FACULDADES INTEGRADAS

“ANTÔNIO EUFRÁSIO DE TOLEDO”

FACULDADE DE DIREITO DE PRESIDENTE PRUDENTE

SEGURANÇA JURÍDICA NAS RELAÇÕES POR MEIO ELETRÔNICO

Osvaldo Minoru Itano

Presidente Prudente (SP)

Novembro/2002

FACULDADES INTEGRADAS

"ANTÔNIO EUFRÁSIO DE TOLEDO”

FACULDADE DE DIREITO DE PRESIDENTE PRUDENTE

SEGURANÇA JURÍDICA NAS RELAÇÕES POR MEIO ELETRÔNICO

Osvaldo Minoru Itano

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do grau de Bacharel em Direito, sob orientação do Prof. Edson Freitas de Oliveira.

Presidente Prudente (SP)

Novembro/2002

SEGURANÇA JURÍDICA NAS RELAÇÕES POR MEIO ELETRÔNICO

Trabalho de Conclusão de Curso aprovado como requisito parcial para obtenção do grau de Bacharel em Direito.

_____

PROF. EDSON FREITAS DE OLIVEIRA
Orientador

_____

PROF.ª GILMARA PESQUERO FERNANDES MOHR FUNES
Examinadora

_____

PROF. MARCO ANTONIO DE ALMEIDA PRADO GAZZETTI
Examinador

Presidente Prudente (SP),

“Não se deve nunca esgotar de tal modo um assunto, que não se deixe ao leitor nada a fazer.

Não se trata de fazer ler, mas de fazer pensar.”

Montesquieu

(Do Espírito das Leis, livro XI, cap. XX)

AGRADECIMENTOS

Agradeço à Rosa e Fabiana, esposa e filha, que colaboraram imensamente para que eu atingisse meus objetivos.

Agradeço ao orientador Prof. Edson, pelos ensinamentos ministrados e pela prestação do valoroso auxílio na consecução do presente trabalho, tanto na parte formal quanto material, e também pela extrema disponibilidade e cortesia que sempre me dispensou.

Agradeço à Vera Lúcia T. P. G. Campos pelos seus conselhos sempre oportunos e, ao Alexandre H. Tokashiki, pela prestimosa colaboração, ajudando-me sobremaneira na pesquisa bibliográfica e no entendimento de tecnologia desconhecida.

Osvaldo Minoru Itano

RESUMO

O presente trabalho focaliza a segurança jurídica nas relações por meio eletrônico. Nestas são envolvidas tanto empresas (desde as microempresas até as gigantescas multinacionais) quanto pessoas (na condição estritamente particular ou interagindo com outras pessoas, com órgãos ou com empresas). Atinge, ainda, entre outros, o Poder Judiciário. Enfim, toda a infindável atividade humana exercitada por meio eletrônico.

Nesta monografia de compilação foi pesquisada apenas parte da bibliografia disponível. Como resultado deste trabalho de pesquisa, é possível afirmar que existem sistemas que possibilitam, utilizando-se da técnica de assinaturas assimétricas, dar segurança total aos documentos firmados por meio eletrônico, assegurando às partes envolvidas a garantia de que está sendo preservado o sigilo da comunicação, que reciprocamente emissores e receptores são realmente quem dizem ser, que eventual adulteração por terceiros das mensagens trocadas não passarão imperceptíveis e que, ante à demonstração do sistema aplicado na assinatura digital, a parte contrária não poderá repudiar o que foi contratado.

Para os documentos autenticados com a aplicação da tecnologia das chaves assimétricas, a legislação ora em vigor em nosso ordenamento é suficientemente hábil para torná-los perfeitamente admissíveis como prova em nossos tribunais, não carecendo, portanto, de nova intervenção legislativa.

Por tratarem do assunto, foram enfocados a medida provisória n.º 2.200-2, de 24/8/2001, o projeto de lei n.º 1.589/99, e o projeto ICP/OAB, que se acha em fase de testes, e feitos breves comentários sobre a literatura existente sobre o tema.

PALAVRAS-CHAVE: Contrato. Meio eletrônico. Internet. Documento eletrônico. Criptografia. Chave assimétrica. Chave pública. Chave privada.

ABSTRACT

The present work focus on the juridical safety in the electronic way relations. In these relations are involved both enterprise (since the microenterprise until the giant multinational firms) and people (in a strictly private condition or interacting with other people, with organs or with enterprises). It also affects, among others, the judiciary power. At last, all the unending human activity exercised by electronic way.

As a result of this research work, it is possible to affirm that there are systems that make possible, using the asymmetrical signature technique, to give total security to the documents settled by electronic way, securing to the involved parts the guarantee that it is being preserved the communication secrecy, which reciprocatly the transmitter and the receiver are really who they told they are, that fortuitous adulteration of the exchanged messages, by third parts, is not going to pass unperceptible and that, in view of the demonstration of the applied system in the digital signature, the adversary part will not be able to repudiate what was contracted.

For the certified documents with the asymmetrical keys tecnology application, the actual legislation is sufficiently able to make them perfectly admissible as evidence in our courts, being not necessary, therefore, a new legislative intervention.

Because of dealing with the subject, number 2.200-2, provisional remedy, from 08/24/2001, number 1.589/99 bill and the project ICP/OAB, which is in test phase, were tackled.

KEY-WORDS: Contract. Electronic way. Internet. Electronic document. Cryptography. Asymmetrical key. Public key. Private key.

SUMÁRIO

1 INTRODUÇÃO..... 9

2 A ELETRÔNICA NO COMÉRCIO E NO PODER JUDICIÁRIO..... 11
2.1 Comércio Eletrônico..... 11
2.2 Poder Judiciário..... 15
2.2.1 Execução fiscal eletrônica..... 16
2.2.2 Diário da Justiça eletrônico..... 17
2.2.3 Revista Eletrônica da Jurisprudência do STJ..... 18
2.2.4 Penhora on line na Justiça Trabalhista..... 18
2.2.5 E-Justitia..... 19
2.2.6 Transmissão de peças processuais – Projeto de Lei n.º 5.828/01..... 20

3 DOCUMENTO ELETRÔNICO E CONTRATO ELETRÔNICO..... 22
3.1 Histórico..... 22
3.2 Documento..... 22
3.3 Contrato..... 24
3.4 Documento Eletrônico e Contrato Eletrônico..... 28
3.5 O "Tradicional" e o Eletrônico..... 31
3.5.1 Diferenças..... 31

4 SEGURANÇA JURÍDICA NA MANIFESTAÇÃO DA VONTADE POR MEIO ELETRÔNICO..... 33
4.1 A Prova..... 33
4.2 A Aceitação dos Arquivos Digitais como Prova..... 34
4.3 Segurança, validade, integridade e autoria..... 36
4.4 Criptografia..... 37
4.4.1 As técnicas de criptografia..... 39
4.4.2 Tempo e evolução tecnológica..... 42
4.4.3 Custos e benefícios..... 42
4.5 Assinatura Convencional e Assinatura Digital..... 44
4.5.1 Assinatura convencional..... 44
4.5.2 Assinatura digital..... 45
4.6 O Sistema de Chaves Simétricas..... 47

4.7 O Sistema de Chaves Assimétricas..... 47
4.8 Certificadora Autorizada..... 49
4.8.1 A ICP-OAB..... 53
4.9 Tabelião Virtual..... 54

5 LEGISLAÇÃO..... 58
5.1 Medida Provisória n.º 2.200-2, de 24/8/2001..... 58
5.2 Projeto de Lei n.º 1.589/99..... 59

6 CONCLUSÕES..... 62

7 REFERÊNCIAS BIBLIOGRÁFICAS..... 65

1 INTRODUÇÃO

A motivação do presente trabalho consistiu em averiguar a existência, ou não, de segurança que é essencial às manifestações de vontade expressas através de meio eletrônico.

Buscou-se, ainda, o entendimento de termos incomuns como “criptografia” e “chave assimétrica” e a sua conseqüente inter-relação com a segurança.

Conhecê-los e entendê-los é de fundamental importância para a atividade diária, não só de juristas e empresários, como de integrantes dos demais segmentos da sociedade.

Veja-se, para exemplificar, a insegurança que cerca a formalização da Declaração Anual de Rendimentos para efeito de Imposto de Renda. Na sistemática vigente, a Secretaria da Receita Federal não tem certeza de que ela esteja sendo prestada pelo próprio contribuinte ou por alguém se fazendo passar por ele.

No tópico 2 foi feita breve abordagem sobre o papel da eletrônica no comércio e de suas incursões no meio do Poder Judiciário.

No comércio, ela assumiu grandes proporções.

No Judiciário, inúmeros exemplos indicam que aquele Poder sofrerá os efeitos da informática e da Internet em tempo menor do que as expectativas mais otimistas dos demandantes por Justiça. Supõe-se que isto ocorrerá inicialmente de forma localizada em alguns segmentos mais permeáveis a inovações e, em seguida, generalizando-se.

Se, há cinco ou seis anos, ainda era possível conceder-se ao luxo de subestimar o uso da Internet no cotidiano profissional, pessoal ou cultural, atualmente isso não é mais possível.

É certo, contudo, que ainda não tem acesso à rede parte expressiva da sociedade.

Porém, mais rapidamente do que se poderia imaginar há pouco tempo, a Internet invade o cotidiano de mais e mais parcelas da população. No Estado de São Paulo, a propósito, o Governo Estadual mantém o Programa Acessa São Paulo – INFOCENTRO, com o objetivo de instalar centros para acesso gratuito à Internet. Na área privada, os “cibercafés”, lojas destinadas a atender usuários sem computador (incluindo-se aqueles que, deslocados de seu domicílio, necessitarem de computador para suprir situação eventual), estão surgindo e ao que tudo indica, multiplicar-se-ão.

Os institutos versados no tópico 3 estão diretamente ligados à manifestação de vontade em sua natureza até então conhecida e sob forma eletrônica.

Foi estudado, com brevidade, se o documento eletrônico e o contrato eletrônico são simplesmente espécies dos gêneros, respectivamente, documento e contrato já previstos na legislação e doutrina pátrias, ou o momento está a exigir que o legislador aponte caminhos que os regulamentem, como novos institutos.

Após rápida abordagem dessas entidades jurídicas, pretendeu-se, de forma destituída de tecnicidade, situar o leitor nas matérias atinentes à criptografia e à chave assimétrica (tópico 4) que constituem o cerne deste trabalho. São elas as ferramentas que dão garantia de segurança e confiabilidade aos documentos eletrônicos.

No tópico 5, foi analisada a legislação brasileira no que reporta à criptografia e à chave assimétrica já que, nesse inter-relacionamento, orbitam os principais requisitos ligados à segurança jurídica da contratação efetuada por meio eletrônico.

Este trabalho foi iniciado em novembro de 2001 e concluído em julho de 2002. Considerando a dinâmica formidável da tecnologia da informática, não se pretendeu fazê-lo, nem de longe, completo e atualizado, porquanto seria tarefa impossível. Como as mudanças ocorrem em ritmo veloz, dentro de poucos meses poderá estar superado em alguns aspectos. Todavia, para os não-iniciados,

poderá ele servir de instrumento de familiarização com o assunto para posterior atualização e aprofundamento.

2 A ELETRÔNICA NO COMÉRCIO E NO PODER JUDICIÁRIO

2.1 Comércio Eletrônico

Nas últimas duas décadas, tanto nações como empresas, estas de caráter nacional ou multinacional, assistiram a transformações assombrosas.

A conhecida economia tradicional, hoje, é chamada de velha economia para diferenciá-la da nova economia, esta originada daquelas transformações.

No Brasil, em particular, até fins da década de oitenta, as empresas tinham-se habituado a contar com uma proteção governamental, chamada de reserva de mercado, em que determinados itens não eram admitidos na pauta de importações.

A política nacional de abertura às importações e o sucesso inicial das metas de estabilização do Plano Real causaram profundos reflexos no consumo.

Estabilizada a moeda e tendo à sua disposição uma infinidade de artigos estrangeiros, o consumidor brasileiro pôde constatar que os preços que pagava pelos produtos nacionais, em muitos casos, superavam e estavam completamente descasados da realidade mundial.

Aliados a esses fatores, a doutrina da globalização financeira foi angariando mais adeptos e partidários e, via de conseqüência, seus reflexos estenderam-se a todos os cantos do mundo.

Internamente, daí decorreu que boa parte do empresariado nacional viu-se forçado a batalhar pela competitividade de seus produtos.

Cortar custos não bastava. Era preciso buscar a otimização da produtividade e isso só era possível aderindo às novas tecnologias existentes em outras paragens.

Muitas dessas tecnologias eram produtos da assim recém batizada nova economia.

E, dentre elas, a que mais popularizou-se, sem dúvida, foi a Internet.

A Internet foi inicialmente concebida nos EUA exclusivamente para fins militares. Visava desenvolver um instrumento de comunicação para interligar a estrutura militar, de forma ágil, flexível, descentralizada e que não sofresse solução de continuidade, mesmo em caso de destruição parcial de estrutura.

Em seguida, essa tecnologia foi compartilhada pelo meio acadêmico. Nessa segunda fase, inúmeras redes menores de caráter privado foram sendo criadas, multiplicaram-se e, evoluindo, com a interligação entre aquelas redes, surgiu a rede das redes, a famosa Internet – rede mundial de computadores.

A expansão dessa magnitude constituiu a terceira e atual fase, iniciada a partir da última década do século XX. Disseminou-se a Internet entre o homem comum, no mundo todo, graças aos custos inerentes que baixaram sensivelmente e às diversas vantagens oferecidas por tal tecnologia, revolucionando as formas até então conhecidas de comunicação.

Apresenta ela quatro características (Yves Poullet, 1999, apud LORENZETTI, 2001, p. 423):

> “a) É uma rede aberta, visto que qualquer um pode ter acesso a ela;
> b) é interativa, já que o usuário gera dados, navega e estabelece relações;
> c) é internacional, no sentido de que permite superar as barreiras nacionais;
> d) há uma multiplicidade de operadores.”

O número de seus usuários passou de um milhão a quatro milhões de 1994 a 1998. Hoje, quatro anos depois, já são centenas de milhões.

Com a ampla disseminação da Internet no cotidiano das pessoas, abrangendo, dentre outras, as áreas de lazer, arte e cultura, tornou-se inevitável

que fosse ela utilizada para uma finalidade que sempre apeteceu ao homem por nela vislumbrar a possibilidade de gerar lucros: negócios.

De forma natural, inicialmente entre empresas (*business to business, b2b*) e, numa fase subseqüente, entre empresas e consumidores finais, foi expandindo-se esse ágil sistema para o comércio.

Tanto se comerciava bens imateriais (compra de *software*, informação sobre serviços, reserva em hotéis etc.) quanto bens móveis em lojas virtuais.

A despeito de as partes não se fazerem presentes fisicamente e nem se conhecerem, essa modalidade de comércio difundiu-se rapidamente.

Em parte, por causa da comodidade em se adquirir bens não acessíveis na própria cidade do adquirente (discos, livros, informações etc.) e também por serem eles de valores não elevados.

Isso, apesar do inconveniente, para o consumidor, na quase totalidade das vezes, da exigência de que cumprisse primeiramente a sua obrigação de efetuar o pagamento através de cheque, boleto bancário ou cartão de crédito.

Satisfeita a obrigação, só então o vendedor dava início à sua obrigação contratual, remetendo ao adquirente, via *download,* o produto informático ou, no caso de mercadoria física, através do correio, geralmente acrescida de despesa postal.

Esses negócios, portanto, passaram a ser realizados de uma forma nova mediante acordos exclusivamente via Internet, ou seja, num ambiente em que os contratantes não se conhecem, não se vêem, nem podem se assegurar de que a outra parte seja realmente quem diz ser e que adimplirá o convencionado. Inseridos estão na modalidade, sem dúvida, a confiança e o risco.

Foi com a prática, conseqüentemente, que foi construído o arcabouço dessa forma de contratar.

Tratando-se de uma nova modalidade de contrato, o assim chamado comércio eletrônico expandiu-se, na fase inicial, por impulso próprio, com riscos calculados, sem o concomitante aval legislativo, uma vez que quase sempre a reforma legal está descompassada da realidade temporal.

Nesse sentido, "*houve, de início, a assunção, pelos meios comerciais, de um risco calculado para fazer funcionar o sistema, elaborando-se, em seguida, as normas cabíveis*" (WALD, 2001, p. 19).

Porém, esse "risco calculado" não foi assumido apenas pelos meios comerciais, eis que o consumidor também se arrisca quando paga antecipadamente e pode deixar de receber a mercadoria ou, recebendo-a, estar ela em desacordo com prazos e características prometidos.

Como essa prática não poderia evidentemente abranger todas as hipóteses de questões dela decorrentes, com os seus incontáveis desdobramentos, surgiram dúvidas e questionamentos que até então não existiam.

Pondere-se que essa rede cresce sem parar, a uma velocidade ímpar e de forma caótica, e que, sem dúvida, se contém inúmeros atributos positivos, em contrapartida pode ser e é utilizada para fins ilícitos. Levando-se em conta, pois, a magnitude dessa rede, não se poderiam evitar importantes indagações.

Como regulamentar essa rede "sem passaporte" que está atingindo as pessoas nos mais variados pontos do planeta, seja mercê de suas qualidades ou, tal qual uma mitológica Hidra, lançando seus tentáculos em atividades ilícitas?

Contestando autores que propunham que a Internet se regulamentasse por si própria, Lorenzetti (2001, p. 423) é de opinião que essa tese se contradiz quando seus defensores apontam para a necessidade de normas (nacionais ou internacionais?) que proporcionem segurança, tais como "*a assinatura digital, o pagamento eletrônico, a proteção da propriedade intelectual...*". Estariam, pois, aqueles autores, pretendendo a flexibilização absoluta da rede para sua auto-regulamentação mas simultaneamente acoplada à proteção de determinados valores como a segurança, a propriedade e o cumprimento dos contratos.

Realmente, apontou-se, numa etapa posterior, para a necessidade de se regular juridicamente esse instituto.

Outras nações já o fizeram. No Brasil, há a edição de uma medida provisória a respeito de autenticação eletrônica, além de alguns projetos de lei já

encaminhados para análise no Congresso sobre as contratações por meio eletrônico.

A esse respeito será tratado no tópico 5.

2.2 Poder Judiciário

O uso do meio eletrônico, como não poderia deixar de ser, vem sendo adotado gradativamente pelos órgãos do Poder Judiciário visando à disponibilização de uma melhor prestação de justiça aos cidadãos.

Em todas essas inovações – tenham elas a participação de um autor individualmente, como uma petição de advogado ou sentença de juiz monocrático, ou tenham elas conteúdo institucional, como a publicação da jurisprudência dos tribunais –, faz-se mister um elemento que será tratado neste trabalho. Este componente é a assinatura digital, sistemática que, acoplada a qualquer documento eletrônico, possibilita o reconhecimento de determinados requisitos tais como a autoria, a integridade e a autenticidade.

Serão citados, a seguir, alguns exemplos do que está acontecendo. Como é de se crer que iniciativas semelhantes e até mais ousadas estejam sendo praticadas pela maioria dos órgãos ligados ao Poder Judiciário, infere-se que o efeito multiplicador da mistura fervilhante da capacidade criativa e do desejo de aperfeiçoamento superará o tradicionalismo de que se vê impregnado aquele Poder.

É possível, portanto, vislumbrar transformações que inevitavelmente ocorrerão em futuro próximo alcançando resultados que beneficiarão a toda a sociedade.

2.2.1 Execução fiscal eletrônica

Esclarece Nagib Slaibi Filho[1], Juiz de Direito no Rio de Janeiro, que a execução fiscal é processada eletronicamente em alguns aspectos. A inscrição da Dívida Ativa[2] é realizada através de registro em bancos de dados cujo sistema emite as certidões respectivas e as petições iniciais que são assinadas pelos Procuradores.

Prossegue o autor afirmando que, cumprindo as leis estaduais que criaram os Cartórios da Dívida Ativa, também o ajuizamento dos executivos fiscais se faz por meio eletrônico, regulamentado pela Consolidação Normativa da Corregedoria Geral da Justiça do Rio de Janeiro, no art. 2.º [3].

Essa Consolidação Normativa prevê que, proferido o despacho liminar positivo, estará autorizada a citação, a penhora, o arresto, o registro da penhora ou do arresto, e até a avaliação, sendo de se observar que todos esses atos

---

[1] Nagib Slaibi Filho. Execução fiscal virtual. Disponível em: <http://www.teiajuridica.com/af/Execvirt.htm>. Acesso em: 26jun.2002.

[2] Lei n.º 6.830, de 22/09/1980:
"Art. 1.º A execução judicial para cobrança da Dívida Ativa da União, dos Estados, do Distrito Federal, dos Municípios e respectivas autarquias será regida por esta Lei e, subsidiariamente, pelo Código de Processo Civil.
Art. 2.º Constitui Dívida Ativa da Fazenda Pública aquela definida como tributária ou não-tributária na Lei n.º 4.320, de 17 de março de 1964, com as alterações posteriores, que estatui normas gerais de direito financeiro para elaboração e controle dos orçamentos e balanços da União, dos Estados, dos Municípios e do Distrito Federal.
(...)
§ 3.º A inscrição, que se constitui no ato de controle administrativo da legalidade, será feita pelo órgão competente para apurar a liquidez e certeza do crédito e suspenderá a prescrição, para todos os efeitos de direito, por 180 (cento e oitenta) dias ou até a distribuição da execução fiscal, se esta ocorrer antes de findo aquele prazo."

[3] "... § 2º - A distribuição de execuções fiscais através do sistema de processamento eletrônico de dados observará o seguinte:
a) o exeqüente relacionará as execuções, de idêntico teor, por Vara e Ofício, se houver, numerando-as em ordem crescente, por número de inscrição, em três vias, mantida a numeração para o tombamento;
b) o registro de distribuição será lançado na própria relação, arquivando-se a primeira via no cartório de registro de distribuição e outra na escrivania; devolver-se-á a terceira ao exeqüente, como recibo;
c) o exeqüente encaminhará a petição inicial e os documentos que a instruem à escrivania somente após a distribuição e a expedição da relação referida na alínea ‘‘a’’;
d) a petição inicial indicará o número que a identifica na relação respectiva".

processuais são impulsionados pelo exeqüente, que emite as cartas de citação, diligencia para a penhora, seu registro e a avaliação[4].

De sua parte, o contribuinte, ao receber a citação, faz o pagamento junto à repartição fazendária (e não junto ao cartório), através de guia emitida pelo sistema compreendendo o principal e os acessórios da dívida ativa, inclusive o pagamento de custas e demais despesas forenses.

O banco arrecadador separa a receita para a repartição fiscal e as custas para o Poder Judiciário.

Prossegue Slaibi esclarecendo que:

> "... o sistema emite diariamente as relações das guias pagas pelos contribuintes, sendo uma delas remetida para o Cartório, prolatando-se sentença conjunta para todas as execuções.
> (...)
> As execuções fiscais em suporte de papel não são autuadas, salvo quando novamente submetidas a despacho judicial quando suscitados incidentes como a exceção de pré-executividade ou após a avaliação, para fins de realização do leilão, ou quando estão apensas aos respectivos embargos à execução."

É plenamente visível a contribuição que essa sistemática traz para a celeridade processual, sendo passível de mais avanços e estando a servir de exemplo para outras medidas.

2.2.2 Diário da Justiça eletrônico

O STJ anunciou em 22/05/2002 que foi criado um grupo especial para estudar mudanças nos Códigos de Processo Civil e Penal a fim de viabilizar a publicação on line no DIÁRIO DA JUSTIÇA ELETRÔNICO[5].

Assim, sentenças, acórdãos e decisões de juízes, desembargadores e ministros do Poder Judiciário surtirão efeitos no exato instante em que forem incluídas, via on line, nos sites dos tribunais.

---

[4] Neste sentido, a Súmula nº 190, do Superior Tribunal de Justiça: "na execução fiscal processada perante a Justiça Estadual, cumpre à Fazenda Pública antecipar o numerário destinado ao custeio das despesas com o transporte dos oficiais de justiça."

[5] Notícias do Superior Tribunal de Justiça. 22/05/2002 - Nilson Naves: decisões do Judiciário serão publicadas on line no Diário da Justiça eletrônico. Disponível em: <http://www.stj.gov.br/webstj/noticias/Default.asp>. Acesso em 11jun.2002.

Por conseguinte, a contagem dos prazos se fará a partir do momento do registro junto ao sistema.

Disso decorre a necessidade de se proceder a alterações nos Códigos Processuais, pois, tecnicamente, conforme afirmado, o sistema é passível de ser posto em prática.

Conclui-se que a medida contribuiria para a redução das custas judiciais e agilização dos processos.

2.2.3 Revista Eletrônica da Jurisprudência do STJ

Em 18/06/2002, o STJ anunciou o lançamento, para 1.º de setembro de 2002, da REVISTA ELETRÔNICA DA JURISPRUDÊNCIA DO STJ[6].

Será disponibilizado, no site do STJ, o inteiro teor de todos os acórdãos do Tribunal, em página certificada em formato texto.

Fica possibilitado aos profissionais do Direito ou a quaisquer cidadãos, através da Internet, extrair cópias das decisões colegiadas.

Tais cópias poderão ser diretamente utilizadas em processos pois estarão autenticadas pelo Tribunal.

Essa medida também servirá para agilizar e baixar os custos das ações judiciais.

2.2.4 Penhora on line na Justiça Trabalhista

A partir de junho de 2002, a Justiça Trabalhista passou a contar com o sistema de penhora on line, tornando mais ágil a execução de sentenças[7].

---

[6] Notícias do Superior Tribunal de Justiça. 18/06/2002 - STJ cria Revista Eletrônica de Jurisprudência permitindo ao cidadão economia de tempo e dinheiro. Disponível em: <http://www.stj.gov.br/webstj/noticias/Default.asp>. Acesso em: 25jun.2002.

[7] Justiça Trabalhista inaugura sistema on line de Penhora. Consultor Jurídico - 30/05/2002. Disponível em: <http://cf6.uol.com.br/consultor/view.cfm?id=10784&ad=b>. Acesso em: 27jun.2002.

Através de convênio firmando entre o Tribunal Superior do Trabalho e o Banco Central do Brasil, o magistrado de primeiro grau obterá do BACEN, via on line, informações sobre a existência de valores em contas correntes ou aplicações financeiras, em nome de empregadores executados, em qualquer instituição financeira no País.

De posse desses dados, poderá determinar o bloqueio da quantia necessária para garantir a execução da sentença.

O sistema elevará a credibilidade da Justiça do Trabalho na medida em que possibilitará a efetividade das execuções trabalhistas. As ordens de bloqueio, antes realizadas por via postal e cujo cumprimento demorava cerca de 60 dias, agora passam a ser executadas em 24 ou 48 horas.

É permitido concluir-se que, se a metodologia tem aplicabilidade na Justiça do Trabalho, seria perfeitamente extensível para os outros ramos do Judiciário.

2.2.5 *E-justitia*

Em seminário realizado em 14/05/2002, o presidente do Tribunal de Justiça do Estado de São Paulo anunciou que o Poder Judiciário do Estado estará totalmente informatizado até o final de 2003.[8]

Dentre as inovações, será oferecido um serviço chamado *"e-justitia"* a advogados e demais profissionais do Direito, possibilitando aos usuários previamente cadastrados receber, diariamente, via e-mail, informações sobre a data e edição do Diário Oficial além da origem da matéria onde foi publicada determinada palavra, ou combinação de palavras, determinadas pelo assinante.

---

[8] Fonte: Diário Oficial de São Paulo, edição de 15/05/2002. Disponível em: <http://www.certisign.com.br/imprensa/2002/05152002.html>. Acesso em: 13jul.2002.

2.2.6 Transmissão de peças processuais - Projeto de Lei n.º 5.828/01

Em 11/06/2002, a Comissão de Constituição e Justiça e de Redação da Câmara dos Deputados aprovou o Projeto de Lei n.º 5.828/01, proposto pela Associação dos Juízes Federais do Brasil (Ajufe), que autoriza o uso de correio eletrônico na transmissão de peças processuais como petições, recursos e cartas precatórias[9].

Em 19/6/2002, o Plenário da Câmara aprovou o Projeto de Lei. A matéria seguiu para o Senado.

Pelo Projeto de Lei, será admitido o uso de meio eletrônico na comunicação de atos e a transmissão de peças processuais, aplicando-se indistintamente aos processos civil, penal e trabalhista e em todos os graus de jurisdição.

Uma grande inovação consiste na dispensa da apresentação dos respectivos documentos originais. Relativamente ao termo “original”, no decorrer deste trabalho, ver-se-á que um documento eletrônico, assinado digitalmente conforme diretrizes da Medida Provisória 2.200-2/01, é considerado documento original. Não faz sentido, portanto, a exigência ou dispensa da apresentação, em objeto “papel”, de um documento original só porque firmado eletronicamente.

Haverá a necessidade de os advogados credenciarem-se junto aos órgãos do Poder Judiciário, mediante procedimento que assegure o sigilo, a identificação e a autenticidade de suas comunicações. Nesse aspecto, há crítica da OAB/SP pleiteando a hegemonia no cadastramento de advogados.

De nossa parte, a posição da OAB/SP seria defensável se ela credenciasse seus membros a partir de chaves públicas oriundas de AC Raiz definida em lei. Ou seja, propomos que todo profissional do Direito, sem exceção, seja cadastrado no órgão ao qual se ache institucionalmente vinculado. O importante é que todas essas instituições (Tribunais, OAB, Ministério Público) vinculem-se à mesma Autoridade Certificadora Raiz, ou seja, o Instituto Nacional

---

[9] Câmara aprova transmissão de peças processuais pela Internet. Consultor Jurídico. 11/06/2002. Disponível em: <http://cf6.uol.com.br/consultor/view.cfm?id=11009&ad=b>. Acesso em 26jun.2002.

de Tecnologia da Informação - ITI, em consonância com o estabelecido na Medida Provisória n.º 2.200-2/01, que será tratada adiante, no tópico 5.

Voltando ao Projeto de Lei, o envio de petições, de recursos e demais peças processuais por meio eletrônico considerar-se-á realizado no dia e hora do seu recebimento pelo provedor do Judiciário.

A publicação de atos e de comunicações processuais poderá ser efetuada por meio eletrônico e considerada como data da publicação a da disponibilização dos dados no sistema eletrônico para consulta externa.

Os prazos processuais terão início no primeiro dia útil seguinte ao da publicação.

A intimação pessoal poderá ser feita, para as partes previamente cadastradas, através de correio eletrônico com aviso de recebimento eletrônico.

As cartas precatórias, de ordem e, de um modo geral, todas as comunicações oficiais que transitem entre órgãos do Poder Judiciário, bem assim entre os deste e dos demais poderes, far-se-ão preferencialmente por meio eletrônico.

Diz o art. 8.º, do Projeto de Lei, que os órgãos do Poder Judiciário poderão desenvolver sistemas de comunicação de dados, com distribuição de programa de acesso aos cadastrados, que será de uso obrigatório nas comunicações eletrônicas de que cuida essa lei.

Seu parágrafo único especifica os requisitos do sistema:

a) Aviso automático de recebimento e abertura das mensagens.
b) Numeração automática ou outro mecanismo que assegure a integridade do texto.
c) Protocolo eletrônico das mensagens transmitidas, especificando data e horário.
d) Visualização do arquivo para confirmação de seu teor e forma antes do envio.
e) Proteção dos textos transmitidos, obstando alterações dos arquivos recebidos.
f) Armazenamento por meio eletrônico dos atos praticados, bem como dos acessos efetuados na forma da presente lei.

Dentre os exemplos ora coletados, indubitavelmente, essa medida é a que tem mais possibilidades de imprimir maior celeridade à prestação da justiça.

3 DOCUMENTO ELETRÔNICO E CONTRATO ELETRÔNICO

3.1 Histórico

O nosso Código Comercial antecedeu o Código Civil de 1916 em quase sete décadas, criando uma situação *sui generis*, na qual a lei especial surgiu antes da lei geral.

Embora tenha sofrido inúmeras mudanças em virtude de normas estabelecidas no Código Civil, as suas regras de caráter geral continuam em vigor uma vez que lei geral não derroga lei especial.

Até há pouco mais de uma década, o que estava então estabelecido na legislação e doutrina relativamente a dois institutos muito utilizados no meio comercial − o documento e o contrato − era suficiente para normalizar a operacionalização dos negócios. Veja-se, pois, o que existia em nosso ordenamento:

3.2 Documento

Será abordado inicialmente o documento, reproduzindo-se, a seguir, conceitos de autoria de diversos doutrinadores, coletados por Diniz (1999, p.12-14):

Para Marco Aurélio S. Viana (1993) *“a declaração de vontade pode ser reduzida a escrito, perpetuando-se em um instrumento público ou privado. O documento ou instrumento é o veículo em que se materializam graficamente as palavras que expressam a vontade das partes”*.

Segundo Ulderico Pires dos Santos (1994, p. 3), *"documento, sabe-se, é declaração escrita e assinada de caráter informativo destinada a servir de prova das assertivas encontradas em seu conteúdo"*.

Caio Mário da Silva Pereira (1996) diz que *"a mais nobre das provas é a documental. Por via do escrito perpetua-se o ato, enunciando-se a declaração de vontade de modo a não depender sua reconstituição da falibilidade de fatores precários".*

De acordo com Ovídio A. Baptista da Silva (1991):

> "Sempre que se faz alusão a documento, ou, em direito processual, a prova documental, em geral se imagina que estas categorias de direito probatório equivalham ao conceito de prova literal (*littera*, a letra, aquilo que está escrito). O conceito de documento, todavia, é bem mais amplo, abrangendo outras formas de representação além das formas gráficas ou simplesmente literais".

De outra parte, um outro autor, Lucca (2001, p. 43), traz as lições de dois mestres italianos.

O primeiro deles, Francesco Carnelutti (1938, p. 105-6), disse que documento é *"meio real de representação gráfica do fato"* e, o segundo, Giuseppe Chiovenda (1965, p. 127), que é *"toda representação material destinada a reproduzir determinada manifestação do pensamento"*.

Finalmente, tanto Diniz (1999, p. 12-14) quanto Lucca (2001, p. 43) trazem a reafirmação posterior de Francesco Carnelutti (1947) de que *"o documento não é somente uma coisa, mas uma coisa representativa, ou seja, capaz de representar um fato"*, e acrescentam a definição de Paolo Guidi (1950, p. 46):

> "O documento é um objeto corpóreo, produto da atividade humana da qual conserva os traços, o qual, por intermédio da percepção dos sinais sobre ele impressos, ou das luzes ou sons que possa fornecer, é capaz de representar, de modo permanente, a quem o observa, um fato exterior a esse documento".

Dos conceitos citados, de diferentes autores e de épocas diversas, pode-se extrair que, juridicamente, o documento:

a) Deve ter a capacidade de representar um fato jurídico relevante. Esse fato deve ser decorrente do trabalho humano. O objeto dessa representação deve

ter a capacidade de guardá-la pelo tempo necessário a se prestar numa eventual futura prova.

b) Pode ser de caráter público ou particular.

c) Além da forma escrita, pode fazer-se representar por sons, símbolos, imagens.

A propósito, Diniz (1999, p. 16) afirma que, conceitualmente, o documento se constitui de três elementos básicos:

a) Continente: é um suporte corpóreo que contém a representação. Nesse sentido, documento é coisa corpórea, passível de posse, é único e não é fungível.

b) Conteúdo: é a representação idônea de um fato jurídico, a manutenção de sua integridade referente aos atos ou fatos jurídicos que documentar, não podendo ser confundido com a veracidade do conteúdo do documento mas sim com a sua capacidade de perenizar a representação dos fatos aos quais aludem o seu conteúdo.

c) Autoria do documento: da determinação da autoria decorrem conseqüências jurídicas, as quais podem tanto gerar a produção de efeitos lícitos quanto à responsabilização pela prática de atos ilícitos.

3.3 Contrato

Em segundo lugar, será analisado o instituto denominado contrato.

RODRIGUES (1986, p. 9) ensina que, do gênero negócio jurídico, existe uma espécie que é o contrato, dependente da conjunção da vontade de duas ou mais partes. E, prosseguindo, insere a definição de Clóvis Beviláqua (1950): *"o contrato é o acordo de vontades para o fim de adquirir, resguardar, modificar ou extinguir direitos".*

Em nosso ordenamento jurídico, antes da expansão do comércio eletrônico, existiam normas legais que tratavam:

a) Da forma de contratação e eventual exigência de solenidades especiais (arts. 129, 134 e 1.079 do Código Civil[10] e art. 124 do Código Comercial[11]).

b) Da assinatura (art. 131 do Código Civil[12]).

c) Dos documentos públicos (art. 134 do Código Civil[13]) e particular (art. 135 do Código Civil[14], art. 122 do Código Comercial[15] e art. 385 do Código de Processo Civil[16]).

d) Se os contratos podiam ser verbais, por escrito (art. 126 do Código Comercial) ou por correspondência/entre ausentes (art. 127 do Código Comercial).[17]

---

[10] Art. 129. A validade das declarações de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir (art. 82).
Art. 134. É, outrossim, da substância do ato a escritura pública:
I – nos pactos antenupciais e nas adoções;
II – nos contratos constitutivos ou translativos de direitos reais sobre imóveis de valor superior a Cr$ 50.000 (cinqüenta mil cruzeiros), excetuado o penhor agrícola.
Art. 1.079. A manifestação da vontade, nos contratos, pode ser tácita, quando a lei não exigir que seja expressa.

[11] Art. 124. Aqueles contratos para os quais neste Código se estabelecem formas e solenidades particulares não produzirão ação em juízo comercial, se as mesmas formas e solenidades não tiverem sido observadas.

[12] Art. 131. As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários.

[13] Art. 134. É, outrossim, da substância do ato a escritura pública:
I – nos pactos antenupciais e nas adoções;
II – nos contratos constitutivos ou translativos de direitos reais sobre imóveis de valor superior a Cr$ 50.000 (cinqüenta mil cruzeiros), excetuado o penhor agrícola.

[14] Art. 135. O instrumento particular, feito e assinado, ou somente assinado por quem esteja na disposição e administração livre de seus bens, sendo subscrito por 2 (duas) testemunhas, prova as obrigações convencionais de qualquer valor. Mas os seus efeitos, bem como os da cessão, não se operam, a respeito de terceiros (art. 1.067), antes de transcrito no Registro Público.
Parágrafo único. A prova do instrumento particular pode suprir-se pelas outras de caráter legal.

[15] Art. 122. Os contratos comerciais podem provar-se:
1. por escrituras públicas;
2. por escritos particulares;
3. pelas notas dos corretores, e por certidões extraídas dos seus protocolos;
4. por correspondência epistolar;
5. pelos livros dos comerciantes;
6. por testemunhas.

[16] Art. 385. A cópia de documento particular tem o mesmo valor probante que o original, cabendo ao escrivão, intimadas as partes, proceder à conferência e certificar a conformidade entre a cópia e o original.
§ 1.º Quando se tratar de fotografia, esta terá de ser acompanhada do respectivo negativo.
§ 2.º Se a prova for uma fotografia publicada em jornal, exigir-se-ão o original e o negativo.

[17] Art. 126. Os contratos mercantis são obrigatórios; tanto que as partes se acordam sobre o objeto da convenção, e os reduzem a escrito, nos casos em que esta prova é necessária.
Art. 127. Os contratos tratados por correspondência epistolar reputam-se concluídos e obrigatórios desde que o que recebe a proposição expede carta de resposta, aceitando o contrato proposto sem condição nem reserva;

e) Como fazer prova do acordado, em ocorrendo dúvida (arts. 131 "caput" e parágrafo único, 136 a 138 do Código Civil[18], arts. 122, 123 e 126 do Código Comercial[19] e arts. 385 e 401 do Código de Processo Civil[20]).

Da leitura dessas normas, ainda vigentes, há que se concluir que:

a) Somente se exigido expressamente por lei, tornar-se-á obrigatório o instrumento público (ex.: escritura de compra e venda de imóveis), a forma

---

até este ponto é livre retratar a proposta; salvo se o que a fez se houver comprometido a esperar resposta, e a não dispor do objeto do contrato senão depois de rejeitada a sua proposição, ou até que decorra o prazo determinado.
Se a aceitação for condicional, tornar-se-á obrigatória desde que o primeiro proponente avisar que se conforma com a condição.

[18] Art. 131. 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.
Art. 136. Os atos jurídicos, a que se não impõe forma especial, poderão provar-se mediante:
I - confissão;
II - atos processados em juízo;
III - documentos públicos ou particulares;
IV - testemunhas;
V - presunção;
VI – exames e vistorias;
VII – arbitramento.
Art. 137. Farão a mesma prova que os originais as certidões textuais de qualquer peça judicial, do protocolo das audiências, ou de outro qualquer livro, a cargo do escrivão, sendo extraídas por ele, ou sob a sua vigilância, e por ele subscritas, assim como os traslados de autos, quando por outro escrivão concertados.
Art. 138. Terão também a mesma força probante os traslados e as certidões extraídas por oficial público, de instrumentos ou documentos lançados em suas notas.

[19] Art. 122. Os contratos comerciais podem provar-se:
1. por escrituras públicas;
2. por escritos particulares;
3. pelas notas dos corretores, e por certidões extraídas dos seus protocolos;
4. por correspondência epistolar;
5. pelos livros dos comerciantes;
6. por testemunhas.
Art. 123. A prova de testemunhas, fora dos casos expressamente declarados neste Código, só é admissível em juízo comercial nos contratos cujo valor não exceder a quatrocentos mil réis.
Em transações de maior quantia, a prova testemunhal somente será admitida como subsidiária de outras provas por escrito.
Art. 126. Os contratos mercantis são obrigatórios; tanto que as partes se acordam sobre o objeto da convenção, e os reduzem a escrito, nos casos em que esta prova é necessária.

[20] Art. 385. A cópia de documento particular tem o mesmo valor probante que o original, cabendo ao escrivão, intimadas as partes, proceder à conferência e certificar a conformidade entre a cópia e o original.
§ 1.º Quando se tratar de fotografia, esta terá de ser acompanhada do respectivo negativo.
§ 2.º Se a prova for uma fotografia publicada em jornal, exigir-se-ão o original e o negativo.
Art. 401. A prova exclusivamente testemunhal só se admite nos contratos cujo valor não exceda o décuplo do maior salário mínimo vigente no país, ao tempo em que foram celebrados.

especial (ex.: testamento particular) ou solenidades especiais (ex.: casamento).

b) Em contratos de valor acima de dez salários mínimos não basta a prova exclusivamente testemunhal. Esta é de natureza subsidiária. Via de regra, o contrato escrito faz prova considerada *juris tantum*.

c) Como regra geral, os Códigos Civil e Comercial não dispensam a forma escrita para a celebração de contratos.

De um outro ângulo de visão, analisando a legislação vigente e o contrato eletrônico, Wald (2001, p. 24) registra que *"em tese e salvo interpretação construtiva dos tribunais, não há, pois, no momento, como equiparar a prova eletrônica à prova escrita"*.

E continua esse autor asseverando que os tribunais consideram a regulamentação probatória norma cogente, de ordem pública, e nem sempre aceitam contratos eletrônicos como prova, mesmo quando as partes firmem contrato escrito admitindo determinadas formas de prova eletrônica.

Numa opinião divergente, (DINIZ, 1999, p. 41-44) afirma que o julgador pode atribuir a um arquivo digital os efeitos de um documento particular, desde que, nessa espécie, a lei não exija requisitos formais. Em havendo, pois, liberdade de forma, será bastante a comunicação da proposta e da aceitação entre contraentes capazes e legítimos para a perfeição dos contratos digitais lícitos. Finaliza o autor ponderando que, se:

> "... o problema central é o reconhecimento da autoria e integridade de conteúdo das declarações de vontade que convergem para o negócio, a tecnologia das assinaturas digitais cai como uma luva para permitir que os arquivos digitais sejam um meio de prova destas declarações. (...) Ela permite meios diretos de prova dos contratos entre ausentes celebrados por mensagens enviadas em arquivos digitais".

Conclui-se que, se aplicada a assinatura digital ao documento, o contrato eletrônico tornar-se-á perfeitamente apto a servir de prova entre as partes.

3.4 Documento Eletrônico e Contrato Eletrônico

Portanto, já a partir do último qüinqüênio, a situação tornara-se mais complexa. Com o crescimento das contratações através de meio eletrônico, surgiram dúvidas e questionamentos.

Necessário se faz abrir um parênteses para definir alguns termos como computadores, programas de computador, telemática e arquivo digital.

Para Diniz (1999, p. 20), computadores são *"máquinas hábeis para realizar tarefas respondendo a instruções (comandos) que possam ser previamente organizadas em um arquivo (programa)".* Esse autor prossegue explicando que, ao combinarem os bits por equações matemáticas, os computadores proporcionam a simulação de eventos, tais como a representação de letras, sons, figuras, imagens e outros sinais.

Sobre programas, Lucca (2001, p. 47) ensina que:

> "Programas de computador são aqueles comandos escritos em determinada linguagem de máquina que ministram instruções ao equipamento eletrônico para a realização de tarefas das mais diversas modalidades. Exemplo: sistemas operacionais (Windows, Linux etc.), processadores de texto (Word, Starwriter etc.), planilhas de cálculo (Excel, Lotus123 etc.) e navegadores de Internet (Internet Explorer, Netscape Navigator etc.)".

Telemática é a conjugação da tecnologia de telecomunicação com a informática.

A respeito de arquivo digital, é definido como uma coleção finita de informações digitalizadas à qual se atribui um nome (DINIZ, 1999, p. 21).

Conforme esse mesmo autor (1999, p. 20), para redigir um texto, envia-se, através dos teclados, sinais digitais que são lidos e reconhecidos por inúmeros programas que se acham incorporados a um processador de textos. Simultaneamente, aqueles sinais digitalizados são transformados no monitor em símbolos inteligíveis aos nossos sentidos, como letras, e armazenados em um arquivo, que tanto pode ser gravado em meio magnético (um disco fixo ou um disquete) como também enviado para um dispositivo de impressão (impressora) ou de telecomunicação (modem).

O que seriam, por conseguinte, documento eletrônico e contrato eletrônico?

Existem diversas formas de enxergar esses institutos.

Inicialmente, será apresentada a definição de Miguel Angel Moreno Navarrete (1999, p. 35), citado por TUCCI (2001, p. 275):

> "Na verdade, o que afasta o contrato tradicional de um contrato eletrônico, sob a perspectiva estrutural, é apenas a formação do mesmo, quanto ao modo de manifestação do consentimento e de aperfeiçoamento do negócio, bem como de sua respectiva prova, tanto judicial ou extrajudicial. Em suma: desde que comprovadas a proposta e a aceitação, o negócio via Internet, em princípio, não só existe, como desponta válido e eficaz".

Queiroz (2001, p. 380-83), primeiramente, define documento eletrônico *"como aquele que foi gerado ou arquivado por sistema computadorizado, em meio digital"*. Em segundo lugar, aponta, assim como os demais autores, como pontos críticos desse tipo de documento o da comprovação da identidade das partes, tanto na autoria quanto na aceitação, e o da prova do seu conteúdo e da sua integridade.

Prossegue, tratando da preocupação que suscita o fenômeno da desmaterialização do documento.

A explicação técnica é a de que, assim como o documento tradicional se compõe de escrito com pigmento de tinta sobre objeto corpóreo denominado papel, o documento digital nada mais é do que uma representação por códigos binários[21] guardados magneticamente em suporte até então não convencional, o disquete ou o disco rígido de computador. O documento continua disponível, acessível e inteligível. É uma simples substituição de um suporte clássico por um magnético.

Todavia, para Queiroz, o problema quanto à desmaterialização emerge pela facilidade com que códigos binários podem ser manipulados, transmitidos, copiados ou modificados, sem limite de vezes, sem resultar em perda de

[21] Códigos binários, ou bits, são códigos em linguagem própria de que se valem os computadores para realizar todo e qualquer tipo de operação, especialmente as representações gráficas dos documentos digitais. Após interpretados os bits, o computador pode lidar com imagens, sons e vídeos.

qualidade e sem deixar mínimos vestígios dessas operações, sejam elas de boa ou de má-fé e sejam elas efetuadas pelo possuidor do documento ou por terceiro que porventura tenha interceptado a citada mensagem eletrônica quando de sua transmissão.

Daí concluir esse autor asseverando que a insegurança de um documento digital não lhe permite conferir força probatória sem a utilização de uma adequada tecnologia de segurança.

Em terceiro lugar, Wald (2001, p. 18) cita Olivier Iteanu (1996, p. 23) que definiu contrato eletrônico como sendo *"o encontro de uma oferta de bens ou serviços que se exprime de modo audiovisual através de uma rede de telecomunicações e de uma aceitação suscetível de manifestar-se por meio de interatividade".*

De outra parte, Lucca (2001, p. 46-47) dá o conceito de Semy Glanz ("Internet e Contrato Eletrônico", in Revista dos Tribunais, v. 757, nov. 1998, p. 72):

> "Contrato eletrônico é aquele celebrado por meio de programas de computador ou aparelhos com tais programas.
>
> Dispensam assinatura ou exigem assinatura codificada ou senha.
>
> A segurança de tais contratos vem sendo desenvolvida por processos de codificação secreta, chamados de criptologia ou encriptação".

Em prosseguimento, afirma não ver diferença ontológica de relevo em se usar as expressões "contrato eletrônico" ou "contrato informático" para designar o contrato celebrado através de meio eletrônico. Parece aceitar igualmente o termo "contrato telemático" que significa a conjugação da informática com a telecomunicação.

3.5 O "Tradicional" e o Eletrônico

Diante do anteriormente exposto, tanto nos aspectos legais quanto nos doutrinários, sobre documento e contrato e a nova modalidade de contratação, sob forma eletrônica, surge a indagação se os arquivos digitais teriam as características do documento tradicional.

A resposta é que, devido à facilidade para se manipular um documento digital sem deixar rastros identificáveis, nele não se vislumbram, por si só, as características da autoria, da singularidade e da integridade do conteúdo. Essa carência pode ser suprida com sinais de identificação, em forma digital, que conferem segurança ao documento digital, sendo o principal método hoje em uso o da criptografia (DINIZ, 1999, p. 26-28).

Um outro autor (LUCCA, 2001, p. 46) afirma que o contrato eletrônico não é um novo tipo no âmbito da teoria geral dos contratos. Exemplifica que contratos, independentes da forma, serão sempre de compra e venda, ou de prestação de serviço, ou de locação de coisa.

De nossa parte, diante dos conceitos examinados no tópico anterior e se imaginarmos a informática chegando aos nossos tribunais e tabelionatos, constataremos que entre documento *lato sensu* e documento eletrônico existem muitas semelhanças e poucas diferenças.

3.5.1 Diferenças

Quanto às diferenças, necessário se faz tecer algumas considerações com referência aos quesitos autoria e integridade e objeto.

No primeiro quesito, o documento eletrônico deve possibilitar fazer prova irrefutável de autoria e integridade. Tal documento deve ter recursos que lhe permitam a capacidade de manutenção perene, íntegra e imodificável de suas características originais. Tudo isso será possível com o uso da assinatura digital, como será visto mais adiante no subtópico “4.5.2 – Assinatura digital”.

Quanto ao objeto, não carece, por parte do legislador, de especificar o suporte corpóreo para representar os fatos relevantes. Desde tempos remotos, já existiram documentos representados tanto em pedra, tábua e papiro quanto em papel, microfilme, fita magnética ou fotografia. Sabe-se, hoje, que o documento eletrônico é passível de representação no disco rígido de um computador, num CD, disquete ou no velho e conhecido papel, porém ignora-se o que o futuro nos reserva em termos de representação de documentos.

Conclui-se que não há necessidade de regulamentação legal de documento eletrônico e contrato eletrônico, independentemente de serem considerados novos gêneros ou meramente espécies de institutos atualmente existentes.

Regulamentá-los significaria, certamente, sujeitar-se ao risco de ter de atualizar a norma legal periodicamente porque a tecnologia avança vertiginosa e irrefreavelmente, acarretando transformações atualmente inconcebíveis. Convém, portanto, atuar-se com cautela e contentar-se com os conceitos *lato sensu*, estes sim mais sábios e perenes.

Porém, pela insegurança que geram no mundo jurídico quanto à forma de sua constituição, devia-se estabelecer – legalmente – a forma de validar seu uso como meio probatório.

No nosso entender, atingiu-se esse objetivo com a edição da Medida Provisória n.º 2.200-2, de 24/08/2001, que estabeleceu a forma legal para a aplicação da assinatura digital (vide tópico 5). Esta MP, não revogada explicitamente pelo Congresso Nacional, a contrário senso, adquiriu vigência plena, de acordo com o art. 2.º da Emenda Constitucional n.º 32, de 11/09/2001[22].

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

4 SEGURANÇA JURÍDICA NA MANIFESTAÇÃO DA VONTADE POR MEIO ELETRÔNICO

4.1 A Prova

No Capítulo VI, Título VIII, Livro I, do Código de Processo Civil, o legislador estabeleceu extenso rol de meios legais de prova. Não obstante, além desses, permite outros inominados, desde que “moralmente legítimos” (art. 332).[23]

Desse modo, para demonstrar a verdade do que diz, a parte deve apresentar provas. Porém, seu interesse não atinge a plenitude unicamente com a apresentação de uma prova legal ou moralmente legítima. É preciso que o juiz se convença da verdade do fato alegado.

A força probante de livros comerciais, por exemplo, a princípio privilégio de banqueiros, estendeu-se, desde a Idade Média, aos comerciantes. Os livros são a consciência dos comerciantes e o repositório de provas de inestimável valor. Mas, se os lançamentos efetuados nos livros fazem plena prova contra o comerciante que os registrou, necessitará ele de documentos adicionais para fazer prova contra terceiros (REQUIÃO, 1998, p. 161-62).

Do mesmo modo, observa-se na prova processual a existência de duas finalidades: uma objetiva, o instrumento em si para demonstrar a existência de um fato, a verdade do que se alega, e, outra subjetiva, a convicção que se forma no espírito do julgador após a produção da prova (THEODORO JÚNIOR, 2000, p. 367-68).

4.2 A Aceitação dos Arquivos Digitais como Prova

Seja nos códigos, seja na doutrina ou na jurisprudência, há concordância com os pontos básicos ligados à questão dos institutos documento e contrato, tais como os relativos à diferenciação entre documento público e particular, à forma e natureza de constituição, à possibilidade de autenticação da assinatura pelo tabelião, à exigência, ou não, de registro em cartório, e ao meio de prova nos tribunais.

Já no que concerne aos contratos celebrados por meio eletrônico, como dito acima, surgiram alguns questionamentos dentre os quais destacam-se os principais: identificação das partes, autenticidade das assinaturas, impossibilidade de repúdio pelo autor e integridade do contrato celebrado através de bits.

Sendo a Internet um meio de comunicação tecnicamente qualificado como inseguro, em que as partes não se conhecem, não existindo garantia recíproca de identidade das partes, e em que o contrato é celebrado através de bits, como fazer prova em juízo da identidade da outra parte ou de que ela realmente expressou a sua concordância em assumir tudo que estava especificado no contrato eletrônico?

Darão margem a discussão quanto à sua validade jurídica os documentos eletrônicos perpetrados sem a observância da autenticação da assinatura digital por parte de autoridades certificadoras. E por serem frágeis, poderão não ser aceitos como prova em tribunais.

Tome-se como exemplo o boleto bancário.

À semelhança da *Lettre de Change-Relevé* - LCR[24], utilizado na França, o boleto bancário é amplamente empregado pelo sistema bancário nacional.

---

[23] Art. 332. 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.

[24] Instituto do direito francês, criado em 1973, para facilitar a circulação de créditos comerciais, consubstanciando-se em um título que pode existir tanto em papel, como em forma eletrônica. As ordens de pagamento são digitalizadas e armazenadas em fitas magnéticas que circulam entre instituições bancárias representando créditos negociáveis, passíveis de cessão, a serem liquidadas mediante o saque da quantia da

Esses dois institutos, dada a sua circulabilidade exclusiva por meio eletrônico, no caso francês, ou da substituição do título de crédito pelo boleto bancário, no caso brasileiro, transitando eletronicamente após sua liquidação, não admitem a possibilidade da prática de atos comuns aos mais conhecidos títulos de crédito, tais como o aceite e o aval. Estes se tornam materialmente impossíveis de serem realizados. Quanto ao protesto, esse é impossível de ser efetivado no caso da LCR e, na hipótese do boleto bancário, faz-se o protesto por indicação, criatividade dos costumes pátrios que, se agilizam os procedimentos negociais, acabam por, pelo menos parcialmente, descaracterizar a cartularidade inerente aos títulos de crédito.

Em ocorrendo a retirada da corporalidade de um título de crédito substituindo-a por bits eletrônicos, como no exemplo citado acima, fazia-se oportuna a manifestação do legislador definindo se um documento, particular ou público, tem valor jurídico sem que esteja representado em um objeto corpóreo, seja este pedra, tábua, papiro, papel, microficha, filme fotográfico, fita de vídeo, arquivo digital, ou quaisquer outros que vierem a ser obtidos com o avanço da tecnologia.

Especificamente quanto à forma dos atos jurídicos, se a lei prevê forma especial (instrumentos corpóreos, conseqüentemente, escritos, sejam particulares ou públicos) não haveria a possibilidade de os arquivos digitais fazerem prova em juízo.

De outro ângulo de visão, considerando que a lei possibilita a apresentação de provas consideradas atípicas, inominadas, não há necessidade de os arquivos digitais, para serem aceitos como prova, serem enquadrados expressamente na categoria de documentos. Todavia, caracteriza-se, no caso, que esses arquivos digitais estarão providos de fragilidade.

Para que fossem reconhecidos como documentos, fazia-se mister que, por meio de legislação específica, fossem agregados a tais arquivos digitais, recursos

---

conta-corrente do devedor e o correlato depósito na de seu titular, quando da data do vencimento. (DINIZ, 1999, p. 47-48). Para mais detalhes sobre a LCR e a duplicata escritural vide ainda Lucca (2001, p. 38-44).

que possibilitassem a determinação do agente-autor, bem como uma forma de impedir a negação de autoria e a má-fé, mantendo sua perenidade e integridade.

Tal meta foi alcançada com a edição da Medida Provisória n.º 2200-2, de 24/08/2001 (vide tópico 5, adiante), que adotou a metodologia da criptografia assimétrica, também chamada de criptografia de chave pública *(public key)*.

Não tendo a legislação de até então estabelecido forma especial, seriam plenamente aceitáveis em tribunais arquivos digitais autenticados por tabeliães digitais ou por entidades de certificação privada, a critério do magistrado.

Ora, se a lei não estabelece requisitos especiais de forma, isto é, havendo liberdade de forma e não exigência de solenidades especiais, as mensagens trocadas – mediante o uso de assinaturas digitais – entre contraentes capazes e legítimos vinculam os respectivos policitantes e oblatos, podendo ser exibidas como prova em tribunais, já que tanto autoria quanto integridade estarão comprovadas.

Poder-se-ia, então, deduzir que, tecnicamente, um texto com assinatura eletrônica validada por autoridade certificadora pública (tabelião virtual) conteria capacitação para garantir: a manutenção da integridade original de um documento digital (detectando, e como conseqüência, impossibilitando adulterações posteriores) e a autoria dos contratantes (assegurando ao contratante eletrônico que a outra parte é realmente quem diz ser).

Quanto a isso, pode-se inferir que a Medida Provisória retrocitada, por si só, foi suficiente para validar a prova eletrônica.

4.3 Segurança, validade, integridade e autoria

Neste subtópico será detalhado o aspecto segurança nas contratações por meio eletrônico, de maneira que possam ser apresentadas como prova em tribunais, com os atributos que a lei estende a documento.

Num contrato eletrônico, relativamente à parte formal, interessam às partes, principalmente:

a) A confidencialidade e a privacidade da negociação. A garantia de que somente usuários autorizados poderão tomar conhecimento da informação.

b) A integridade do convencionado. A garantia de que os originais não foram adulterados ou corrompidos.

c) A identidade da outra parte.

d) *Nonrepudiation*. A garantia ao recipiente de que o emissor não poderá – falsamente – negar a autoria de uma mensagem, ou seja, renegar o conteúdo de sua manifestação no contrato.

Essas características poderão ser, *juris tantum*, asseguradas mediante o uso das chaves assimétricas.

4.4 Criptografia

De início, importa esclarecer que convém o uso da criptografia sempre que duas pessoas pretendam trocar mensagens, a salvo da curiosidade alheia, num meio relativamente inseguro, como a Internet, por exemplo.

Muito utilizadas em tempos de guerra, mensagens criptografadas visavam impossibilitar ou dificultar que o inimigo viesse a ter conhecimento de informações sigilosas.

Da forma mais elementar em que se substitui uma letra do alfabeto por outra (Por exemplo, a letra “A“ seria substituída pela 5.ª letra “E”; a letra “B, pela 6.ª letra ”F”; a letra “C”, pela 7.ª letra “G”, e, assim sucessivamente), chega-se aos tempos atuais em que se atribui uma chave a qualquer mensagem através de programa de computador por meio de complexas fórmulas matemáticas.

A criptografia, por conseguinte, através de processo eletrônico-matemático, com o uso de algoritmos, torna determinados dados ininteligíveis a quem não conhece a chave criptográfica.

Criptografia[25] é uma técnica destinada a dar segurança e sigilo às comunicações, funcionando pela aplicação de um padrão secreto de substituição de caracteres, de maneira que a mensagem se torne ininteligível para quem não conheça o padrão criptográfico utilizado. Este, modernamente, baseia-se em conceitos matemáticos avançados e abstratos. Sua aplicação tornou-se elemento essencial na formação de uma infra-estrutura para o comércio eletrônico e a troca de informações (QUEIROZ, 2001, p. 389-90).

Um outro conceito de criptografia é *"uma escrita que se baseia em um conjunto de símbolos cujo significado é conhecido por poucos, permitindo com isto que se criem textos que serão incompreensíveis aos que não saibam o padrão de conversão necessário para a sua leitura"* (DINIZ, 1999, p. 28).

Ao se criptografar, estabelece-se uma relação arbitrária entre o conteúdo original e o novo arquivo criado.

---

[25] Do Dicionário Aurélio, foram extraídos os significados de alguns termos relacionados com a criptografia:

* Algoritmo:
Conjunto de regras e operações bem definidas e ordenadas, destinadas à solução de um problema, ou de uma classe de problemas, em um número finito de etapas.

* Criptografia:
Arte de escrever em cifra ou em código.
Conjunto de técnicas que permitem criptografar informações (como mensagens escritas, dados armazenados ou transmitidos por computador etc.).

* Criptografar:
Tornar incompreensível, com observância de normas especiais consignadas numa cifra ou num código, o texto de (uma mensagem escrita com clareza).
Codificar (uma informação) de forma a tornar difícil sua decodificação sem a chave adequada.

* Encriptar:
Codificar (os sinais de um programa ou transmissão) para evitar utilização indevida deles.

* Decriptar:
Traduzir ou decifrar (mensagens cifradas, das quais não se tem a chave).

* Decodificar:
Fazer operação inversa à de codificar.
[Sin.: descodificar. Conjug.: v. trancar].

Como conseqüência dessa relação tem-se o padrão de conversão, ou seja, a *"relação de significância entre o arquivo original e o seu criptograma"* (DINIZ, 1999, p. 29).

Existem programas de computador oferecendo infinitos padrões de conversão. A informação que guarda essa correlação de sinais aplicados é registrada em um conjunto de bits, que recebe o nome de chave.

Utilizado o programa de computador, a chave, portanto, serve ao mesmo tempo para encriptar e decodificar determinada mensagem.

Diferentemente da criptografia, criptologia é a ciência que estuda as relações entre dois entes, em lados opostos mas não necessariamente como adversários. De uma parte, o criptógrafo e, de outra, o criptoanalista. Enquanto aquele busca a segurança escondendo a informação à maioria dos que a ela tiverem acesso, este tenta decifrar a chave do segredo.

Na realidade, um sistema criptográfico deve ser testado pelo criptoanalista, que analisa o grau de dificuldade, a impossibilidade de ele ser desvendado pelas técnicas conhecidas. Tudo isso à semelhança do provador de vinho que, após degustá-lo, o classifica numa entre categorias diversas.

O elemento central é a segurança. Mas diversos fatores, todos interdependentes, afetam um sistema criptográfico, tais como: as técnicas de criptografia, a evolução tecnológica dos recursos materiais, par a par com o correspondente tempo que se leva para a quebra do segredo e os custos exigidos e os benefícios alcançáveis, tanto para se proteger como para atacar.

A seguir, esses fatores serão vistos, separadamente.

4.4.1 As técnicas de criptografia

Relativamente às técnicas criptográficas, leva-se em conta que a defesa primária fundamental contra ataque é o comprimento da chave de codificação.

Técnicas que se valerem de comprimentos fundamentais mais longos aumentam o número de combinações possíveis diminuindo a possibilidade de

ataques prósperos, ou seja, ataques coroados de êxito nas investidas dos visitantes indesejáveis.

Por isso, desde a primeira delas, diversas outras, mais evoluídas, foram surgindo: a de 40, 56, 128 bits. As técnicas hoje em uso são de 512, 1.024 e 2.048 bits.

Tanto os criptoanalistas legais quanto os *hackers* buscam o constante aperfeiçoamento de técnicas.

Anteriormente, na técnica de 40 bits, usando um computador pessoal que pudesse tentar 1 milhão de chaves por segundo, um atacante poderia violar uma chave em aproximadamente 13 dias.

Numa técnica mais avançada, de 56 bits, alguns peritos em criptografia tinham calculado em vários milhões de dólares o custo para se construir um computador que pudesse desvendar o algoritmo DES.

Mas, em julho de 1998, a *Eletronic Frontier Foundation de San Francisco* (Califórnia), usando um supercomputador construído parcialmente com componentes usados conseguiu, ao custo de duzentos e cinqüenta mil dólares, lançar um ataque próspero em uma mensagem codificada com aquele algoritmo.

O computador procurou 92 bilhões de chaves por segundo e decifrou a mensagem em 56 horas, depois de tentar aproximadamente 25% das chaves possíveis.

Em janeiro de 1999, a mesma entidade, aperfeiçoando seu supercomputador, pôde quebrar a mensagem codificada em aproximadamente 22 horas.

Chaves de pelo menos 64 bits geralmente são consideradas suficientes para proverem proteção forte contra ataques de força bruta, ou seja, ataques não autorizados, efetivados sem a utilização da chave correspondente.

Afirma-se hoje que, na técnica de 128 bits, mesmo tendo à disposição 10 milhões de computadores que permitissem cada um tentar 100 bilhões de chaves por segundo, levar-se-ia aproximadamente 10 anos para examinar todas as possibilidades.

Atualmente, chaves simétricas de 128 bits ou do algoritmo IDEA são consideradas irrompíveis para ataques de força bruta.

Ainda no que concerne à segurança da informação deve-se levar em conta o fato de que, como se poderia imaginar, ela não é diretamente proporcional ao grau de tecnologia empregada na criptografia.

Isso porque um sistema de criptografia é constituído de processos e estes, de procedimentos. Há uma inter-relação entre os diversos elos. O nível de segurança é igual ao elo mais fraco da corrente.

Primeiramente, infere-se que o mais aperfeiçoado sistema de criptografia proporciona segurança à informação em grau elevadíssimo. Contudo, essa certeza pode reduzir-se drasticamente se o computador de que se vale o emissor ou receptor não estiver protegido por um singelo programa anti-vírus e de *firewall*.

Sem essa proteção, é grande a possibilidade, dependendo do grau de interesse que desperte a informação protegida, que o computador em foco seja infectado por um vírus tipo "cavalo-de-tróia". Instalam-se os vírus no computador da vítima e sempre que forem digitadas determinadas palavras-chaves previamente selecionadas, os programas da espécie transmitem ao invasor informes valiosíssimos. Tudo isso acontece sem que o proprietário da informação detecte ou ao menos suspeite do que está ocorrendo.

Além disso, é conveniente a instalação de um programa *firewall*. Um *firewall* protege um computador contra acessos não autorizados por parte de terceiros. Se, de um lado, integrando-se à Internet, o usuário passa a ter acesso ao mundo, a recíproca também é verdadeira. Com uma facilidade até relativa, um *hacker* ou *cracker* pode bisbilhotar o computador da vítima e, com o simples clicar no botão de seu mouse, causar danos enormes e irreparáveis.

Firewall são definidos como equipamentos que *"atuam como uma 'válvula de mão única', ou seja, os usuários que estão dentro do tráfego original podem sair, mas nenhum tráfego externo pode entrar"* (STARLIN e NOVO, 1998, p. 45) ou conjuntos de *software* e *hardwar*e que abrangem desde simples sistemas de arquivo com registro de tráfego até métodos mais complexos. Ocorre aí um permanente conflito entre facilidade de uso e paranóia de segurança. (ALBERTIN, 1999, p. 170-71).

Finalmente, para manter a integridade de seus sistemas, o usuário deve treinar-se pessoalmente e capacitar seus assessores, bem como preocupar-se

com medidas de segurança lógica, tais como a realização periódica de *backup*, o controle de instalação de novos sistemas, o controle da integridade dos sistemas existentes, entre outros.

4.4.2 Tempo e evolução tecnológica

O segundo ponto a se considerar relativamente ao sistema criptográfico é que o tempo exigido para um ataque de procura próspero diminui na proporção inversa ao do aumento do poder de computação à disposição dos atacantes. Além disso, ocorre a constante redução no preço dos computadores poderosos e o fato de que os atacantes desenvolvem novas técnicas para melhorar a eficácia dos ataques.

Em decorrência desse avanço da tecnologia, o poder dos computadores pessoais tem dobrado historicamente a cada 18 meses.

Portanto, devem ser constantemente revisadas as estimativas de tempo requeridas para ataques prósperos de procura de chaves.

A evolução das técnicas se mostra necessária porque um sistema nunca é infalível, inviolável. Qualquer sistema pode ter o seu segredo desvendado porquanto todos se valem necessariamente de um dado conhecido: a palavra.

A diferença entre eles é tão somente o maior ou menor grau de segurança, ou seja, apenas não se sabe o tempo que se levará para quebrá-lo: alguns meses ou milhares de anos.

4.4.3 Custos e benefícios

O terceiro fator é a importância de um sistema de criptografia propiciar segurança a custos aceitáveis.

Do ponto de vista de quem pretende proteção, esses custos não podem ser superiores ao benefício da segurança.

Da ótica do atacante, um dado a se considerar é a comparação entre o benefício e o custo para se obter a quebra do sistema.

Uma pesquisa que enseje o uso de sistemas sofisticados de computadores, de altíssimo custo, por longo tempo, só será viável se trouxer o retorno do investimento realizado.

Tudo depende, portanto, do objeto de proteção e ataque.

Segredos de uma indústria farmacêutica relativamente pequena ou trilhões de dólares circulando diariamente nas finanças globalizadas pelo mundo afora?

Ou, ainda, dados confidenciais e comprometedores que, caindo em mãos erradas, poderiam fazer despencar e inviabilizar uma candidatura à Presidência da República, por mais avantajada que estivesse em termos de "Ibope"?

Ou, por derradeiro, de quais artifícios não-éticos ou até ilícitos se valem certas agências de inteligência para descobrir onde estaria determinada pessoa classificada como o terrorista número 1 do mundo?

Não se pode atribuir essas possibilidades meramente à imaginação fértil de romancistas.

Vejamos, por exemplo, o que comenta Lucca (2001, p. 56), a respeito da segurança dos sistemas criptográficos:

> ... “consideram que o tempo necessário para descobrir o conjunto numérico capaz de decriptar a mensagem criptografada está ficando cada vez menor, além de outros problemas relacionados à criptografia.
>
> Suspeita-se, por exemplo – e a desconfiança parte da França e de alguns outros países – de que os sistemas operacionais de criptografia exportados pela Microsoft tenham 'passagens secretas' que poderiam ser utilizadas somente por agentes dos EUA na tarefa de espionar empresas e governos de outros países. A China se nega a permitir que o recém-lançado Windows 2000 seja vendido no país, não tendo havido acordo, até o momento, entre a Microsoft e a Comissão Estatal para Administração da Criptografia chinesa, conforme divulgado pela imprensa."

Ou ainda, Queiroz (2001, p. 394), sobre as americanas NSA - *National Security Agency* e a CIA:

> "De acordo com versões que circulam nos veículos noticiosos e entre especialistas, a NSA costumaria manter relações promíscuas com o setor privado. São muitos os boatos de que essa agência tentaria, insistentemente e pelos meios mais heterodoxos, forçar um acordo com desenvolvedores de tecnologia, a fim de obter uma cópia da chave privada de todos os códigos criptográficos, para serem utilizadas no combate ao terrorismo.
>
> Não obstante o apelo politicamente correto do combate a essa praga social moderna, também não são poucos os boatos de que aquela agência,

> após o fim da guerra fria, estaria encabeçando, juntamente com a CIA, o esquema (extra-oficial) de espionagem industrial em benefício das empresas e dos interesses comerciais norte-americanos (quem não se lembra das reviravoltas ocorridas no caso da concorrência para implantação do SIVAM?)."

Logo, voltando ao terceiro fator em exame neste subtópico, custo proibitivo é um componente a imprimir segurança a um sistema criptográfico. Em contrapartida, também para despertar a cobiça de mentes desejosas de envidar esforços para desvendá-lo.

De todas essas assertivas, o que de concreto se pode concluir é que:

a) Tem-se mais proteção contra ataque quanto mais longa for a chave.
b) Não existe proteção absoluta. O prazo que leva-se para desvendá-la é apenas uma questão de tempo.
c) Menos pessoas aventurar-se-ão na empreitada quanto maiores forem os custos para se “quebrar” a chave.
d) Quanto maiores forem os benefícios potenciais, mais compensatórios tornar-se-ão os “investimentos” para descobrir a chave.

4.5 Assinatura Convencional e Assinatura Digital

4.5.1 Assinatura convencional

A assinatura convencional foi o principal meio escolhido pelo legislador como instrumento para demonstrar-se, de forma segura, a existência e a eficácia das declarações de vontade. À exceção de quando esteja tratando da chancela mecânica, sempre que a norma legal se reporta à assinatura, vem-nos à lembrança um sinal gráfico particular produzido manualmente e aposto em objeto corpóreo.

Sua aposição gera presunção de aceitação das declarações constantes do objeto, identificando o autor da assinatura (DINIZ, 1999, p. 36-37).

Conseqüentemente, são requisitos imprescindíveis na assinatura a ação manual do signatário e a existência de um objeto corpóreo. Esse ato corresponde à aposição da assinatura autográfica no próprio instrumento documental em que a declaração se faz representar.

4.5.2 Assinatura digital

Quanto à forma de operacionalização, a assinatura digital não deve ser confundida com a senha utilizada no relacionamento entre clientes e bancos, por meio de terminais eletrônicos. O código bancário, via de regra, limita-se a permitir o acesso aos computadores do banco e aos programas neles inseridos, limitados à conveniência de cada instituição.

Queiroz (2001, p. 398), fundamentando-se em diversos autores, resume e caracteriza a assinatura digital como

> “espécie do gênero assinatura eletrônica, que compreende diversas espécies de processos eletrônicos de identificação, tais como senhas, assinaturas autográficas digitalizadas, chancela mecânica, biometria (leitura de íris, de digitais ou timbre vocal) etc.”

E esse autor (2001, p. 390) esclarece que se aplica essa técnica criptografando os próprios bits do documento original e não simplesmente embaralhando as palavras das frases ou as letras das palavras.

Diniz (1999, p. 32), por sua vez, define a assinatura digital, atribuída a determinado agente, como *"uma técnica que permite a estabilização do conteúdo do arquivo e a identificação do seu criador, atribuindo, com permanência, certo grau de infungibilidade aos elementos imateriais ali expressos"*.

Greco (2001, p. 88-89) explica que:

> a) "Os bits da escritura eletrônica são entidades magnéticas e, portanto, à sua maneira, realidades materiais, ainda quando não perceptíveis pelos sentidos humanos".

b) "Existem documentos direta e indiretamente representativos de determinados fatos. Os documentos que registram sons e imagens são diretamente representativos. As declarações humanas em linguagem escrita são indiretamente representativas".

c) "O registro magnético convencional, em fita ou disco, é facilmente adulterável.

Diz-se que o procedimento de criptografia evita que o documento seja adulterado depois de aposta a assinatura eletrônica.

Mas a convicção dessa segurança ainda não penetrou na consciência coletiva".

Para Augusto Tavares Rosa Marcacini[26], o emprego na assinatura digital da tecnologia da criptografia de chave pública preenche os requisitos da identidade, da integridade e da perenidade do conteúdo:

> "O uso e o controle da chave privada devem ser de exclusividade do proprietário, permitindo a individualização da autoria da assinatura (função declarativa); a autenticidade da chave privada deve ser passível de verificação, a fim de ligar o documento ao seu autor (autenticação, ligada à função declaratória); a assinatura deve estar relacionada ao documento de tal maneira que seja impossível a desvinculação ou a adulteração do conteúdo do documento, sem que tal operação seja perceptível, invalidando automaticamente a assinatura (função probatória)".

Esse autor prossegue esclarecendo que a assinatura digital,

> "é, na verdade, um número, resultado de uma complexa operação matemática que tem como variáveis o documento eletrônico e a chave privada, detida pelo signatário com exclusividade. Como a chave privada se encontra em poder exclusivo do seu titular, somente ele poderia ter chegado no número representado pela assinatura. A assinatura digital de uma mesma pessoa será diferente, para cada documento assinado, pois, sendo este uma das variáveis da função matemática, o seu resultado (assinatura), será diferente para cada documento. Isto evita que uma mesma assinatura possa ser utilizada para outros documentos."

Quanto a essa conceituação, permitimo-nos fazer um comentário. Não obstante Marcacini defina assinatura digital como "um número", o mais esclarecedor seria "um conjunto de caracteres", os quais não seriam necessariamente constituídos somente de números. Relativamente à parte final dessa definição, Queiroz (2001, p. 399-400) concorda que "*como a assinatura é gerada a partir dos bits contidos no próprio documento assinado*", ela vale exclusivamente para esse documento.

---

[26] In O documento eletrônico como meio de prova. Revista de Direito Imobiliário n.º 47. RT, p. 71, apud Costa (2001, p. 204-05).

Caso ocorra qualquer alteração na quantidade ou na seqüência dos bits do documento, mesmo ocasionado por simples inclusão de um espaço ou a correção de um insignificante erro de datilografia, invalidar-se-á automaticamente a assinatura digital.

4.6 O Sistema de Chaves Simétricas

Existem, a propósito, dois sistemas de chaves: a simétrica e a assimétrica.

O primeiro deles é o da chave simétrica, em que o programa codificador do texto em caracteres indecifráveis se vale da mesma chave tanto para criptografar como para descriptografar a mensagem. A chave é única para o emissor e para o receptor.

Daí decorre a sua fragilidade, deixando a desejar no tocante à segurança, pois, em algum momento, por qualquer meio, deverá ocorrer a troca de uma mensagem de um para outro comunicando a chave simétrica.

Por apoiar-se nesse sistema de maior vulnerabilidade, é mais utilizado em redes fechadas ou apenas para garantir o sigilo de arquivos pessoais armazenados em computadores isolados.

4.7 O Sistema de Chaves Assimétricas

O segundo deles, o da chave assimétrica, funciona com duas chaves formando um par único: é composto de chave privada, de exclusivo conhecimento do seu portador (não circula pela rede de computadores), e da correspondente chave pública, que pode ser divulgada a terceiros.

Uma delas serve para criptografar e a outra, para descriptografar.

Por essa razão, no meio eletrônico, pela segurança que propicia, é o mais aceito dos sistemas. Apesar de essa segurança oferecida não ser absoluta, tem a vantagem de que, para desvendá-la, exigir-se-ia a utilização de muitos supercomputadores por longo período.

Essa técnica assimétrica, também chamada de chave pública *(public-key)*, baseia-se no sistema de criptografia.

Essa técnica envolve (ALBERTIN, 1999, p. 168):

> "um par de chaves, uma chave privada e uma chave pública associadas a cada usuário. A informação criptografada pela chave privada pode ser decriptografada somente utilizando a chave pública correspondente. A chave privada, usada para criptografar a informação transmitida pelo usuário, é mantida secreta. A chave pública é utilizada para decriptografar no destinatário e não é mantida secreta. Uma vez que somente o autor de uma mensagem criptografada tem conhecimento da chave privada, uma decriptação com sucesso utilizando a chave pública correspondente verifica a identidade do autor e assegura a integridade da mensagem".

Somente com a chave pública decodifica-se a mensagem original, criptografada com a chave privada. Porém, não haverá garantia de confidencialidade nem privacidade, isto é, além do destinatário almejado, outras pessoas poderão ter acesso à mensagem porque, na sistemática, a chave pública pode ser amplamente divulgada.

Em sentido inverso, a mensagem criptografada com a chave pública somente poderá ser decodificada com a correspondente chave privada, nesse caso, exclusivamente pelo seu titular. Somente nessa hipótese haverá garantia de exclusividade de recepção e total privacidade.

Para que essa garantia ocorra nos dois sentidos, faz-se mister que tanto emissor quanto receptor sejam portadores de chaves assimétricas.

Nessa circunstância, o emissor deverá cifrar a mensagem com a chave pública do destinatário, assinar essa mensagem com a sua chave privada e enviá-la ao destinatário. Quanto ao receptor, deverá decifrar a mensagem utilizando a chave pública do remetente, certificando-se de sua origem e aplicar a sua chave privada; só assim a mensagem tornar-se-á inteligível e segura.

Ao solicitar a certificação digital perante uma Certificadora Autorizada, o interessado recebe em seu computador uma chave privada (de seu exclusivo conhecimento e guarda). Mediante complicados cálculos matemáticos e com a aplicação de algoritmos[27], um programa de computador gera o certificado contendo a chave pública vinculada àquela chave privada.

Em resumo, para aplicar-se a criptografia assimétrica requer-se um par de chaves, uma pública e outra privada, para todos os interessados em participar de comunicações de forma segura.

Para atribuir e preservar as três características - integridade, autenticidade e sigilo - é preciso que o emitente assine a mensagem e criptografe-a digitalmente. Apenas assinar garante a autenticidade e a integridade mas não a confidencialidade e só pode ser efetuada por possuidor de certificado. Tão somente criptografar garante o sigilo, mas não a autenticidade ou a integridade e pode ser efetuada também por não possuidor de certificado desde que receba em seu computador o certificado com a chave pública do destinatário.

4.8 Certificadora Autorizada

Neste subtópico, o monografista procurará apresentar, de maneira simples, a forma prática para a obtenção de chaves assimétricas.

A geradora dessas chaves é uma certificadora autorizada. Esta, baseada na confiança que desfruta no mercado, por meio de um *software* (programa de computador), gera para os interessados uma chave pública fazendo par com uma chave privada. Em seguida, inclui a chave pública no seu *site*. Esse rol, constituído de chaves públicas vigentes e canceladas, destina-se a consultas e a

[27] Strebe e Perkins (2002, p. 108) conceituam algoritmo como uma seqüência de "passos detalhados para realizar uma função" num computador, e acrescentam mais adiante, à p. 114, que semelhante ao algoritmo, o protocolo descreve as etapas que devem efetuar dois ou mais computadores comunicando-se entre si.

certificadora deve obrigar-se a arquivar esses dados de forma segura que impossibilite violações.

Como exemplo desse tipo de certificadora autorizada, aberta a quaisquer interessados, tem-se, entre outras e atuando em diversos países, a VeriSign (maiores detalhes poderão ser obtidos em <http://www.verisign.com>), a qual é representada no Brasil pela CertiSign (<http://www.certisign.com.br>).

Num outro nível, eis que não estão abertas a toda a coletividade, existem outras certificadoras autorizadas. Entre estas, cita-se a ICP da OAB-SP.

Essas certificadoras autorizadas podem ainda ser constituídas por uma entidade definida em relação a seus membros, como uma escola certificar a chave pública de seus funcionários, alunos e professores; uma empresa, a de seus diretores e empregados.

Dando prosseguimento à demonstração do processo, quando concluída a certificação, o usuário identificado como proprietário das chaves recebe um certificado – digital - constante de dados pessoais que vinculam sua pessoa à chave pública.

O certificado, assim distribuído, pode ter diversas classes em cada certificadora autorizada. Cada uma delas busca satisfazer determinado interesse e finalidade pretendidos pelo usuário.

A VeriSign, por exemplo, disponibiliza quatro diferentes “classes” de certificados digitais:

a) Classe 1 – Consta apenas nome e e-mail do signatário.

b) Classe 2 – Há necessidade de maior quantidade de dados pessoais.

c) Classe 3 – Exigência da presença física da pessoa candidata ao certificado.

d) Classe 4 – A concessão do certificado é precedida de investigação do interessado.

São possíveis certificações mais completas, como meio de se provar informações sobre o signatário ou certificar o dia e hora em que o documento foi

firmado ou atestar o conhecimento de algum fato ou certificar estado etc. (QUEIRÓZ, 2001, p. 402).

A propósito, esse autor esclarece que algumas certificadoras autorizadas podem

> "certificar a origem e a propriedade de uma determinada página da Internet. Os próprios navegadores (browsers) mais modernos, já estão capacitados para, ao comando do operador, exibir o certificado da página, que atesta a identidade do proprietário desta, evitando que consumidores ou parceiros comerciais desavisados sejam induzidos em erro por páginas falsificadas. Várias empresas **.**com brasileiras já usam esse sistema que, a cada dia, vai tornando-se uma necessidade para o comércio eletrônico."

Essa certificação vai, portanto, desde a mais simples, na qual não se identifica o interessado, até a mais completa.

Caso o usuário tenha interesse em fazer prova de sua "assinatura digital", deve passar, pelo menos, pelas seguintes etapas, na obtenção de certificado:

a) Solicita a chave à certificadora autorizada através de sua *home page*, informando previamente dados pessoais.

b) Recebe por *e-mail* um contrato de adesão a ser impresso. Em seguida, deve comparecer e assinar o referido contrato pessoalmente perante um tabelião para que sua firma seja reconhecida por autenticidade. Os documentos apresentados são copiados e autenticados pelo tabelião.

c) Devolve à certificadora autorizada, pela via postal, o contrato de adesão. Este contém um número de série do certificado digital. A certificadora autorizada envia a documentação para o Registro de Títulos e Documentos.

d) Recebe o certificado da certificadora autorizada que vale por prazo determinado e é renovável em seu vencimento. Vide no ANEXO B *fac simile* de um certificado digital, tal qual apareceria na tela do computador (MITCHELL, 2001, p. 343).

De posse do certificado e da chave assimétrica, o usuário do sistema poderá se valer do sistema de autenticação digital nas mensagens por ele geradas.

É importante salientar que a assinatura digital, constituída por bits, não é perceptível aos nossos olhos. Suas características não são passíveis de conferência como o é uma assinatura manual aposta em papel.

Ela é diferente para cada mensagem gerada pelo mesmo usuário e nisto reside a segurança quanto à integridade do documento eletrônico.

Costa (2001, p. 205) esclarece que, assim como acontece com a assinatura tradicional aposta em papel, em que às vezes não é possível tão só pela assinatura identificar o seu subscritor, na assinatura digital ocorre o fenômeno como regra.

Portanto, para identificar o autor da assinatura digital, necessita-se da certificação eletrônica, em que uma terceira parte, a certificadora autorizada, assegura a titularidade da chave pública do autor da mensagem.

Na certificação, deve-se registrar a tecnologia empregada na certificação.

Essa tecnologia e o conceito da entidade certificadora, conseqüentemente, serão os critérios fundamentais para se mensurar o grau de confiança que as partes envolvidas emprestarão à mencionada certificação.

Por exemplo, após receber uma mensagem do emissor, o recipiente poderá eventualmente, no futuro, necessitar fazer prova em Juízo do afirmado pelo emitente. Como proceder? Poderá provar a autenticidade e a integridade do documento eletrônico em seu poder valendo-se do certificado da chave pública do emissor combinando-a com os *softwares* disponibilizados pela certificadora autorizada.

Essa comprovação tornar-se-ia impraticável se, numa eventualidade, o recipiente alterasse o teor da mensagem mesmo que em detalhes juridicamente irrelevantes (exemplos: um espaço a mais entre duas palavras ou a supressão de um acento gráfico aposto incorretamente pelo emissor). Em suma, a assinatura digital, do mesmo emissor para o mesmo destinatário, não seria a mesma conforme o conteúdo da mensagem criptografada, por mais imperceptível ou irrisória que fosse a diferença. Para cada mensagem diferente o programa gerará uma assinatura diferente.

Como foi dito no início deste subtópico, a certificadora autorizada estará obrigada a disponibilizar, para consulta e confirmação, em diretórios seguros, as chaves públicas por ela certificadas. Nesses diretórios, qualquer interessado poderá obter cópias autênticas dessas chaves. Importa repetir que, por segurança, as chaves privadas não circulam pela rede de computadores.

4.8.1 A ICP-OAB

A OAB - Conselho Federal e a Seccional de São Paulo disponibilizaram, para os advogados inscritos, a certificação digital.[28]

Diante da possível resistência dos profissionais a elas ligados, seja por apego ao tradicionalismo seja por receio do desconhecido, lançou em fevereiro de 2002 a certificação digital sob a forma de teste, numa iniciativa muito feliz. Nesse período de testes, os funcionários da OAB e os advogados e estagiários nela inscritos poderão praticar e familiarizar-se com a nova tecnologia, aprendendo a lidar, de forma segura, com a criptografia e a assinatura digital.

No site da OAB-SP há orientação pormenorizada sobre estrutura e funcionamento da ICP-OAB, certificação eletrônica e assinaturas digitais, como requerer e instalar um certificado digital da ICP-OAB, uso seguro dos certificados pelos advogados e riscos envolvidos, como escolher uma senha segura e respostas para as dúvidas mais freqüentes.

Nesse empreendimento da OAB, cheia de méritos, todavia, s.m.j., permitimo-nos discordar da escolha da OAB-Conselho Federal como Autoridade Certificadora Raiz.

Como será visto abaixo no subtópico 5.1, a Medida Provisória n.º 2.200-2, de 24/08/2001, instituiu a Infra-Estrutura de Chaves Públicas Brasileira - ICP-

---

[28] Disponível em: <http://cert.oabsp.org.br/teste>. Acesso em: 19maio2002. Efetuado novo acesso em 1out2002, confirmou-se que a entidade mantém a ICP-OAB em caráter de teste.

Brasil, nomeando o Instituto Nacional de Tecnologia da Informação - ITI como a AC Raiz, determinando que as declarações constantes dos documentos em forma eletrônica, produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil, sejam considerados documentos públicos ou particulares e presumidos como verdadeiros em relação aos signatários.

Melhor teria procedido, portanto, a OAB, se fizesse parte da ICP-Brasil, certificando os advogados a partir de Autoridade Certificadora (no caso, as próprias seccionais da OAB) que fosse derivada da AC Raiz, o ITI, que tem base legal.

Agindo dessa maneira, tendo sua certificação derivada do ITI e fazendo parte da ICP-Brasil, conforme comentado ao final do tópico “2.2.6 - Transmissão de peças processuais - Projeto de Lei n.º 5.828/01”, não haverá necessidade de credenciamento dos advogados junto aos órgãos do Poder Judiciário, eis que todos farão parte da mesma e única ICP-Brasil.

A crítica da OAB, nesse aspecto, pleiteando a hegemonia no cadastramento de advogados não tem razão de ser porque entendemos que se tratam de duas funções distintas: uma coisa é o acolhimento e cadastramento de cidadãos para o exercício da advocacia (art. 3.º, da Lei n.º 8.906, de 4/7/1994); e, outra coisa, é o cadastramento de advogados junto ao Poder Judiciário, mormente quando o serão com chaves públicas certificadas pela própria OAB.

4.9 Tabelião Virtual

De acordo com a Constituição Federal de 1988, art. 236, os serviços notariais e de registro são exercidos em caráter privado, por delegação do Poder Público, competindo à lei regular as atividades, disciplinar a responsabilidade civil e criminal dos notários, dos oficiais de registro e de seus prepostos, e definir a fiscalização de seus atos pelo Poder Judiciário.

A Lei n.º 8.935, de 18/11/1994, em seus arts. 1.º e 3.º, respectivamente, estabelece que é inerente à atividade notarial e de registro garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos, sendo que notário, ou tabelião, e oficial de registro, ou registrador, são profissionais do direito, dotados de fé pública, a quem é delegado o exercício da atividade notarial e de registro.

O Projeto de Lei n.º 1.589/99, que tramita pelo Congresso Nacional, em seus arts. 16 e 25, delega ao tabelião a certificação de chaves públicas, mas, em seus arts. 17 e 24, permite que entidades privadas também façam essa certificação, ficando essa aceitação baseada na fé privada que merecerem tais entidades.

A diferença fundamental desses atos fica por conta do valor probante que eles irão gerar. A certificação pública traz a fé pública das funções notariais e a responsabilização civil por eventuais prejuízos causados por inadequação por ocasião dessas certificações.

Greco (2001, p. 90-91), citando deficiências gravíssimas no registro de pessoas naturais e no de imóveis, considera difícil que os tabeliães públicos se disponham a efetuar grandes investimentos que dêem credibilidade a serviços de certificação ou de autenticação.

Queiroz (2001, p. 407-13) compartilha da posição adotada por Greco. Citando inúmeros exemplos, comprova que, buscando a rapidez inerente às contratações por meio eletrônico, toda a legislação comparada estende a certificadores privados a possibilidade de atestarem a autenticidade de um documento eletrônico. A concorrência seria benéfica para todos os usuários dos serviços de certificação, tanto o consumidor como o próprio Estado.

O que se vê em outros países é a preocupação em garantir padrões mínimos de segurança, controlando a idoneidade das empresas certificadoras, mediante exigência de autorização legal para o seu funcionamento.

Prosseguindo, Queiroz assevera que o art. 236 da Constituição Federal remeteu para o legislador ordinário a missão de definir as atividades, os poderes, os deveres e a extensão dos atos do tabelião. A reserva de mercado para os

tabeliães públicos “reconhecerem firmas” decorre, portanto, da Lei n.º 8.935, de 18/11/1994, a qual é passível de ser alterada por outra lei ordinária.

Lucca (2001, p. 68-69), embora reconheça o aprimoramento da qualidade dos serviços prestados pelos tabeliães, alguns dos quais deram inequívoca demonstração de avanço tecnológico, conclui que eles dificilmente superarão os *“prestados por empresas especializadas em informática, dotadas de tecnologia de ponta, em condições de oferecer ao consumidor melhor qualidade a preços mais baixos”*.

Relativamente à responsabilidade por certificações, Costa (2001, p. 207) afirma que:

> "pessoas físicas ou jurídicas que não exerçam atividade empresarial de certificação não devem sofrer o mesmo nível de responsabilização que deve recair sobre aquelas que têm, na certificação, sua atividade principal, posto que das últimas é possível exigir-se um nível de conhecimento e de qualidade diferente do que se espera das primeiras. Por outro lado, deve considerar-se que mesmo as empresas certificadoras dispõem de diferentes níveis de certificados, com diferentes procedimentos de identificação da titularidade da chave pública, razão pela qual também deve ser ponderado o perfil do certificado, na determinação da responsabilidade por ele gerado. Finalmente, as atividades notarial e registral, por serem dotadas de fé pública, devem ter um nível de responsabilidade por danos eventualmente causados a terceiros compatível com a presunção legal de autenticidade inerentes às suas funções".

Em que pesem todos esses argumentos contrários à atividade virtual do tabelião, na prática é constatado que, tal qual no gênero "documento tradicional", circulam diversos documentos em que não se exige o reconhecimento público do tabelião.

E, como nem por isso deixa de se atribuir a tais documentos ditos particulares valor probante, da mesma forma em relação aos documentos digitais, aqueles que contiverem assinatura digital e certificados por entidade privada também, dependendo de provas adicionais, serão valorados em nossos tribunais.

Ademais, a própria Medida Provisória n.º 2.200-2, de 24/08/2001, determina em seu art. 10, § 2.º, que *“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" e nos arts. 8.º e 10, § 1.º, que poderão ser credenciados como Autoridades Certificadoras tanto órgãos e entidades públicos quanto pessoas jurídicas de direito privado, não fazendo qualquer distinção entre estas e aqueles, a ambos estendendo a presunção de veracidade em relação aos signatários, na forma do art. 131 do Código Civil.

5 – LEGISLAÇÃO

5.1 Medida Provisória n.º 2.200-2, de 24/08/2001

Como a questão pertinente a documento eletrônico está sujeita a imprevisíveis inovações tecnológicas e que eventuais detalhamentos poderiam rapidamente ser considerados obsoletos, com muito acerto, a Medida Provisória n.º 2.200-2, de 24/08/2001, limitou-se a estabelecer os pontos básicos necessários à validação de documentos em forma eletrônica.

É uma MP de apenas 20 artigos. A seguir, serão comentados os seus pontos fundamentais.

Com a finalidade de garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras, em seu art. 1.º, institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.

Determinam o "caput" e parágrafos do art. 10 que as declarações constantes dos documentos em forma eletrônica, produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil, consideram-se documentos públicos ou particulares e presumem-se verdadeiros em relação aos signatários, na forma do art. 131 do Código Civil. Nada obsta, todavia, 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.

Conforme o art. 2.º, a ICP-Brasil terá sua organização definida em regulamento e será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta por Autoridade Certificadora Raiz - AC Raiz, Autoridades Certificadoras - AC, e Autoridades de Registro - AR.

Nos arts. 5.º e 12 a 14, nomeia o Instituto Nacional de Tecnologia da Informação - ITI, como a AC Raiz, que desempenhará atividade de fiscalização, podendo ainda

aplicar sanções e penalidades, na forma da lei. A ele compete 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 e das AR e dos prestadores de serviço habilitados na ICP.

As AC, de acordo com o art. 6.º, são as entidades credenciadas para emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, competindo-lhes emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações. Ressalva em seu parágrafo único que o par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de controle, uso e conhecimento exclusivos.

Atribui o art. 7.º às AR, entidades operacionalmente vinculadas a determinada AC, competência para identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Possibilita o art. 8.º que, observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR as entidades e os órgãos públicos e as pessoas jurídicas de direito privado.

Por fim, pelo art. 9.º, é vedado a qualquer AC certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

5.2 Projeto de Lei n.º 1.589/99

O Projeto de Lei n.º 1.589/99, apresentado pela OAB/SP, em seus 52 artigos, tem como âmbito de aplicação, conforme seu art. 1.º, regular o comércio eletrônico, a validade e o valor probante dos documentos eletrônicos, bem como a assinatura digital.

O projeto de lei trata de comércio eletrônico, ofertante, destinatário, intermediário; normas de proteção e de defesa do consumidor; eficácia jurídica e

falsidade dos documentos eletrônicos; certificados eletrônicos privados e públicos, e responsabilidade, sanções administrativas e penais dos tabeliães.

Relativamente à certificação feita por particular, normatiza o art. 17 que é uma declaração de que a chave pública certificada pertence ao titular indicado e não gera presunção de autenticidade perante terceiros. Completando, o art. 24 diz que esses serviços prestados são de caráter comercial, essencialmente privados e não se confundem em seus efeitos com a atividade de certificação por tabelião.

Nos arts. 25 a 49, o projeto detalha os certificados eletrônicos públicos, a atividade notarial e sanções administrativas e penais.

Desse tratamento desproporcional entre a atividade de certificação privada e pública, especificamente no art. 16 (a certificação feita pelo tabelião faz presumir sua autenticidade) e no art. 17 (a certificação feita por particular não gera presunção de autenticidade perante terceiros), surgiram diversas críticas ao projeto (vide subtópico 4.9 acima).

Assim como a MP 2.200-2, o projeto não adota posição de neutralidade no que se reporta ao sistema de certificação, definindo compulsoriamente que documento eletrônico é aquele no qual se emprega a criptografia assimétrica (art. 14).

O art. 15 estabeleceu a presunção de veracidade em relação ao signatário desde que a assinatura digital seja única e exclusiva para o documento assinado; seja passível de verificação; seja gerada sob o exclusivo controle do signatário; esteja de tal modo ligada ao documento eletrônico que, em caso de posterior alteração deste, a assinatura seja invalidada, e não tenha sido gerada posteriormente à expiração, revogação ou suspensão das chaves.

Queiroz (2001, p. 405) bem resume os aspectos relacionados com a eficácia jurídica dos documentos eletrônicos, no projeto ora em estudo:

> "Estabelece que os documentos elaborados diretamente em meio digital são considerados originais (art. 14, "caput"), sendo cópia a ulterior materialização física daquele (§ 1.º do art. 14), sendo esta passível de autenticação pelo escrivão (§ 2.º do art. 14).
>
> O Projeto consigna expressamente que a cópia simples do documento eletrônico (isto é, aquela que não foi autenticada) terá o mesmo valor do original, desde que não seja impugnada pela parte contra quem foi

> lançada (art. 15). Cuida-se, a nosso ver, de uma evolução que, segundo esperamos, deverá ter aplicação analógica a todo tipo de documento utilizado judicialmente, especialmente àqueles trasladados para a formação do agravo de instrumento, que muitos tribunais ainda exigem sejam autenticados".

De nossa parte, concluímos que conviria o acolhimento pelo legislador das críticas doutrinárias à distinção entre AC pública e privada, com a ressalva de que fossem mantidas as sanções civis e penais aos representantes das AC, em caso de prática de ilícito ou de infração à norma legal.

Nesse aspecto, adotando-se simplesmente o critério estabelecido na Medida Provisória n.º 2.200-2/01 e, portanto, excluindo-se todos os artigos que se referem ao tabelião público virtual, terá o Projeto de Lei em exame o mérito de bem estabelecer as normas para as contratações por meio eletrônico, a validade e o valor probante dos documentos eletrônicos, os direitos do consumidor e a assinatura digital.

6 CONCLUSÕES

Neste trabalho, buscou-se demonstrar, pela sua importância, a maneira de conferir-se segurança a todas as manifestações de vontade expressas através de meio eletrônico, mormente quando envolvendo valores patrimoniais (ex.: contratos celebrados entre duas partes, sejam elas pessoas físicas ou jurídicas) ou decisões relacionadas com a Justiça, na próxima etapa de evolução tecnológica que o Poder Judiciário fatalmente deverá atingir.

Diante do desconhecido, deve-se desvendá-lo. Conhecendo-o, adquire-se confiança. À medida que essa confiança for se generalizando, resultará a credibilidade que a sociedade depositará nos documentos eletrônicos.

No tocante à legislação pertinente ao documento eletrônico, não obstante encaremos as medidas provisórias com certa reserva pelo conteúdo autoritário de que se revestem, pode dizer-se que a Medida Provisória n.º 2.200-2, de 24/08/2001, foi de extrema felicidade.

Em apenas vinte artigos "enxutos", estabeleceu a natureza jurídica dos documentos e contratos eletrônicos autenticados digitalmente, considerando-os documentos públicos ou particulares, para todos os fins legais, conferindo-lhes presunção de veracidade e determinou que a autenticação digital dos documentos eletrônicos seja feita pelo sistema de chave assimétrica, designando o Instituto Nacional de Tecnologia da Informação - ITI como a Autoridade Certificadora Raiz.

Quanto ao Projeto de Lei n.º 1.589/99, em tramitação no Congresso, ressalvem-se os seus méritos ao definir as obrigações dos comerciantes eletrônicos e as cominações penais aplicáveis aos agentes infratores. Contudo, no que tange à assinatura eletrônica, o PL privilegia a figura do tabelião virtual. Em razão desse particular, concluímos ser mais eficaz a metodologia estabelecida pela medida provisória anteriormente focalizada.

Relativamente à tecnologia das chaves assimétricas, se hoje podem ser consideradas extremamente seguras, não é possível prever por mais quanto tempo essa segurança perdurará. Novo método poderá surgir substituindo o atual

porque é inerente à criptografia a exigência de contínuo e permanente aperfeiçoamento.

Por enquanto, diante do valor probatório que a MP 2.200-2 atribui ao sistema de chaves assimétricas, convém que todas as entidades, públicas e privadas, ao criarem suas Certificadoras Autorizadas, vinculem-se à Autoridade Certificadora - Raiz, o ITI. Assim procedendo, evitar-se-á que documentos eletrônicos tenham a sua validade questionada, porque somente aos autenticados, obedecendo-se aos requisitos estabelecidos pela MP, atribuir-se-á a presunção de veracidade.

Além disso, com o crescimento na quantidade de CA no mercado, a existência de uma só AC-Raiz, única e conhecida no País inteiro, contribuirá para facilitar a operacionalização por parte dos milhares de usuários, além de não sobrecarregar desnecessariamente seus computadores.

Uma outra conclusão a que o autor chegou é que, se no aspecto jurídico a MP 2.200-2 equacionou quase que plenamente a questão, no aspecto técnico da certificação digital encontra-se razoável grau de dificuldade em se apreender o assunto.

Quanto às fontes de pesquisa, estas dificuldades podem ser sintetizadas conforme abaixo.

Relativamente aos artigos apresentados em sites, a maioria aborda o tema teoricamente de forma genérica e superficial. Somente um ou outro autor faz uma abordagem completa sobre a proposta por ele apresentada.

Já os livros teóricos são muito úteis na parte teórica, obviamente. Na parte prática, para os iniciantes, como foi o caso do monografista, falta o detalhamento através de exemplos concretos.

Com referência aos livros práticos, não há literatura farta especificamente sobre o tema. Muitos autores enfocam a certificação digital como parte de suas obras. Mesmo apresentando inúmeros gráficos e figuras, mostrando as telas tal qual apareceriam em nossos computadores, em algumas situações, a matéria continua parcialmente incompreensível. Para isso contribuem as referências a

inúmeras siglas, terminologia técnica e estrangeira e nomes de *hardwares* e *softwares* que só são conhecidos por técnicos e especialistas do ramo.

Sites específicos de Certificadoras Autorizadas foram consultados. No tópico 4.8.1, analisou-se a ICP da OAB-SP. Em outro site de entidade privada, consultou-se o da CertiSign <http://www.certisign.com.br>. Traz muitas informações e esclarecimentos, mas não soluciona todas as dúvidas dos neófitos, principalmente as dúvidas práticas. Aquela CA, mediante prévia inscrição, disponibiliza alguns cursos em São Paulo (SP), com duração de um a três dias e carga diária de oito horas. O curso para interessados em certificação digital, pessoa física, seria de dois dias, custando aproximadamente R$ 2.400,00.

Considerando-se o valor elevado, inacessível para grande parte dos interessados, conclui-se que somente com a prática, exercitando, errando, corrigindo e aprendendo, poder-se-á assinar digitalmente com segurança e tranqüilidade.

Colaborando para atingir-se esse mister, repetimos, é louvável a maneira como a OAB-SP disponibilizou a sua certificação digital aos advogados, sob a forma de teste.

Iniciativas semelhantes contribuirão para que a assinatura digital seja popularizada e adquira credibilidade. De início, poderão ocorrer desconfianças e erros, da mesma forma que na sistemática, hoje em uso, de senha e cartão de clientes de bancos. Nessa modalidade ainda ocorrem falhas que não podem ser imputadas a procedimentos incorretos por parte dos clientes. No sistema da assinatura digital, acreditamos, serão raros e quase impossíveis de ocorrer erros, excetuados aqueles derivados de desinformação, não observância dos requisitos de segurança e até ingenuidade do usuário. Se acontecerem, limitar-se-ão a casos excepcionais envolvendo valores patrimoniais ou extra-patrimoniais fora da esfera de interesse da maioria dos mortais.

Diante da tecnologia envolvendo o emprego do certificado digital, da legislação vigente e de tudo o mais que foi pesquisado, pode-se deduzir que há plena eficácia e segurança, para todas as partes, nas vontades expressas nos

documentos eletrônicos.

7 REFERÊNCIAS BIBLIOGRÁFICAS

ALBERTIN, Alberto Luiz. **Comércio eletrônico:** modelo, aspectos e contribuições de sua aplicação. São Paulo: Atlas, 1999, 220 p.

ARAÚJO, Kleitor Franklint Correa de. **ASP:** Active server pages técnicas e estratégias. São Paulo: Érica, 2001, 348 p.

COSTA, Marcos da. **Movimentações financeiras eletrônicas no mercado bancário.** In: GRECO, Marco Aurelio; MARTINS, Ives Gandra da Silva (Coords.). **Direito e Internet:** relações jurídicas na sociedade informatizada. São Paulo: RT, 2001, 257p.

DINIZ, Davi Monteiro. **Documentos eletrônicos, assinaturas digitais:** da qualificação jurídica dos arquivos digitais como documentos. São Paulo: LTr, 1999, 64p.

GRECO, Leonardo. **O processo eletrônico.** In: GRECO, Marco Aurelio; MARTINS, Ives Gandra da Silva (Coords.). **Direito e Internet:** relações jurídicas na sociedade informatizada. São Paulo: RT, 2001, 257p.

LIMA NETO, José Henrique Barbosa Moreira. **Assinatura digital e a eficácia probatória dos contratos eletrônicos.** Rio de Janeiro: CEPAD, 1997. Fita de vídeo.

LORENZETTI, Ricardo Luis. **Informática, cyberlaw, e-commerce.** In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coords.). **Direito & Internet:** aspectos jurídicos relevantes. São Paulo: Edipro, 2001, 512p.

LOTUFO, Renan. **Responsabilidade civil na Internet.** In: GRECO, Marco Aurelio; MARTINS, Ives Gandra da Silva (Coords.). **Direito e Internet:** relações jurídicas na sociedade informatizada. São Paulo: RT, 2001, 257p.

LUCCA, Newton de. **Títulos e contratos eletrônicos:** O advento da informática e seu impacto no mundo jurídico. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coords.). **Direito & Internet:** aspectos jurídicos relevantes. São Paulo: Edipro, 2001, 512p.

LUCON, Paulo Henrique dos Santos. **Competência no comércio e no ato ilícito eletrônico.** In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coords.). **Direito & Internet:** aspectos jurídicos relevantes. São Paulo: Edipro, 2001, 512p.

MARZOCHI, Marcelo de Luca. **Direito.br:** aspectos jurídicos da Internet no Brasil. São Paulo: LTr, 2000, 109 p.

MATTE, Maurício. **Internet - comércio eletrônico:** aplicabilidade do Código de Defesa do Consumidor nos contratos de e-commerce. São Paulo: LTr, 2001, 143 p.

MITCHELL, Scott. **Projetando active server pages.** Trad.: Eveline Vieira Machado. Rio de Janeiro: Ciência Moderna, 2001.

NUNES, Luiz Antonio Rizzatto. **Manual da monografia jurídica:** como se faz: uma monografia, uma dissertação, uma tese. 2.ed. rev. e ampl. São Paulo: Saraiva, 1999, 209 p.

QUEIRÓZ, Regis Magalhães Soares de. **Assinatura digital e o tabelião virtual.** In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coords.). **Direito & Internet:** aspectos jurídicos relevantes. São Paulo: Edipro, 2001, 512p.

REQUIÃO, Rubens. **Curso de Direito Comercial.** 23.ed. São Paulo: Saraiva, 1998, v.1.

RODRIGUES, Silvio. **Direito Civil:** Dos contratos e das declarações unilaterais da vontade. 15.ª ed. São Paulo: Saraiva, 1986.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico.** 21.ed. rev. e ampl. São Paulo: Cortez, 2000, 279 p.

STARLIN, Gorki. NOVO, Rafael. **Segurança na Internet:** Microsoft Proxy Cache & Novell Border Manager. Rio de Janeiro: Book Express, 1998. 256 p.

STREBE, Mattew; PERKINS, Charles. **Firewalls.** Trad. Lavio Pareschi. São Paulo: Makron, 2002.

THEODORO JÚNIOR, Humberto. **Curso de direito processual civil:** teoria geral do direito processual civil e processo de conhecimento. 31.ed. Rio de Janeiro: Forense, 2000, v.1.

TUCCI, José Rogério Cruz e. **Eficácia probatória dos contratos celebrados pela Internet.** In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coords.). **Direito & Internet:** aspectos jurídicos relevantes. São Paulo: Edipro, 2001, 512p.

VENTURA, Luis Henrique. **Comércio e contratos eletrônicos:** aspectos jurídicos. São Paulo: Edipro, 2001, 134 p.

WALD, Arnoldo. **Um novo direito para a nova economia:** os contratos eletrônicos e o Código Civil. In: GRECO, Marco Aurelio; MARTINS, Ives Gandra da Silva (Coords.). **Direito e Internet:** relações jurídicas na sociedade informatizada. São Paulo: RT, 2001, 257p.

ANEXOS

ANEXO A - Medida Provisória n.º 2.200-2, de 24 de agosto de 2001.

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1.º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, 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.

Art. 2.º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3.º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:
I - Ministério da Justiça;

II - Ministério da Fazenda;
III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;
IV - Ministério do Planejamento, Orçamento e Gestão;
V - Ministério da Ciência e Tecnologia;
VI - Casa Civil da Presidência da República;
VII - Gabinete de Segurança Institucional da Presidência da República.
§ 1.º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.
§ 2.º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.
§ 3.º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.
§ 4.º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4.º Compete ao Comitê Gestor da ICP-Brasil:
I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;
II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;
III - estabelecer a política de certificação e as regras operacionais da AC Raiz;
IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;
V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;
VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC

e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais;

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.

Art. 5.º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

Art. 6.º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os

certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.
Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

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

Art. 8.º Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Art. 9.º É vedado a qualquer AC certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.
§ 1.º 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 n.º 3.071, de 1.º de janeiro de 1916 - Código Civil.
§ 2.º 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.

Art. 11. A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei n.º 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.

Art. 12. Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal.

Art. 13. O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.

Art. 14. No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei.

Art. 15. Integrarão a estrutura básica do ITI uma Presidência, uma Diretoria de Tecnologia da Informação, uma Diretoria de Infra-Estrutura de Chaves Públicas e uma Procuradoria-Geral.
Parágrafo único. A Diretoria de Tecnologia da Informação poderá ser estabelecida na cidade de Campinas, no Estado de São Paulo.

Art. 16. Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.
§ 1.º O Diretor-Presidente do ITI poderá requisitar, para ter exercício exclusivo na Diretoria de Infra-Estrutura de Chaves Públicas, por período não superior a um ano, servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a

serem exercidas.
§ 2.º Aos requisitados nos termos deste artigo serão assegurados todos os direitos e vantagens a que façam jus no órgão ou na entidade de origem, considerando-se o período de requisição para todos os efeitos da vida funcional, como efetivo exercício no cargo, posto, graduação ou emprego que ocupe no órgão ou na entidade de origem.

Art. 17. Fica o Poder Executivo autorizado a transferir para o ITI:
I - os acervos técnico e patrimonial, as obrigações e os direitos do Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia;
II - remanejar, transpor, transferir, ou utilizar, as dotações orçamentárias aprovadas na Lei Orçamentária de 2001, consignadas ao Ministério da Ciência e Tecnologia, referentes às atribuições do órgão ora transformado, mantida a mesma classificação orçamentária, expressa por categoria de programação em seu menor nível, observado o disposto no § 2.º do art. 3.º da Lei n.º 9.995, de 25 de julho de 2000, assim como o respectivo detalhamento por esfera orçamentária, grupos de despesa, fontes de recursos, modalidades de aplicação e identificadores de uso.

Art. 18. Enquanto não for implantada a sua Procuradoria Geral, o ITI será representado em juízo pela Advocacia Geral da União.

Art. 19. Ficam convalidados os atos praticados com base na Medida Provisória n.º 2.200-1, de 27 de julho de 2001.

Art. 20. Esta Medida Provisória entra em vigor na data de sua publicação.

Brasília, 24 de agosto de 2001; 180.º da Independência e 113.º da

República.

FERNANDO HENRIQUE CARDOSO
José Gregori
Martus Tavares
Ronaldo Mota Sardenberg
Pedro Parente