erro recebidos em resposta.
Servidor de Autenticação e Sincronismo (SAS)	Dispositivo constituído por *hardware* e *software* que audita e sincroniza SAS ou SCT. Deve possuir um HSM com relógio para sincronização e capacidade de processamento criptográfico para geração de chaves criptográficas e realização de assinaturas digitais.
Servidor de Carimbo de Tempo (SCT)	Dispositivo único constituído por *hardware* e *software* que gera os carimbos de tempo, sob o gerenciamento da ACT. Deve possuir um HSM contendo um relógio a partir do qual são emitidos os carimbos do tempo. Nesse HSM devem ser também realizadas as funções criptográficas de geração de chaves e assinaturas digitais.
SHA-1 (*Secure Hash Algorithm)*	O *Secure Hash Algorithm,* uma função de espalhamento unidirecional inventada pela NSA, gera um valor *hash* de 160 bits, a partir de um tamanho arbitrário de mensagem.
SHA-224, SHA-256,SHA-384 e SHA-512 (SHA-2 Family - Secure Hash Algorithm)	O NIST publicou quatro funções adicionais da família *SHA*, cada uma com valores *hash* maiores, conhecidos coletivamente como *SHA-2*. As variantes individuais são nomeadas, através de seus comprimentos de *hash* (em *bits*): SHA-224, SHA-256, SHA-384, e SHA-512. O SHA-224 foi definido para combinar o comprimento da chave com duas chaves TripleDES. SHA-256 e SHA-512 são funções de *hash* computadas com palavras de 32 bits e 64 bits respectivamente. Usam quantidades diferentes de deslocamento e constantes adicionais, mas suas estruturas são virtualmente idênticas, diferindo somente no número de voltas. SHA-224 e SHA-384 são simplesmente versões truncadas das duas primeiras, computadas com valores iniciais diferentes.
Sigilo	Condição na qual dados sensíveis são mantidos secretos e divulgados apenas para as partes autorizadas. Os titulares de certificados de assinatura digital emitidos pela AC são responsáveis pela geração, manutenção e pela garantia do sigilo de suas respectivas chaves privadas, bem como pela divulgação ou utilização indevidas dessas mesmas chaves.
Signatário	É a pessoa/entidade que cria uma assinatura digital para uma mensagem com a intenção de autenticá-la.
Signed Data	O tipo de conteúdo *signed data* consiste em um conteúdo de todos os tipos e zero ou mais valores de assinatura digital. Qualquer número de assinantes pode assinar em paralelo qualquer tipo de conteúdo. A aplicação típica do tipo de conteúdo *signed data* é representada por uma assinatura digital do assinador no conteúdo do tipo de conteúdo de dados. Uma outra aplicação típica disseminada são os certificados digitais e as listas da revogação do certificado (CRL).
Sincronização de	Processo pelo qual dois ou mais relógios passam a indicar o mesmo tempo.

PALAVRA CHAVE	DESCRIÇÃO
Relógio	
Sistema de Autenticação e Sincronismo (SAS)	Dispositivo constituído por hardware e software que audita e sincroniza SAS ou SCT. Deve possuir um HSM com relógio para sincronização e capacidade de processamento criptográfico para geração de chaves criptográficas e realização de assinaturas digitais.
Servidor de Carimbo de Tempo (SCT)	Dispositivo único constituído por hardware e software que emite os carimbos de tempo, sob o gerenciamento da ACT. Deve possuir um HSM contendo um relógio a partir do qual são emitidos os carimbos do tempo. Nesse HSM devem ser também realizadas as funções criptográficas de geração de chaves e assinaturas digitais.
Sistema Criptográfico	Sistema composto de documentação normativa específica de criptografia aplicada na ICP-Brasil, conjunto de requisitos de criptografia, projetos, métodos de implementação, módulos implementados de *hardware* e *software*, definições relativas a algoritmos criptográficos e demais algoritmos integrantes de um processo criptográfico, procedimentos adotados para gerência das chaves criptográficas, métodos adotados para testes de robustez das cifras e detecção de violações dessas.
Sistema de Certificação Digital	Todo e qualquer programa de computador, ainda que embarcado, que compõe meio necessário ou suficiente à realização de Certificação Digital.
Sistema de Detecção de Intruso (IDS)	Ferramentas de segurança que ajudam os administradores a evitarem danos na rede quando as outras proteções, tais como controle de acesso ou *firewalls*, não conseguem afastar os intrusos. Detecta tentativas ou ataques bem-sucedidos nos recursos monitorados. Os recursos monitorados podem fazer parte de uma rede ou um sistema *host*.
Sistema de Pagamento Brasileiro (SPB)	Sistema responsável pela interação entre o Banco Central, o governo, as instituições financeiras, as empresas e até mesmo as pessoas físicas. Gerencia o processo de compensação e liquidação de pagamentos por meio eletrônico, ligando as Instituições Financeiras credenciadas ao Banco Central do Brasil. Utiliza certificados digitais da ICP-Brasil para autenticar e verificar a identidade dos participantes em todas as operações realizadas;
Sistema Operacional	Programa principal que se dedica às tarefas de organização e controle das atividades do computador e seus periféricos.
Skew	Diferença de freqüência entre dois relógios (primeira derivada do *offset* no tempo).
Slot	Em um *HSM (Hardware Security Module)*, um *slot* é um leitor lógico que pontencialmente contém um *token.*
Smart Card	i. É um tipo de cartão plástico semelhante a um cartão de crédito com um ou mais *microchips* embutidos, capaz de armazenar e processar dados. Um *smart card* pode ser programado para desempenhar inúmeras funções, inclusive pode ter capacidade de gerar chaves públicas e privadas e de armazenar certificados digitais. Pode ser utilizado tanto para controle de acesso lógico como para controle de acesso físico.

PALAVRA CHAVE	DESCRIÇÃO
	ii. Um pequeno dispositivo, geralmente do tamanho de um cartão de crédito, que contém um processador e é capaz de armazenar informação criptográfica (como chaves e certificado) e realizar operações criptográficas.
S/MIME (Secure / Multipurpose Internet Mail Extensions)	*S/MIME* é um protocolo de segurança de *e-mail*. Foi desenhado para prevenir a interceptação e falsificação de *e-mail* usando cifração e assinatura digital. S/MIME constrói a segurança em cima do protocolo MIME e é baseado na tecnologia desenvolvida originalmente pela *RSA Data Security, Inc.*
SO	i. Sistema Operacional; ii. Em um *HSM (Hardware Security Module)*, é o *Security Officer,* é um usuário do dispositivo criptográfico com poderes de administrador do sistema.
Software	i. Programa de computador que utiliza uma seqüência lógica de instruções que o computador é capaz de executar para obter um resultado específico. ii. Conjunto de programas e instruções que operam o computador. São dois os tipos de *software* de computador: *software* de sistema, o qual engloba operações básicas necessárias para operar o *hardware* (por exemplo, sistema operacional, utilitários de comunicação, monitores de performance, editores, compiladores etc.) e *software* aplicativo, o qual executa tarefas específicas para auxiliar os usuários em suas atividades. iii. Programas e componentes de dados que podem ser dinamicamente modificados durante a execução, usualmente armazenados em mídias regraváveis.
SSL (Secure Socket Layer)	Protocolo de segurança que provê privacidade na comunicação através da internet. O Protocolo permite que aplicativos cliente e servidor se comuniquem utilizando mecanismos criados para proteger o sigilo e a integridade do conteúdo que trafega pela internet. Desenvolvido pela Netscape para transmitir documentos privativos pela internet.
Subscritor	Pessoa física ou jurídica que solicita os serviços de uma Autoridade de Carimbo do Tempo (ACT), implícita ou explicitamente concordando com os termos mediante os quais o serviço é oferecido.
Suspensão de Certificado	Suspensão do uso de um certificado digital por um período determinado de tempo. A suspensão de certificado digital não é permitida no âmbito da ICP-Brasil.
Switch	Dispositivo que direciona pacotes em uma rede.
Template	Na especificação do *PKCS#11 (Cryptoki),* um *template* é um vetor de atributos e é usado para criar, manipular e procurar objetos.
TRC (Teorema de Resto Chinês)	Este algoritmo, utilizado para resolver sistemas de congruências lineares, é muito antigo e foi inventado, independentemente, pelos chineses e pelos gregos, para resolver problemas de astronomia. O algoritmo chinês do resto tem este nome porque um dos primeiros lugares em que aparece é o livro *Manual de aritmética do mestre Sun*,

PALAVRA CHAVE	DESCRIÇÃO
	escrito entre 287 d.C. e 473 d.C.
Tempo Universal Coordenado (UTC)	Escala de tempo adotada como padrão de Tempo Oficial Internacional, utilizada pelo sistema de Metrologia Internacional, Convenção do Metro, determinada e disseminada pelo *Bureau International des Poids et Mesures* - BIPM, França.
Terceira Parte	i. É a parte que age confiante no teor, validade e aplicabilidade do certificado digital emitido por uma das AC integrantes da ICP-Brasil. ii. Pessoa ou instituição que age com total independência de fabricantes, desenvolvedores, representantes comerciais, prestadores de serviços de certificação digital e de potenciais compradores de sistemas e equipamentos de certificação digital
Termo de Responsabilidade	Termo assinado por uma pessoa física, que será a responsável pelo uso do certificado, quando o titular do certificado é uma organização. No termo, estão estabelecidas as condições de uso do certificado.
Termo de Titularidade	Termo assinado pelo titular do certificado digital emitido para pessoa física ou jurídica onde são estabelecidas as condições de uso do mesmo.
Termo Inicial de Fiscalização (TIF)	O documento que inicia o procedimento de fiscalização.
Texto Cifrado	Dado que foi criptografado. O texto cifrado é a saída do processo de criptografia e pode ser transformado novamente em informação legível em forma de texto claro a partir da chave de decifração.
Texto Claro	Dado que está no estado não cifrado ou decifrado.
Thread-safe	É um conceito de programação de computador aplicado ao contexto de programas *multi-threaded*. Uma parte do código é t*hread-safe* se funcionar corretamente durante a execução simultânea para *threads* múltiplas. Em particular, deve satisfazer à necessidade para *threads* múltiplas para acessar os mesmos dados compartilhados e a necessidade para uma parte compartilhada dos dados ser acessada por somente uma *thread* de cada vez.
Time-stamping	Vide Datação de Registros
Tipo de Certificados	Na ICP-Brasil estão definidos oito (08) tipos de certificados para titulares, classificados da seguinte forma: A1, A2, A3, A4, S1, S2, S3 e S4 e um tipo de certificado para Autoridades Certificadoras.
Titular de Certificado	São as entidades, pessoa física ou jurídica, para as quais foram emitidos um certificado digital. O assinante é o titular da chave privada correspondente à chave pública contida no certificado e possui a capacidade de utilizar tanto uma quanto a outra.
Token	i. Dispositivo para armazenamento do Certificado Digital de forma segura, sendo seu funcionamento parecido com o *smart card,* tendo sua conexão com o computador via USB. ii. Em um *HSM (Hardware Security Module),* um *token* é a visão lógica de

PALAVRA CHAVE	DESCRIÇÃO
	um dispositivo criptográfico definido em *PKCS#11 (Cryptoki).*
Topologia	Disposição física dos nós e dos meios de rede dentro de uma estrutura de rede corporativa.
Transporte de Chaves (*Key Transport*)	Processo ou protocolo que possibilita que uma chave criptográfica simétrica compartilhada seja transferida aos participantes legítimos da entidade geradora para parceiros. Neste método, a chave é definida por uma das entidades e repassada para as demais.
Trilhas de Auditoria	i. Histórico das transações de sistemas que estão disponíveis para a avaliação com o objetivo de provar a correção de sua execução comparada com os procedimentos ditados pela política de segurança. ii. rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. iii. conjunto cronológico de registros que proporcionam evidências do funcionamento do sistema. Estes registros podem ser utilizados para reconstruir, revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para rastrear o uso do sistema, detectando e identificando usuários não autorizados.
Triple DES (3DES)	O 3DES é uma variação do DES, utilizando-o em três ciframentos sucessivos, podendo empregar um versão com duas ou com três chaves diferentes. Seu tamanho de chave é de 112 ou 168 bits.
Unidade de Dado	No contexto da norma ISO 7816-4 representa o menor conjunto de bits que pode ser referenciado de forma não ambígua [ISO/IEC 7816-4].
URL (Uniform Resource Locator)	Um mecanismo padronizado para identificar e localizar certos cadastros e outros recursos localizados na *World Wide Web*. A maioria das URLs aparece na forma familiar de endereços de sites.
Usuário	i. Pessoa que utiliza certificado digital apresentado por um titular. ii. Papel de acesso que quando assumido por uma entidade usuária externa permite realizar serviços de segurança no módulo criptográfico após sua iniciação, incluindo operações criptográficas, geração de chaves criptográficas, o uso do sistema de arquivos, sobrescrita do valor de chaves criptográficas (*key zeroization*), etc.
Usuário Final	É uma pessoa física ou jurídica que possui um certificado digital. Sinônimo de Titular de Certificado.
Validação da Cadeia de Certificados	Consiste na verificação da validade do certificado, nomeadamente a data, assinatura e validade dos certificados que estejam na sua cadeia de certificação, até ao certificado de confiança.
Validade de LCR	Período de tempo em que a LCR está com sua data de validade operacional. As LCR possuem prazo máximo de validade de acordo com o tipo de certificado previsto na ICP-Brasil.
Validade do Certificado	Período de tempo em que o certificado está com sua data de validade operacional. Os Certificados possuem prazo máximo de validade de acordo

PALAVRA CHAVE	DESCRIÇÃO
	com o tipo de certificado previsto na ICP-Brasil.
Verificação	Ratificação da identidade de uma pessoa física ou jurídica mediante a solicitação de certificado através de documentação apresentada pelo solicitante e da reconfirmação dos dados da solicitação.
Verificação da Validade do Certificado	Processo realizado por um destinatário ou terceira parte para confirmar que o certificado de um titular, usuário final, é válido e era operacional na data e hora que uma assinatura digital pertinente foi criada.
Verificação de Assinatura digital	Ação realizada para determinar com precisão que: i. a assinatura digital foi criada durante o período operacional de um certificado válido por uma chave privada correspondente à chave pública contida no certificado e ii. que a mensagem associada não tenha sido alterada desde que a assinatura digital foi criada.
Vírus	Os vírus são pequenos segmentos de códigos programados, normalmente com más intenções, que têm a característica de se agregar ao código de outros programas. Assim que são executados, disparam o código maliciosamente alterado a fim de causar modificações indevidas no processamento normal do sistema em que este se encontra, causando (ou não) desde danos leves a irreparáveis.
VPN (Virtual Private Networks)	É definida como a conectividade de uma corporação e suas unidades através de uma infra-estrutura compartilhada de comunicação com as mesmas características de segurança de uma rede privativa. Os nós são conectados por meio de recursos de uma rede pública de telecomunicações, utilizando criptografia e outros dispositivos de segurança para garantir que os dados dessa rede não serão interceptados.
Vulnerabilidade	É uma fraqueza em uma máquina, programa ou sistema que pode ser explorada por um agressor. Agressores procuram por essas vulnerabilidades para explorá-las como forma de tomar acesso ao sistema. Um bom administrador de redes se mantém informado e atualizado de todas as vulnerabilidades descobertas nos sistemas, para agir de forma rápida na correção daquelas que dizem respeito ao ambiente que administra.
Worms	São programas maliciosos semelhantes aos vírus, porém se diferenciam na forma de infecção e nos tipos de danos que podem causar.
X.509	Recomendação ITU-T, a especificação X.509 é um padrão que especifica o formato dos certificados digitais, de tal maneira que se possa amarrar firmemente um nome a uma chave pública, permitindo autenticação forte. Faz parte das séries X.500 de recomendações para uma estrutura de diretório global, baseadas em nomes distintos para localização. Na ICP-Brasil utilizam-se certificados no padrão X-509 V3.
Zeramento de Chaves	Vide *Key Zeroization*