ICP – BRASIL

Edilane Del Rio Copalo

RESUMO

Examina sucintamente a evolução tecnológica da nova era digital e sua relação com o Direito, bem como de que forma isso contribui para a formação de uma sociedade da informação no Brasil, surgida com a criação de sistemas aplicativos como, por exemplo: o Posto Fiscal Eletrônico (PFE), em São Paulo; o Cartão Nacional de Saúde (CNS), do Ministério da Saúde; o Projeto Interlegis, do Senado Federal; e o Sistema Comprasnet, do Ministério do Planejamento.

Comenta sobre o uso da criptografia como mecanismo auxiliar na manutenção da privacidade das informações.

Trata da inserção da ICP – Brasil, Infra-estrutura de Chaves Públicas, cuja função é garantir a integridade e a autenticidade dos documentos produzidos ou transmitidos eletronicamente. Para isso, expõe sua estrutura, finalidade, repercussão e legislação pertinente.

Acredita ser fundamental a aplicação da tecnologia da informação para o aperfeiçoamento da gestão governamental do País em todos os níveis.

PALAVRAS-CHAVE

Tecnologia da Informação; Direito da Informática; ICP – Brasil – Infra-estrutura de Chaves Públicas; internet; criptografia; Medida Provisória n. 2.200.

* Conferência proferida no "Congresso Internacional de Direito e Tecnologias da Informação", realizado pelo Centro de Estudos Judiciários, nos dias 3 e 4 de outubro de 2002, no auditório do Superior Tribunal de Justiça, Brasília-DF.

1 INTRODUÇÃO: O DIREITO E A EVOLUÇÃO TECNOLÓGICA.

Assistir à televisão, falar ao telefone, movimentar a conta no terminal bancário e, pela internet, verificar multas de trânsito, comprar discos, trocar mensagens com o outro lado do planeta, pesquisar e estudar são hoje atividades cotidianas, no mundo inteiro e no Brasil. Rapidamente nos adaptamos a essas novidades e passamos – em geral, sem uma percepção clara nem maiores questionamentos – a viver na sociedade da informação, uma nova era em que a informação flui a velocidades e em quantidades há apenas poucos anos inimagináveis, assumindo valores sociais e econômicos fundamentais.

Como essa revolução vem acontecendo? Que conseqüências tem trazido para as pessoas, as organizações e o conjunto da sociedade? São perguntas cuja importância mal percebemos e as quais, na maioria das vezes, não nos preocupamos em responder.

Subjacente a todas aquelas atividades corriqueiras há uma imensa malha de meios de comunicação que cobre países inteiros, interliga continentes e chega às casas e empresas: são fios de telefone, canais de microondas, linhas de fibras óticas, cabos submarinos transoceânicos, transmissões via satélite. São computadores, que processam informações, controlam, coordenam e tornam compatíveis os diversos meios. Aglutinando e dando sentido à estrutura física, estão as pessoas que a operam ou dela se utilizam. Tal é a capacidade de transmissão e a qualidade dos serviços oferecidos, que o usuário nem percebe todo o complexo aparato que apóia esses serviços, e a maioria das pessoas não tem a menor idéia de como é feita a comunicação – se pela transmissão sem fio de um telefone celular, pelo canal de um satélite em órbita, ou por um cabo no fundo do oceano. O conjunto desses recursos forma uma verdadeira superestrada de informações e serviços freqüentemente chamada de "infovia" ou "supervia".

Três fenômenos inter-relacionados estão na origem da transformação em curso. O primeiro, a convergência da base tecnológica, decorre do fato de se poder representar e processar qualquer tipo de informação de uma única forma, a digital. Pela digitalização, a computação (a informática e suas aplicações), as comunicações (transmissão e recepção de dados, voz, imagens etc.) e os conteúdos (livros, filmes, pinturas, fotografias, música etc.) aproximam-se vertiginosamente – o computador vira um aparelho de TV, a foto favorita sai do álbum para um disquete, e pelo telefone entra-se na internet. Um extenso leque de aplicações abre-se com isso, função apenas da criatividade, curiosidade e capacidade de absorção do novo pelas pessoas.

O segundo aspecto é a dinâmica da indústria, que tem proporcionado contínua queda dos preços dos computadores relativamente à potência computacional, permitindo a popularização crescente do uso dessas máquinas.

Finalmente, em grande parte como decorrência dos dois primeiros fenômenos, o terceiro aspecto na base dessa revolução é o fantástico crescimento da internet: nos EUA, a internet atingiu 50 milhões de usuários em somente quatro anos, enquanto, para atingir esse número de usuários, o computador pessoal tardou 16 anos, a televisão, 13, e o rádio, 38. Outro dado que confirma a rapidez da disseminação da internet é o da evolução da conectividade internacional no período de 1991 a 1998.

No curto período de oito anos, a internet se disseminou por praticamente todo o mundo, propiciando conectividade a países até então fora de redes e substituindo outras tecnologias mais antigas. Mesmo ainda sendo, em muitos países, um serviço restrito a poucos, a velocidade da disseminação da internet, em comparação com a de outros serviços, mostra que ela se tornou um padrão de fato e que se está diante de um fenômeno singular, a ser considerado como fator estratégico fundamental para o desenvolvimento das nações.

A sociedade da informação não é um modismo. Representa uma profunda mudança na organização da sociedade e da economia, havendo quem a considere um novo paradigma técnico-econômico. É um fenômeno global, com elevado potencial transformador das atividades sociais e econômicas, uma vez que a estrutura e a dinâmica dessas atividades inevitavelmente serão, em alguma medida, afetadas pela infra-estrutura de informações disponível. É também acentuada sua dimensão político-econômica, decorrente da contribuição da infra-estrutura de informações para que as regiões sejam mais ou menos atraentes em relação aos negócios e empreendimentos. Sua importância assemelha-se à de uma boa estrada de rodagem para o sucesso econômico das localidades. Tem ainda marcante dimensão social, em virtude do seu elevado potencial de promover a integração, ao reduzir as distâncias entre pessoas e aumentar o seu nível de informação.

Não é livre de riscos, entretanto. Noventa por cento da população do planeta jamais teve acesso ao telefone. Como evitar, então, que as novas tecnologias aumentem ainda mais a disparidade social entre as pessoas, as nações e os blocos de países? Os países e blocos políticos, desde meados da década de 1990, defrontam-se com as oportunidades e os riscos que cercam o futuro e, reconhecendo a importância estratégica da sociedade da informação, vêm tomando iniciativas para assegurar que essa nova era venha em seu benefício.

2 A SOCIEDADE DA INFORMAÇÃO NO BRASIL

Em cada país, a sociedade da informação está sendo construída em meio a diferentes condições e projetos de desenvolvimento social, segundo estratégias moldadas de acordo com cada contexto. As tecnologias envolvidas vêm transformando as estruturas e as práticas de produção, comercialização e consumo e de cooperação e competição entre os agentes, alterando, enfim, a própria cadeia de geração de valor. Do mesmo modo, regiões, segmentos sociais, setores econômicos, organizações e indivíduos são afetados diferentemente pelo novo paradigma, em função das condições de acesso à informação, da base de conhecimentos e, sobretudo, da capacidade de aprender e inovar.

Os países economicamente desenvolvidos, bem como boa parte daqueles em vias de desenvolvimento já adotam políticas e iniciativas voltadas para a sociedade da informação.

Ao Brasil urge acelerar o processo de articulação efetiva de um programa nacional para a sociedade da informação. Ao longo da década de 1990, registraram-se sucessos em aspectos críticos para a formulação e implementação de tal programa. A internet brasileira teve grande impulso, primeiramente na comunidade científica e, logo após, como plataforma de expansão do setor privado, estando aberta também a serviços de natureza comercial desde 1995. Nas telecomunicações, houve a privatização de todo o sistema brasileiro e

a criação da Agência Nacional de Telecomunicações (Anatel), fatores que estão permitindo maior e mais rápida disponibilidade de acesso aos meios de comunicação. As atividades comerciais no Brasil que se valem da internet estão ganhando enorme expressão, a ponto de perfazerem praticamente metade do mercado latino-americano em número de usuários, bem como em volume de transações e negócios. Algumas aplicações de governo têm tido enorme impacto, tanto na melhoria da eficiência interna de funcionamento como na prestação de serviços ao cidadão. E, por último, comparativamente com a América Latina, existe uma sofisticada base tecnológica instalada no País e um considerável contingente de recursos humanos qualificados, abarcando desde pesquisa e desenvolvimento até fomento a empreendimentos.

> No curto período de oito anos, a internet se disseminou por praticamente todo o mundo, propiciando conectividade a países até então fora de redes e substituindo outras tecnologias mais antigas. Mesmo ainda sendo, em muitos países, um serviço restrito a poucos, a velocidade da disseminação da internet, em comparação com a de outros serviços, mostra que ela se tornou um padrão de fato e que se está diante de um fenômeno singular, a ser considerado como fator estratégico fundamental para o desenvolvimento das nações.

O País dispõe, pois, dos elementos essenciais para a condução de uma iniciativa nacional rumo à sociedade da informação. E a emergência do novo paradigma constitui, para o Brasil, oportunidade sem precedentes de prestar significativa contribuição para resgatar a sua dívida social, alavancar o desenvolvimento e manter uma posição de competitividade econômica no cenário internacional. A inserção favorável nessa nova onda requer, entretanto, além de base tecnológica e de infra-estrutura adequadas, um conjunto de condições e de inovações nas estruturas produtivas e organizacionais, no sistema educacional e nas instâncias reguladoras, normativas e de governo em geral. O impacto positivo que a "nova economia" pode gerar para o País depende ainda da participação do maior número possível de pessoas, organizações e regiões como usuárias ativas das redes avançadas de informação.

2.1 SISTEMAS APLICATIVOS

Há no Brasil pelo menos duas aplicações de governo utilizando a internet que são modelares e de padrão mundial, a saber: a declaração de imposto de renda; a votação em eleições gerais.

Por outro lado, no nível federal, há, em estágios diversos (desde o estágio de concepção até o estágio de operação), várias aplicações que utilizam tecnologias de informação e comunicação com potencial de revolucionar a gestão de serviços públicos nas suas áreas de atuação.

2.1.1 ARRECADAÇÃO FAZENDÁRIA

Está em funcionamento, na Secretaria de Receita do Estado de São Paulo, o Posto Fiscal Eletrônico (PFE), reprodução de um posto fiscal físico, disponível na internet e acrescido de facilidades e benefícios, como a prestação de serviços com qualidade e precisão impossíveis pelos meios tradicionais. O PFE mantém informações atualizadas, procedimentos, legislação, orientações e serviços ao contribuinte em geral.

Ainda no âmbito fazendário, inúmeras ações estão em curso. O Sistema Integrado de Informações sobre Operações Interestaduais com Mercadorias (Sintegra) está sendo implantado em todo o País, com o objetivo de facilitar o fornecimento de informação dos contribuintes aos fiscos estaduais, bem como a troca de dados entre as diversas unidades da Federação. A implantação definitiva do Sintegra deverá estar concluída em todos os estados em 2001.

2.1.2 CARTÃO NACIONAL DE SAÚDE (CNS), DO MINISTÉRIO DA SAÚDE

O Cartão Nacional de Saúde (CNS) é uma iniciativa do Ministério da Saúde que visa a informatizar todos os serviços de atendimento ambulatório/hospitalar do Sistema Único de Saúde (SUS) no País, mediante introdução de um cartão identificando cada usuário do sistema. Na versão inicial, trata-se fisicamente de um cartão magnético que está sendo testado concomitantemente à implantação de um sistema em 44 municípios do País, cobrindo uma população de mais de 12 milhões de pessoas, atendidas por 2.027 unidades ambulatórias, 300 hospitais e 11.740 consultórios.

O sistema envolve a disponibilização em cada unidade de saúde de equipamentos terminais que permitirão a coleta e a consistência de dados de cada tratamento e o seu envio a um centro municipal, onde a autorização de tipos de tratamento, a tabulação cumulativa de transações e o controle de dispêndios serão feitos. Os centros municipais estarão ligados a um centro por estado, e os centros estaduais estarão interconectados entre si e a dois centros nacionais (no Ministério da Saúde, em Brasília, e no Datasus, no Rio de Janeiro) por meio de uma rede. As características técnicas do sistema enfatizam o uso de padrões abertos de tal forma a estimular o desenvolvimento futuro de aplicações cada vez mais descentralizadas e especializadas, mas sempre compatíveis com o cartão. Por outro lado, a própria evolução do cartão para meios como o *smart cards* abrirá caminho para a introdução de funções como a de prontuário médico em meios eletrônicos.

2.1.3 PROJETO INTERLEGIS, DO SENADO FEDERAL

O Projeto Interlegis visa a montar uma rede de comunicação e participação legislativa no País, interligando casas legislativas dos três níveis de governo. Seus objetivos expressos são a melhoria da comunicação e do fluxo de informações entre as casas legislativas e a promoção da participação do cidadão nos processos legislativos.

Iniciado em 1997, o projeto visa a implantar uma rede dedicada interligando as 27 Assembléias Legislativas Estaduais, compondo assim a chamada "Rede Interlegis".

2.1.4 COMPRASNET, DO MINISTÉRIO DO PLANEJAMENTO

O ComprasNet é um sistema *on-line* que permite acessar todos os

convites, tomadas de preços e concorrências realizados pela Administração Federal direta, autárquica e fundacional, além de outros serviços e facilidades que visam a aumentar a transparência das compras e as oportunidades de negócios para as empresas. É passo fundamental para a modernização e a desburocratização dos processos de aquisição, tendo como objetivo principal dotar a sociedade de um instrumento que utilize as inovações tecnológicas da internet, para oferecer facilidades aos fornecedores e, ao mesmo tempo, gerar economia para o Governo Federal, por intermédio da adoção de novos padrões de qualidade e produtividade.

> Um sistema criptográfico, por mais robusto que seja o algoritmo utilizado, não é mais forte do que o seu elemento fraco – o humano. A implementação prática de um sistema criptográfico é delicada e complexa, e pode ter várias falhas onde menos se espera. Por outro lado, deve-se prever que um atacante não vai escolher a solução mais difícil, como tentar quebrar a chave do algoritmo, mas vai tentar obtê-la por outros meios.

O ComprasNet oferece, entre outros, os seguintes serviços e informações: legislação, publicações, áreas de acesso a fornecedores, serviços de livre acesso (consulta a licitações, a contratos do Governo Federal, a linhas de fornecimento de material e serviço e à publicação do fornecedor, serviços por assinatura etc).

Essas aplicações guardam diversas características comuns entre si. Primeiramente, elas se valem de um mesmo conjunto de opções tecnológicas, derivadas da tecnologia internet. Segundo, verticalizam ações em infra-estrutura de redes. Terceiro, são coordenadas centralmente, com uma visão gerencial de médio/longo prazo.

Nos Estados, as aplicações têm adquirido uma tendência natural (e extremamente positiva) a serem mais próximas de atendimento ao cidadão comum, em locais específicos para tal e também em locais de acesso público (via quiosques, telecentros etc). Um exemplo muito interessante nessa classe de aplicações é o de serviços de obtenção de documentos e atestados, abertura de empresas, pagamento de impostos etc., que têm vicejado em diversos Estados sob diferentes nomes (exemplo: Serviço de Atendimento ao Cidadão, Poupa-Tempo etc.) e que, aliás, foram a inspiração de alguns serviços similares em outros países, inclusive na União Européia. Do ponto de vista de tecnologias de informação e comunicação, tais aplicações têm ainda um corte bastante conservador, tendo tido êxito até agora mais por uma revolução na atitude governamental quanto a como prestar serviços do que por qualquer salto de qualidade no uso de tecnologias. Quanto ao uso de tecnologias, as tendências recentes são interessantes: essas aplicações fatalmente ganharão um braço de disseminação por meio de redes para pontos remotos de acesso, via quiosques, centros comunitários etc.

3 A CRIPTOGRAFIA E A SEGURANÇA

A criptografia nasceu da necessidade de manter a privacidade de informações. Na definição do dicionário *Michaelis*, **criptografia** é a arte ou processo de escrita em caracteres secretos ou em cifras. Desde a antigüidade, já se tinha conhecimento da criptografia, na qual era utilizada a substituição ou a troca dos símbolos com o objetivo de confundir um possível interceptador das mensagens. Para a computação, esse princípio é mantido, porém a escrita é substituída pelo processamento digital da informação e com a capacidade de processamento de dados desta tecnologia; a criptografia ganhou corpo e desenvolveu-se.

A segurança dos dados criptografados é inversamente proporcional à facilidade de quebra do código cifrado, geralmente fundamentado na utilização de chaves de codificação e que são, em alguma instância, de conhecimento do emissor e do receptor dos dados. Assim sendo, quando afirmamos a segurança da criptografia, na verdade estamos afirmando que o esforço necessário para a quebra do código cifrado, obtendo a mensagem original, é muito grande se considerados os recursos, conhecimentos e tecnologias atuais, o que torna esta prática inviável. Um outro ponto relevante é que a segurança de um algoritmo criptográfico nunca pode estar vinculada a um segredo de funcionamento. De fato, quanto mais conhecido e explorado o algoritmo, mais seguro ele pode ser considerado. Assim, temos introduzido o conceito de segurança em relação à criptografia.

Com recursos matemáticos aliados ao poder computacional, foram desenvolvidos algoritmos que dificultam imensamente que os dados encriptados com uma determinada chave de codificação possam ser decriptados sem seguir a correta política previamente definida por esse algoritmo. O esforço computacional e o tempo que devem ser despendidos para quebrar um algoritmo ou para descobrir qual a chave que pode decriptar a informação não compensam a utilização desses métodos, tornando, assim, a criptografia um meio seguro de confidencializar a informação.

Durante décadas, a criptografia ficou calcada nas técnicas de permutação e substituição de símbolos, em que as partes envolvidas na comunicação entravam em acordo sobre os parâmetros de troca ou substituição (chave de codificação) e, após esse acordo, as mensagens codificadas eram trocadas por um meio inseguro qualquer; porém, durante a fase de acordo e conclusão dos parâmetros a serem utilizados (chaves de codificação), esta informação precisava ser trocada entre as partes e, portanto, circular num meio inseguro, no qual poderia ser interceptada.

A técnica da criptografia simétrica, ou de chave privada, remete-nos a três problemas fundamentais. O primeiro diz respeito à troca de chave, pois, como esta deve ser compartilhada entre as partes, em algum momento ela deve ser enviada pelo meio ainda inseguro, sendo este envio da chave um ponto de forte vulnerabilidade. O segundo problema está relacionado à assinatura das mensagens, pois as duas partes conhecem a chave e portanto são capazes de gerar mensagens codificadas sem, no entanto, termos como nos certificar sobre qual das partes originou a mensagem. Este é um pro-

blema de autenticação ou assinatura da mensagem, fator de extrema importância em aplicações com fins comerciais ou militares, onde é fundamental a validação dos autores das informações geradas. E o terceiro problema reside no fato de que cada par, emissor/receptor, necessita de uma chave para se comunicar de forma segura. Sendo assim, para uma rede de "n" usuários seria necessário uma grande quantidade de chaves, quantidade esta que dificulta sua gerência.

Em 1976, Whitfield Diffie e Martin Hellman, da Universidade de Stanford, Estados Unidos, introduziram publicamente o conceito de criptografia de chave pública ou assimétrica, implementando uma técnica que visava a atacar diretamente os três pontos falhos da criptografia por chave simétrica: o compartilhamento e o gerenciamento das chaves, assim como a autenticação. Tal técnica por eles apresentada utiliza a filosofia das chaves complementares, na qual uma delas é utilizada para codificar os dados, e outra distinta é utilizada para decodificar. A operação executada com a utilização de uma chave só pode ser revestida com a utilização da sua respectiva chave complementar.

Com isso, podemos implementar uma política em que uma das chaves é de conhecimento de todos (chave pública), e a outra é reservada e de conhecimento restrito (chave privada). Essa estratégia permite trocar informações com a combinação de chaves públicas e privadas dos dois indivíduos envolvidos no processo, bem como resolver os três problemas da chave simétrica.

No contexto da criptografia, o processo em que se tenta descobrir o conteúdo de uma mensagem criptografada, a chave utilizada ou ambas é conhecido como criptanálise. A estratégia usada pelo criptanalista depende da natureza do esquema de encriptação e das informações de que dispõe.

O tipo de ataque mais difícil, portanto, em que a segurança da informação é mais garantida, é quando só se dispõe da mensagem cifrada. Nesse caso, se o algoritmo de codificação for seguro, é praticamente impossível descobrir a chave utilizada a partir da análise da informação cifrada, tendo de se testarem todas as chaves possíveis. Este tipo de ataque é conhecido por **tentativa ou erro** ou **força bruta**.

No entanto, embora a robustez e a confiabilidade do algoritmo criptográfico utilizado sejam fundamentais para um processo de codificação seguro, existem vários outros pontos que não devem ser esquecidos ao se implementar uma política de segurança; o ponto mais fraco é geralmente o elemento humano.

Um sistema criptográfico, por mais robusto que seja o algoritmo utilizado, não é mais forte do que o seu elemento fraco – **o humano**. A implementação prática de um sistema criptográfico é delicada e complexa, e pode ter várias falhas onde menos se espera. Por outro lado, deve-se prever que um atacante não vai escolher a solução mais difícil, como tentar quebrar a chave do algoritmo, mas vai tentar obtê-la por outros meios.

4 ICP–BRASIL: FINALIDADE E REPERCUSSÃO

O uso reiterado da assinatura digital e de sua prática em aplicações internas governamentais desencadeou a publicação do Decreto n. 3.587, de 5/9/2000, que estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal, ICP-Gov.

O setor governamental é o principal indutor de ações estratégicas rumo à sociedade da informação. Por quê? Primeiramente, porque cabe ao governo definir o quadro regulatório dentro do qual projetos e iniciativas concretas poderão ser formuladas. Segundo, porque, como regra, o governo é o maior comprador/contratador de bens e serviços de tecnologias de informação e comunicação de um país. Assim, uma decisão do governo em apoio a uma tecnologia ou serviço pode abrir algumas avenidas de atividades ao setor privado, bem como conduzir outras a becos sem saída. Isso posto, suas decisões certamente devem contemplar a satisfação cabal dos requisitos que licitaram a compra/contratação de cada bem ou serviço, mas não devem perder de vista o contexto mais abrangente de atuação no mercado e no apoio concreto a uma política industrial associada a tecnologias de informação e comunicação. Terceiro, porque o governo, com tecnologias de informação e comunicação em suas atividades, pode acelerar o uso dessas tecnologias em toda a economia, em função da maior eficiência e transparência de suas próprias ações.

Com o objetivo de inserir a participação da iniciativa privada no que se refere ao uso de tecnologias de informação e comunicação em âmbito governamental, instituiu-se a ICP-Brasil.

A finalidade da ICP-Brasil, instituída pela Medida Provisória n. 2.200, de 29/6/2001, é garantir integridade e autenticidade aos documentos produzidos ou transmitidos eletronicamente, conferindo validade jurídica à assinatura digital.

O ordenamento jurídico brasileiro utiliza-se do princípio da liberdade de forma. Portanto, as partes têm liberdade de contratar, exceto nos casos em que a lei não prescreve forma especial para a validade do ato jurídico. Não há impedimento legal para a utilização de documentos eletrônicos, seja como forma para documentar atos jurídicos, seja como meio de prova judicial[1]. Segundo o art. 332 do Código de Processo Civil, todos os meios legais, bem como os moralmente legítimos, ainda que não especificados no Código, são hábeis a provar a verdade dos fatos em que se funda a ação ou defesa. De igual maneira, não afronta o art. 5º, inc. LVI, da Constituição Federal, quando diz que são inadmissíveis, no processo, as provas obtidas por meios ilícitos.

A validade jurídica das declarações de vontade não depende de forma especial, senão quando a lei expressamente o exigir (art. 129 do Código Civil). As partes contratantes podem escolher livremente a forma que desejam manifestar a sua vontade, a menos que a lei exija forma especial. Há casos em que a forma escrita é exigida por lei ou por vontade das partes para a celebração do contrato. Logo as declarações de vontade eletrônicas não atendem aos requisitos formais para a validade jurídica do ato jurídico. Os arts. 82 e 129 do Código Civil admitem a utilização da forma verbal de contratação. A inobservância da forma especial prevista em lei, pertencente à essência do ato, culmina com a nulidade do negócio jurídico celebrado entre as partes (art. 130 do Código Civil)[2].

Nem sempre a forma especial é elemento constitutivo do negócio jurídico. Nesse caso, a forma especial é exigida apenas para facilitar a prova, situação em que a declaração de vontade permanecerá válida, mesmo quando não observada a forma prevista em lei. Portanto, a sua omissão não prejudicará a validade da declaração de vontade, mas o valor de prova do documento perante terceiros. Segundo o art. 131 do Código Civil, as declarações constantes de

documentos assinados presumem-se verdadeiras em relação aos signatários. O art. 135 do Código Civil dispõe que o instrumento particular assinado por quem esteja na disposição e administração livre de seus bens, sendo subscrito por duas testemunhas, prova as obrigações convencionais de qualquer valor. Os seus efeitos, no entanto, só se operam perante terceiros depois da transcrição do instrumento no Registro Público. Esses dispositivos legais estabelecem, assim, quais as condições que devem ser preenchidas por um documento para que este tenha valor de prova. Isso não significa, porém, que todos os instrumentos particulares devem ser assinados pelo autor e ainda por duas testemunhas para que sejam válidos; essas condições se referem tão-somente, como já dito, ao valor de prova do documento [3].

O processo de certificação disponibilizado pela ICP-Brasil para os documentos em forma eletrônica é facultativo, uma vez que sua falta não prejudica a validade da declaração de vontade das partes. Sendo a certificação compreendida como obrigatória, ou seja, se a forma exigida por lei é elemento constitutivo do ato jurídico, iremos inviabilizar o comércio eletrônico no País, tornando-o burocrático e caro.

A Medida Provisória n. 2.200 confere à assinatura digital a mesma eficácia e validade jurídica de uma assinatura manual, e declara que seu uso é opcional.

Ao declarar que o uso da certificação é opcional, a Medida Provisória permite, no art. 10, § 2º, a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que se utilizam de certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento. Os documentos eletrônicos não-certificados pela ICP-Brasil terão valor probatório somente entre as partes, não fazendo prova perante terceiros.

Documento eletrônico não é certificação, é gerado a partir de um processo seguro – criptografia – que garante o conhecimento da autoria e da imutabilidade do conteúdo do documento. Esses requisitos estão vinculados para que qualquer documento, seja em papel, seja eletrônico, possa ter validade jurídica.

Nada impede que duas pessoas troquem suas chaves públicas e, por meio de um documento físico, reconheçam validade e eficácia das assinaturas e dos documentos eletrônicos que puderem ser conferidos por meio dessas chaves.

No caso de pessoas conhecidas, a assinatura aposta num documento por um dos envolvidos, seja em papel ou em meio magnético, é plenamente identificada pela outra parte sem necessidade da interferência de um terceiro que assegure que aquela assinatura lhe pertence. Nesse caso, há segurança de que a assinatura é realmente daquele que diz ser. A assinatura digital baseada no sistema de criptografia de chave pública por si só dá segurança relativa à titularidade da parte e à integridade do seu conteúdo. A assinatura digital não prescinde de certificação.

Em negócios envolvendo pessoas desconhecidas, como ter certeza da titularidade da assinatura digital? Surge, então, a função da autoridade certificadora, que irá reconhecer a autenticidade da chave pública.

A certificação deverá ser utilizada naqueles negócios vultosos em que as partes se desconhecem e desejam o reconhecimento da titularidade daquela assinatura digital emitida ou queiram que o documento emitido tenha valor probatório perante terceiros. Os negócios jurídicos corriqueiros realizados pela internet não necessitam de certificação digital, tais como a compra de CD.

A Medida Provisória não coíbe o desempenho da função de certificação por outros entes, que não a ICP-Brasil. O mercado tem liberdade para escolher a entidade certificadora que melhor lhe convier; contudo, o Governo Federal, por meio do Decreto n. 3.996, de 31/10/2001, art. 1º, § 1º, dispõe que os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da ICP-Brasil. Nada impede o credenciamento de pessoas de Direito privado à ICP-Brasil, mediante critérios a serem observados.

A aprovação de uma legislação que regule a assinatura digital aumenta a confiança no comércio eletrônico e evita que outros países que já regulamentaram o assunto tirem do Brasil a sua posição de liderança. Ademais, a legislação de assinatura digital é muito importante para viabilizar as aplicações governamentais, dando uma clara sinalização para os governos estaduais sobre a relevância que está sendo atribuída à matéria.

O Brasil ocupa a liderança do mercado de comércio eletrônico da América Latina, tendo transacionado 450 milhões de dólares em 1999, o que representou cerca de 88% do valor das transações realizadas eletronicamente pelos países latino-americanos. Das transações eletrônicas realizadas no País, em 1999, foram realizadas 88% por empresas da velha economia. No total, 42% são bancos e corretoras, que também ocupam os primeiros lugares no *ranking* das empresas que mais faturam na rede. Enquanto isso, apenas cinco empresas representantes da nova economia figuram na lista das 25 maiores em faturamento na rede, sendo três de *hardware*, uma de telecomunicações e uma de leilão. Entre as 450 lojas virtuais, os produtos e serviços mais vendidos são livros, CDs, computadores e acessórios, serviços de turismo, de corretagem, de venda de automóveis, flores e de leilões [4].

Para desenvolver e apoiar o comércio eletrônico no Brasil, foi criado o Comitê Executivo de Comércio Eletrônico, envolvendo os Ministérios do Desenvolvimento, Indústria e Comércio Exterior, da Ciência e Tecnologia e do Planejamento, Orçamento e Gestão.

É preciso entender o conceito de comércio eletrônico sob dois aspectos: um é o comércio eletrônico como objeto; o outro, o meio eletrônico como instrumento. A legislação brasileira relativa ao comércio eletrônico é suficiente, sendo o Código de Defesa do Consumidor brasileiro um dos mais destacados no mundo inteiro, complementado satisfatoriamente pelo Código Civil, pelo Código Comercial e por uma série de leis esparsas.

No que diz respeito ao instrumento eletrônico, a Medida Provisória n. 2.200 vem garantir eficácia jurídica ao documento eletrônico, a partir de sua criação, pelo sistema de criptografia assimétrica. Os Estados Unidos e a Comunidade Européia dispõem da mesma condição legislativa com relação ao documento eletrônico. Na Alemanha, Itália, Portugal, Espanha e França, as legislações internas asseguram ao documento eletrônico a mesma eficácia do documento em papel. Na América do Sul, o Governo da Argentina expediu um decreto que trata da questão do documento eletrônico no âmbito da administração pública. Também Uruguai e Colômbia já estão em processo de regulamentação da matéria.

A Medida Provisória n. 2.200 adotou o que há de mais moderno no Direito comparado, na medida em que optou por garantir eficácia jurídica ao documento eletrônico, a partir da sua criação, pelo sistema de criptografia assimétrica produzido com a utilização de processo de certificação disponibilizado pela ICP-Brasil. Contudo, não proibiu a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, podendo inclusive serem utilizados certificados não-emitidos pela ICP-Brasil, desde que admitidos pelas partes como válidos ou aceitos pela pessoa a quem for aposto o documento.

Discute-se, em nível mundial, qual o melhor sistema de certificação a ser adotado. Pode-se criar uma hierarquia de certificadoras públicas ou privadas, baseada numa certificadora-raiz que possua as informações de todas as outras certificadoras. Nos Estados Unidos, esse modelo vem sendo duramente criticado, devido à preocupação com privacidade. Observa-se, portanto, uma tendência no sentido de se implantarem sistemas de certificação não-hierárquicos (...)

A primeira lei, no mundo, a regulamentar o uso de assinaturas eletrônicas provém do Estado de Utah, nos Estados Unidos, tendo entrado em vigor em 1995. Depois, no mesmo ano, entrou em vigor na Califórnia lei regulamentando o uso de assinaturas eletrônicas. Menos abrangente do que a do Estado de Utah, que se aplica a qualquer pessoa que queira utilizar-se de assinaturas digitais, a legislação da Califórnia é voltada apenas ao uso de assinaturas eletrônicas em documentos apresentados a órgãos públicos. Muito mais enxuta, esta lei define apenas o que se entende por assinatura digital, atribuindo-lhe a mesma força e efeitos de uma assinatura manual e declarando que seu uso é opcional.

Alguns países só trataram da certificação eletrônica sob o ângulo público, como a Itália, onde somente as certidões emitidas por órgãos públicos têm validade jurídica. Nos Estados Unidos, cujo conceito de responsabilidade difere do adotado na legislação brasileira, as legislações estaduais reconhecem eficácia jurídica inclusive à certidão privada, mas com participação de uma empresa chamada "*Verisign*", a maior certificadora privada do mundo. Desse modo, nos Estados Unidos, a *Verisign* e outras entidades privadas se encarregam da tarefa de comprovar se a pessoa que se apresenta como titular de uma chave pública é efetivamente quem se diz ser. Essa atividade exercida pelas certificadoras privadas exige a adoção de diferentes classes de certificação, a saber: classe 1, com um determinado nível de responsabilidade e indenização; classe 2, com um nível de responsabilidade e indenização mais ampla; classe 3, com responsabilidade e indenização mais próxima do nível pleno, utilizado nos Estados Unidos para atender à base de órgãos públicos, notários, consulados e outras entidades que tenham fé pública, com a finalidade de assegurar plena validade à titularidade da chave pública que esses órgãos certificam.

O sistema de certificação adotado pelo Brasil é baseado numa Autoridade Certificadora-Raiz – AC Raiz – com informações de todas as outras certificadoras e o certificado de nível mais alto, contendo a chave pública correspondente à chave privada da AC Raiz, utilizada para assinar o seu próprio certificado, os certificados das ACs de nível imediatamente subseqüente ao seu e sua Lista de Certificados Revogados.

Discute-se, em nível mundial, qual o melhor sistema de certificação a ser adotado. Pode-se criar uma hierarquia de certificadoras públicas ou privadas, baseada numa certificadora-raiz que possua as informações de todas as outras certificadoras. Nos Estados Unidos, esse modelo vem sendo duramente criticado, devido à preocupação com privacidade. Observa-se, portanto, uma tendência no sentido de se implantarem sistemas de certificação não-hierárquicos, baseados no mútuo reconhecimento e na troca de certificados entre várias certificadoras.

5 ICP-BRASIL: ESTRUTURA E LEGISLAÇÃO.

A estrutura organizacional da ICP-Brasil é composta por uma autoridade gestora de políticas, pelo Comitê Gestor da ICP-Brasil e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz – AC Raiz, pelas Autoridades Certificadoras – AC e pelas Autoridades de Registro – AR.

O Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira – CG ICP-Brasil, instituído pela Medida Provisória n. 2.200, de 28/6/2001, e regulamentado pelo Decreto n. 3.872, de 18/7/2001, dispõe sobre sua estrutura organizacional, composição de membros e competência.

O CG ICP-Brasil é composto por onze membros, sendo quatro representantes da sociedade civil, integrantes de setores interessados, e sete representantes de diversos ministérios, designados pelo Presidente da República. Os representantes da sociedade civil serão designados para o período de dois anos, permitida a recondução. A participação na CG ICP-Brasil não será remunerada.

A estrutura organizacional do CG ICP-Brasil é formada pela Secretaria-Executiva e pela Comissão Técnica Executiva – COTEC. Aquela é chefiada por um secretário-executivo e integrada por assessores especiais e por pessoal técnico e administrativo. Esta é coordenada pelo secretário-executivo do Comitê Gestor e integrada por representantes indicados pelos membros do CG ICP-Brasil e designados pelo Chefe da Casa Civil da Presidência da República.

Compete ao CG ICP-Brasil expedir toda a regulamentação da ICP-Brasil, especialmente: adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil; estabelecer a política, os critérios e as normas para licenciamento das ACs, das ARs e dos demais prestadores de serviços de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação; estabelecer a política de certificação e as regras operacionais da AC Raiz; homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço; estabelecer diretrizes e normas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação; aprovar políticas de certificados e regras operacionais das ACs e das ARs e definir níveis da

cadeia de certificação; aprovar políticas de certificados e regras operacionais, licenciar e autorizar o funcionamento das ACs e das ARs, bem como autorizar a AC Raiz a emitir o correspondente certificado; identificar e avaliar as políticas de ICP externas, quando for o caso, certificar sua compatibilidade com a ICP-Brasil; negociar e aprovar, observados os tratados, acordos e atos internacionais, acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional; bem como 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.

> A assunção pelo Estado do papel intervencionista em muitos segmentos da atividade econômica, como regulador, vem-se mostrando inadequada, em situações especialmente em que o mercado, mediante consumidores organizados, fosse capaz de criar mecanismos de composição. Isso é difícil de acontecer no Brasil, onde não há organização eficiente por parte do usuário.

O CG ICP-Brasil publicou diversas resoluções extensas e extremamente detalhistas. Com estrutura e técnica diversas daquelas empregadas na nossa legislação, essas resoluções contêm várias definições, desde conceitos técnicos como custódia, senha fraca ou óbvia e assinatura digital. Em linhas gerais, as resoluções estabelecem qual deve ser o conteúdo dos certificados de autenticidade das chaves públicas, quem pode exercer as funções de autoridade certificadora, como estes entes deverão operar, seus deveres e responsabilidades, que critérios devem ser observados para emissão, expedição e distribuição do certificado de autenticidade, como se dá a revogação e expiração desses certificados, de que forma é feita a auditoria, bem como quais são os efeitos de uma assinatura digital, para destacar os temas mais relevantes.

A Resolução n. 1, de 25/9/2001, trata da Declaração de Práticas de Certificação e descreve as práticas e os procedimentos empregados pela AC Raiz da ICP-Brasil na execução de seus serviços. Dispõe sobre as obrigações, responsabilidades, controle de segurança técnico e físico, procedimental e de pessoal da AC Raiz. A Resolução n. 4, de 22/11/2001, altera alguns dispositivos da Declaração de Práticas de Certificação da AC-Raiz da ICP-Brasil.

As diretrizes de segurança que deverão ser adotadas pelas entidades participantes da ICP-Brasil estão reguladas pela Resolução n. 2, de 25/9/2001. A Política de Segurança Geral do ICP-Brasil tem por objetivo: definir o escopo da segurança das entidades; orientar, por meio de suas diretrizes, todas as ações de segurança das entidades, para reduzir riscos e garantir integridade, sigilo e disponibilidade das informações e recursos; permitir a adoção de soluções de segurança integradas e servir de referência para auditoria, apuração e avaliação de responsabilidades.

A Resolução n. 6, de 22/11/2001, aprova os critérios e os procedimentos para o credenciamento, a manutenção e o descredenciamento de Autoridades Certificadoras – AC, de Autoridades de Registro – AR e de prestadores de serviço de suporte, no âmbito da ICP-Brasil.

A Resolução n. 7, de 12/12/2001, aprova os requisitos mínimos para as políticas de certificado na ICP-Brasil. Por último, a Resolução n. 8, de 12/12/2001, aprova os requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da ICP-Brasil.

O art. 13 da Medida Provisória n. 2.200/2001 dispõe que o Instituto Nacional de Tecnologia da Informação – ITI – é a Autoridade Certificadora Raiz da ICP-Brasil. Integram a estrutura básica da ITI: Presidência, Diretoria de Tecnologia da Informação, Diretoria de Infra-Estrutura de Chaves Públicas e Procuradoria-Geral.

O ITI é uma autarquia federal vinculada ao Ministério da Ciência e Tecnologia e dispõe de autonomia financeira e receita orçamentária. A destinação de receita para o ITI está prevista no art. 17 da referida Medida Provisória. O quadro de pessoal é composto inicialmente por servidores civis ou militares requisitados e empregados dos órgãos e entidades integrantes da administração pública federal direta ou indireta.

As agências reguladoras se caracterizam por: capacidade de produção normativa; independência dos seus dirigentes, detentores de mandatos; autonomia financeira e receita orçamentária prevista em lei; e material humano especializado em seus quadros de pessoal, atuando em setores específicos.

Podemos dizer que o ITI é uma agência reguladora, apesar da dificuldade na adequação do modelo importado do Direito americano em relação ao nosso ordenamento. A queixa principal refere-se à relativa e não à absoluta independência das agências reguladoras. A doutrina denomina esses entes de "autoridades administrativas independentes", porque, em verdade, eles são semi-independentes, pois vinculam-se aos ministérios da área de atuação.

A estrutura das agências é tentadora, porque o contrato de gestão cria facilidades em relação à administração, à gestão de recursos públicos, sem as formalidades inerentes ao modelo tradicional. As autarquias no Direito brasileiro foram criadas na década de 1930, no momento em que o Estado passou a assumir uma pluralidade de serviços que não existiam na vigência das Cartas anteriores, como a de 1891. Em termos de gestão de recursos financeiros, as entidades autárquicas têm uma total independência do poder central. Contudo, em relação a pessoal, não há autonomia. Desempenham serviços especializados, como os assuntos de álcool, café e área previdenciária. As autarquias foram criadas, tiveram seu apogeu e hoje estão em declínio.

Quando se fala em regulação, deve-se ter em vista que regular significa normatizar, implementar as medidas concretas para fazer com que as normas sejam cumpridas, fiscalizar o cumprimento dessas normas gerais e dar implementações concretas.

As agências brasileiras têm muito menos autonomia do que a agência americana. Quanto à regulação, existe um conflito entre a necessidade de produção normativa

cada vez maior e setorizada e a observância de certos princípios, como o da legalidade. É a legitimidade de um ente público, cujos dirigentes não foram eleitos, para criar normas que obriguem as pessoas. No caso brasileiro, o assunto está disposto nos arts. 37 e 84, IV, da Constituição Federal. Qual seria a competência normativa das agências frente ao princípio da legalidade e ao poder regulamentar específico do presidente da República? Essa desproporção entre a necessidade de normatização e a competência do Parlamento constitui um problema de foro universal.

Há duas questões importantes: a existência de um Estado regulador e como é feita esta regulação. A necessidade de se criarem entes públicos, disciplinando atividades privadas, sobretudo nas áreas exploradas por essas empresas, é evidente. A assunção pelo Estado do papel intervencionista em muitos segmentos da atividade econômica, como regulador, vem-se mostrando inadequada, em situações especialmente em que o mercado, mediante consumidores organizados, fosse capaz de criar mecanismos de composição. Isso é difícil de acontecer no Brasil, onde não há organização eficiente por parte do usuário. Para regular é preciso ter agências? Um traço característico que se vem apresentando nos Estados atuais é a pluralidade de entes normativos. Isso é um problema que gera dificuldade de adequação ao modelo tradicional de divisão de Poderes: Poder Legislativo, produtor de normas; Poder Executivo e Poder Judiciário. Há um pluralismo de entes normativos. Temos como exemplo norte-americano a *Federal Trade Comission* e inúmeras agências reguladoras que têm seus dirigentes nomeados pelo Presidente, com mandato e possuindo estabilidade. Essas pessoas regulam um setor da atividade econômica, sem a presença do Estado, produzindo normas, decidindo sobre conflitos. Alguns autores dizem que, em função da normatização realizada pelas agências norte-americanas, podem ser tidas como entes "quase-executivos", "quase-legislativos" e "quase-judiciais".

6 CONCLUSÃO

Uma administração pública mais transparente, eficaz e voltada para a prestação de informações e serviços à população: essa é a grande contribuição que as tecnologias de informação e comunicação podem dar ao relacionamento do governo com os cidadãos. Emissão de documentos, prestação de informações ligadas aos serviços públicos, acompanhamento das ações de governo, condução dos negócios públicos, acesso aos governantes e representantes eleitos são exemplos das possibilidades do uso das tecnologias de informação e comunicação pela máquina administrativa pública.

A tecnologia pode ainda ser largamente aplicada para aperfeiçoar a própria gestão do governo – coordenação, planejamento, execução e controle de ações, contabilidade pública etc. – e suas transações comerciais com o setor privado.

A possibilidade de acesso aos serviços, de participação nas decisões e de acompanhamento dos atos governamentais por parte de todos os cidadãos, portanto, impõe a adoção de meios e métodos digitais pelo governo, em todos os poderes constituídos e níveis governamentais, do emprego das tecnologias de informação e comunicação em benefício da eficácia, responsividade, transparência e governança.

NOTAS BIBLIOGRÁFICAS

1 Para saber mais sobre o valor probatório do documento eletrônico ver MARCACINI, Augusto Tavares Rosa. *O documento eletrônico como meio de prova*. Disponível em: <http://www.augustomarcacini.cjb.net/textos/docelet2.html.> Acesso em: 2 abr. 2001.

2 Para saber mais sobre os aspectos de Direito Contratual aplicados aos contratos eletrônicos ver GAMBOGI, Ana Paula Carvalho. *Contratos via internet*. Belo Horizonte: Del Rey, 2001. p. 59-84

3 PONTES DE MIRANDA, F. C. *Tratado de direito privado: parte geral*. 2. ed. Rio de Janeiro: Borsoi, v. 3, 1954. p. 368; PEREIRA, Caio Mário da Silva. *Instituições de direito civil: introdução ao direito civil*, v. 1, 1986. p. 409.

4 *Sociedade da Informação no Brasil – Livro verde*. Brasília: Ministério da Ciência e Tecnologia. Setembro 2000. p. 24-25.

BIBLIOGRAFIA COMPLEMENTAR

AMARAL, José Levi Mello Júnior. *Infra-estrutura de chaves públicas brasileira: instrumento de democratização da certificação digital no Brasil*. Disponível em: <http://www.planalto.gov.br/ccivil_03/revista/Rev28/artigos/art_Levi.htm>. Acesso em: 1 fev. 2002.

COSTA, Marcos da e MARCACINI, Augusto Tavares Rosa. *O apagão do comércio eletrônico no Brasil*. Disponível em: <http://www.cic.unb.br/docentes/pedro/trabs/apagao.htm>. Acesso em: 4 fev. 2002.

GAMBOGI, Ana Paula. *Contratos via internet*. Belo Horizonte: Del Rey, 2001. p. 122-153.

GARFINKEL, Simson and SPAFFORD, Gene. *Web Security & Commerce*. Sebastopol: O'Reilly, 1997. p. 99-229.

REZENDE, Pedro Antonio Dourado de. *Sobre a criação do ICP-Brasil*. Disponível em: <http://www.cic.unb.br/docentes/pedro/trabs.htm>. Acesso em: 22 ago. 2001.

ABSTRACT

The authoress examines briefly the technological evolution of the new digital era and its relation with Law, as well as how it contributes to the formation of an information society in Brazil, which has arisen with the creation of application systems as, for example: the Electronic Fiscal Station (*PFE*), in São Paulo; the National Health Card (*CNS*), of the Ministry of Public Health; the *Interlegis* Project, of the Federal Senate; and the *Comprasnet* System, of the Ministry of Planning.

She comments about the use of the encryption as an auxiliary mechanism in the maintenance of the information privacy.

She talks about the insertion of the *ICP* – Brazil, Public Keys' Infrastructure, whose function is to guarantee the integrity and the authenticity of the documents electronically produced or transmitted. In order to obtain it, she exposes its structure, purposes, repercussion and pertinent legislation.

She believes that is fundamental the application of the information technology for the improvement of the governmental management of the country at all levels.

KEYWORDS - Information Technology; Informatics Law; *ICP* – Brazil – Public Keys' Infrastructure; internet; encryption; Provisional Measure n. 2,200.

Edilane Del Rio Copalo é Assessora Parlamentar, Brasília-DF.