UNIVERSIDADE FEDERAL DO CEARÁ

CURSO DE DIREITO

ROMULO DA SILVA BEZERRA

O VOTO ELETRONICO: A PARTICIPAÇAO EM CONSULTA POPULAR VIA INTERNET UTILIZANDO A ASSINATURA ELETRONICA

FORTALEZA
2006

ROMULO DA SILVA BEZERRA

O VOTO ELETRONICO: A PARTICIPAÇAO EM CONSULTA POPULAR VIA INTERNET UTILIZANDO A ASSINATURA ELETRONICA

Monografia apresentada como exigência parcial para a obtenção do título de Bacharel em Direito pela Universidade Federal do Ceará sob orientação do Professor Dr Raimundo Helio Leite.

FORTALEZA
2006

O VOTO ELETRONICO: A PARTICIPAÇAO EM CONSULTA POPULAR VIA INTERNET UTILIZANDO A ASSINATURA ELETRONICA

ROMULO DA SILVA BEZERRA

Aprovada em ____/____/_____.

BANCA EXAMINADORA

_____

RAIMUNDO HELIO LEITE - DOUTOR
UNIVERSIDADE FEDERAL DO CEARA

_____

RUI VERLAINE OLIVERIA MOREIRA - DOUTOR
UNIVERSIDADE FEDERAL DO CEARA

_____

FRANCISCO ALEXANDRE COLARES MELO CARLOS - MESTRANDO
UNIVERSIDADE FEDERAL DO CEARA

Agradeço ao professor e orientador Dr. Raimundo Helio Leite, pelo apoio e encorajamento contínuos na pesquisa, ao professor e Mestre Flávio José Moreira Gonçalves, pelo suporte e apoio neste trabalho, aos demais Mestres da casa, pelos conhecimentos transmitidos, e à Diretoria do curso de graduação da Universidade Federal do Ceará, pelo apoio institucional e pelas facilidades oferecidas.

Dedico à minha esposa, aos meus filhos e aos meus pais pelo apoio, dedicação, incentivo, contribuição e compreensão durante todo o Curso de Direito.

Aos meus amigos e amigas, pela ajuda, incentivo, carinho e preocupação dispensados a mim em toda a elaboração deste trabalho.

RESUMO

O presente trabalho procura demonstrar a viabilidade da utilização do instituto da Consulta Popular através da internet, utilizando a tecnologia como uma forma de proporcionar segurança, agilidade, comodidade, menor custo para o Estado e assim possibilitar uma maior utilização deste instituto tão importante para a democracia.

Será abordada a tecnologia da criptografia moderna com seus algorítimos seguros e de domínio público, aberto, demonstrando a publicidade e segurança das suas funções. A assinatura digital e a certificação digital como instrumentos para contornar a insegurança do ambiente virtual da internet. A Infra-estrutura de Chaves Públicas brasileira, as Autoridades Certificadoras, a legislação brasileira que regula a aceitação da assinatura eletrônica, bem como as normas eleitorais referentes à informatização do voto serão demonstradas como uma forma de justificar a aplicação do voto eletrônico via internet no Brasil.

Palavras-chave: Criptografia, assinatura digital, voto eletrônico

ABSTRACT

The present work looks for to demonstrate to the viability of the use of the institute of the Popular Consultation through the internet, using the technology as a form to provide security, agility, comfort, minor cost it Estate and thus to make possible a bigger use of this so important institute for the democracy. The technology of the modern cryptography with its will be boarded algorítimos safe and of public domain, opened, demonstrating to the advertising and security of its functions. The the digital signature and the digital certification as instruments to skirt the unreliability of the virtual environment of the internet. The Infrastructure of Public Keys Brazilian, the Authorities Certifiers, the Brazilian legislation that regulates the acceptance of the electronic signature, as well as the referring electoral norms to the computerization of the vote will be demonstrated as a form to justify the application of the electronic vote saw InterNet in Brazil.

Key-words: Cryptography, digital signature, electronic vote

SUMÁRIO

1 INTRODUÇÃO

A difusão dos computadores e da internet trouxe consigo uma radical alteração no modo de vida das pessoas e do modo como interagem entre si. A internet cresce ainda mais a cada dia, modificando paulatinamente o cotidiano das pessoas, incorporando-se na vida, trazendo novas possibilidades para a escola, pesquisas, comércio, governo, trocas de informações das mais diversas. A rapidez das mudanças deixa o mundo jurídico perplexo diante das inúmeras dúvidas que surgem acerca das novas relações travadas pelos seres humanos.

Trata-se de verdadeira revolução tecnológica e, como não poderia deixar de ser, questões jurídicas surgem desta nova forma de inter-relacionamento. Essas questões devem começar a ser pensadas, refletidas pelos profissionais do direito; O Brasil é o décimo país no mundo em número de usuários de internet, de acordo com um relatório divulgado pela Organização das Nações Unidas (ONU)[1] em 10 de novembro de 2004. O país encerrou o ano de 2004 com uma base de mais de 22 milhões de internautas, cerca de quatro vezes e meia maior do que era no ano 2000. Em relação a 2003, o Brasil ganhou cerca de 4 milhões de novos usuários de internet, de acordo com o estudo. O país é o primeiro em acesso à internet na América Latina, seguido pelo México, com 14 milhões de internautas, e pela Argentina, com 5 milhões de usuários.

No total, segundo o relatório da ONU, havia 875 milhões de pessoas com acesso a internet no mundo em 2005. Isso significa que, em menos de dez anos, grande parte do mundo e do país vai estar interligada na rede, fazendo negócios, compras, pesquisas, namorando ou quem sabe até casando pela internet.

---

[1] COMPUTER WORLD. IDG Now. Brasil é 10º em número de internautas, diz ONU. São Paulo, 2005. Disponível na internet no endereço http://computerworld.com.br/AdPortalv5/adCmsDocumentShow.aspx?GUID=83AAE922-BED6-4BEE-BEBE-7992982604EB&ChannelID=20

Como se sabe, a Internet não tem proprietário e sua maior característica é a liberdade "ilimitada" que fornece aos usuários. Ao mesmo tempo em que essa é a maior virtude da rede mundial, é justamente neste ponto que encontramos as maiores dificuldades para atuação do Direito. Não são poucas as questões de cunho jurídico que surgiram com a expansão da utilização dos computadores pela internet. O campo das relações contratuais está repleto de novidades, tais como, empresas que só existem no mundo virtual, com endereço físico simbólico; vendas de produtos que não estão nas prateleiras e/ou estoque; os contratos são fechados via comunicação eletrônica sem papel e sem assinatura de próprio punho; nos casos de danos, como deve ser a apuração das responsabilidades civis? Na área penal, como identificar o agente da prática ilícita? Qual o local em que foi praticado o crime? Será necessário criar novos tipos penais ou a internet é apenas o meio? Até mesmo o conceito de território é abalado com a internet, o que leva a questionar o atual significado de soberania estatal. Quem tem poder sobre a rede? Quais os limites da soberania estatal para os assunto relativos à internet? Como se verá neste trabalho, a criptografia permite respostas a problemas jurídicos emergentes, mas, por outro lado, ela própria está sujeita a um enquadramento jurídico.

Para os padrões tecnológicos atuais, garantir a segurança, a autenticidade, o sigilo e o não repúdio na troca de informações na internet, consiste na utilização da chamada assinatura digital baseada na criptografia assimétrica de chave pública (e chave privada). A rigor, num par de chaves matematicamente vinculadas entre si. A criptografia consiste numa técnica de codificação de textos de tal forma que a mensagem se torne ininteligível para quem não conheça o padrão utilizado. Sua origem remonta às necessidades militares dos romanos. A criptografia moderna lança mão de conceitos técnicos avançados para a cifragem das mensagens: os algoritmos. Estes, numa visão singela, consistem em fórmulas matemáticas extremamente complexas, utilizadas para geração dos padrões ou chaves criptográficas.

A participação popular no processo político brasileiro está disciplinada por um conjunto de instituições que é um pressuposto da democracia representativa, assim configurando os direitos políticos que qualificam a cidadania, tais como as eleições, o sistema eleitoral, os partidos políticos etc, como constam dos arts. 14 a 17 da Constituição Federal brasileira. O art. 14, que abre o capítulo dos direitos políticos, determina que a soberania popular será exercida pelo sufrágio universal e pelo voto, direto e secreto, com valor igual para todos, e, nos termos da lei, mediante plebiscito, referendo e iniciativa popular.

A iniciativa popular consiste na possibilidade de apresentação, pelos cidadãos, de projetos de lei ao Legislativo, desde que subscritos por número razoável de eleitores, conforme determinam os arts. 14, III, e 61, § 2° e demais regulamentações constitucionais. O referendo popular, previsto no art. 14, II, significa a submissão de projetos de lei aprovados pelo legislativo ao exame direto dos cidadãos, atendidos certos requisitos, tais como pedido de determinado número de eleitores, de certo número de parlamentares ou do próprio chefe do executivo. O plebiscito tem sido utilizado nos regimes representativos como instrumento de decisão popular sobre matéria política específica, empregando-se outros institutos, como o referendo, para a consulta popular sobre atos normativos, matérias constitucionais e a manutenção de decisões políticas ou administrativas já tomadas. Também uma consulta popular, semelhante ao referendo, o plebiscito (Constituição, art. 14, I) é diferente quanto ao momento da decisão política, porque objetiva obter uma decisão prévia sobre uma questão política ou institucional, antes de sua formulação legislativa. O referendo é utilizado para confirmar ou rejeitar o projeto aprovado. No plebiscito, a manifestação popular precede o processo legislativo, ou político, e o vincula em termos definitivos, cabendo à autoridade do Estado, após sua realização, apenas praticar os atos formais necessários à concretização da vontade ditada pela manifestação popular.

A utilização destes dois mundos, de um lado, o virtual que é a rede mundial de computadores chamada internet e, do outro, o mundo real, físico, com as necessidades reais de uma sociedade cada vez mais complexa, evoluída e com seus participantes buscando na democracia uma participação mais efetiva na vida política.

O atual estágio tecnológico que se encontra o Brasil com o seu embasamento jurídico em relação a assinatura digital, vem a propiciar uma real utilização dos institutos da consulta popular via internet.

2 CRIPTOGRAFIA E ASSINATURA DIGITAL

Analisando a questão, primeiramente do ponto de vista técnico, não se pode deixar de explicar o que é criptografia, ou o que é a criptografia assimétrica, e também o que é a criptografia simétrica.

A criptografia é tão antiga quanto a própria escrita e não é uma tecnologia que surgiu com a informática. Teve, a criptografia, ao longo da História, aplicação praticamente exclusiva à esfera militar, mas hoje é considerada uma ciência, ramo da Criptologia, que por sua vez é um ramo das Ciências Exatas. Na nova sociedade da informação, a criptografia tem demonstrado imprescindível utilidade para a proteção da transmissão e armazenamento de informações e para a segurança de sistemas computadorizados. O estudo dos métodos e técnicas de codificar uma mensagem é o objeto de estudo da Criptografia. O outro ramo da Criptologia se chama Criptoanálise, e tem por objeto o estudo científico dos métodos para "quebrar" a mensagem cifrada sem conhecer a senha.

Há indícios de que, na antiguidade, foi conhecida no Egito, Mesopotâmia, Índia e China, mas não se sabe bem qual foi a sua origem, e pouco se sabe do seu uso nos primórdios da História. Em Esparta, por volta de 400 ªC., a técnica de escrever mensagens secretas envolvia enrolar, de forma espiral, uma tira de pergaminho ou papiro ao longo de um bastão cilíndrico. O texto era escrito no sentido longitudinal, de modo que cada letra fosse inscrita separadamente numa das voltas do papiro. Desenrolada a faixa, o que se via era uma porção de letras dispostas sem sentido. Para ler a mensagem, seria necessário enrolar a tira num bastão do mesmo diâmetro do original, de forma que as letras se encaixassem na posição correta.

Na Roma antiga, Júlio César utilizava um método para cifrar as mensagens de suas correspondências, pelo qual cada letra era trocada pela terceira letra subseqüente do alfabeto. Ou seja, para enviar uma mensagem com os dizeres "ESTOU LENDO LIVRO CIFRADO", mediante o cifrado de Júlio César o texto seria escrito da forma "HVXRZ OHQGR OMAUR FMIUDGR".

No século XX a criptografia passou a contar com a valiosa ajuda das máquinas. Até a Primeira Guerra Mundial, todas as técnicas de criptografia eram aplicadas à mão, de modo que apenas as mensagens mais importantes eram codificadas, pois demandavam muito trabalho. Durante a Segunda Guerra Mundial, houve um grande aumento ao uso de mensagens cifradas, sendo que utilizavam máquinas. Os alemães cifravam suas mensagens através de uma máquina eletro-mecânica, conhecida por Enigma. Não obstante o seu avanço, o sistema logrou ser quebrado pelos britânicos.

Com o advento e desenvolvimento dos computadores, a capacidade de criptografar mensagens, textos aumentou significativamente, bem como a capacidade de quebrar a criptografia. Os computadores trabalham com as informações, armazenando, processando e exibindo no monitor de vídeo, sendo que internamente tudo é representado por números. A criptografia irá atuar sobre as mensagens, textos, planilhas, documentos, mediante o emprego de operações matemáticas, sendo tudo apenas mais números a serem utilizados pelo computador através dos programas e softwares.

Hoje em dia a criptografia é utilizada para diversos fins e não somente para fins militares, sendo que tais processos se dão mesmo sem o nosso conhecimento, pois os softwares nos computadores executam as funções de criptografar e decifrar sem a interferência humana. Nas transações bancárias é imprescindível um rigoroso sistema de segurança, no qual é utilizada a criptografia. Outro exemplo é a televisão por assinatura, onde

o sinal é codificado e apenas os assinantes que possuem aparelho decodificador podem assistir. Transações de cartão de crédito, operações de *home-banking*[2] e igualmente o sigilo de nossa correspondência eletrônica só serão possíveis com utilização da criptografia.

2.1 Criptografia Simétrica e Assimétrica

Existem dois métodos de se criptografar uma mensagem: por criptografia simétrica ou por criptografia assimétrica. A criptografia simétrica, considerada convencional, é o método onde uma mesma senha, ou chave, é utilizada tanto para codificar como para decodificar a mensagem. Portanto, para se decifrar a mensagem, é necessário conhecer esta chave que, por sua vez, deve ser mantida em sigilo, para preservar a segurança da comunicação. Outro nome para esse método é criptografia de chave privada.

Como exemplo desse método de criptografia é o chamado cifrado de César, onde para cifrar um texto, cada letra era substituída pela terceira letra seguinte no alfabeto; para decifrar, utiliza-se a mesma chave - três -, utilizando uma função inversa - recuar letras no alfabeto. Atualmente, estes cifrados são realizados mediante complexas fórmulas matemáticas, mas seguem o mesmo princípio: para cifrar, usa-se uma função matemática que tem como variáveis a mensagem original e a chave, resultando na mensagem cifrada; para decifrar, emprega-se uma função inversa, que tem como variáveis a mensagem cifrada e a mesma chave utilizada para cifrar, o que retorna à mensagem original. Utilizando o cifrado de César pode-se criar uma variante, tornando o método mais elaborado, onde se mantém o mesmo critério (avançar letras no alfabeto) e, ao invés de utilizar a terceira letra subseqüente,

[2] Serviços dos bancos disponibilizados num endereço eletrônico na internet.

pode-se deixar para o emissor da mensagem a possibilidade de escolher um número, que significará quantas letras serão avançadas no processo de substituição. Se utilizar o número cinco (5) como chave, a mensagem "ESTOU LENDO LIVRO CIFRADO" ficaria "JZATB QJSIT QOCXT HOLXFIT". O receptor sabendo o critério para a codificação, que é a fórmula ou algoritmo, e o número de letras, que é a senha ou chave, chegaria na mensagem original aplicando a fórmula inversa do algoritmo.

O exemplo acima é meramente ilustrativo e apresenta um método fraco, onde as possibilidades de chaves diferentes, que é a quantidade de letras do alfabeto, seriam facilmente descobertas devido ao poder computacional dos tempos atuais. Para conferir maior segurança ao processo de troca de mensagens, é necessário que o número de senhas possíveis seja de tal ordem que um terceiro interceptador não tenha como experimentar todas as possibilidades a tempo de frustrar a utilidade da mensagem criptografada..

Proteger os próprios dados para que ninguém mais tenha acesso, é plenamente realizado com a utilização da criptografia assimétrica. Neste caso, não se pensa em transmitir uma mensagem a outra pessoa, mas apensa em evitar o acesso indevido de intrusos às informações sigilosas pessoais. O usuário encripta seus arquivos utilizando uma chave e depois ele próprio decifra quando quiser acessá-los.

Pode a criptografia simétrica ser utilizada para o envio de mensagens com segurança entre dois interlocutores. Os dois precisam combinar a chave secreta e então poderão trocar as mensagens onde um executa a cifragem da mensagem e o outro decifra utilizando a senha previamente acertada. Mesmo considerando os cifrados modernos que são muito mais poderosos e considerando um método seguro na comunicação, a criptografia padece de limitações. De um lado, as partes devem ter, ao menos uma vez, um meio seguro de comunicação para combinar a senha, a chave secreta. Isso nem sempre é possível,

principalmente utilizando-se a internet, que é uma rede aberta. De outro lado, se a comunicação tiver que ser realizada entre diversas pessoas, a chave terá que ser combinada entre todas elas.

Para contornar esta dificuldade, há tempos já se perseguia uma forma de criptografar a mensagem sem ter que compartilhar a chave secreta com o interlocutor; ou seja, uma forma de codificação que utilizasse duas chaves, uma para cifrar - a chave pública -, e outra para decifrar - a chave privada. Distribuída livremente a chave pública, qualquer um pode cifrar a mensagem dirigida ao titular da chave privada, mas só este poderá decifrá-la. Somente em 1976, porém, a partir de profundo desenvolvimento da teoria dos números, este modelo conseguiu ser implementado por Whitfield Diffie e Martin Hellman, que descobriram o algoritmo conhecido por Diffie-Hellman. Em 1977, foi descoberto outro algoritmo de criptografia assimétrica, o RSA[3]. Passados 29 anos, poucos algoritmos mais foram encontrados, dado que são raras e difíceis as operações matemáticas que permitem esta engenhosa maneira de cifrar e decifrar. Vários deles se mostraram inseguros, ou pouco práticos, de modo que, para gerar assinaturas, são normalmente utilizados apenas os algoritmos RSA, DSA[4] e El-Gamal[5].

A criptografia assimétrica, ao contrário da convencional, utiliza-se de duas chaves: uma das chaves é a chave privada, e a outra, é a chave pública. Estas duas chaves são números que funcionam como complemento um do outro, estando de tal modo relacionadas

---

[3] O mais conhecido dos métodos de criptografia de chave pública é o RSA. Este código foi inventado em 1978 por Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T). As letras RSA correspondem às iniciais dos inventores do código.

[4] O DAS é um algoritmo de assinatura digital (Digital Signature Algorithm). (Também existe um Padrão de Assinatura Digital (Digital Signature Standard), ou DSS. O padrão implementa o algoritmo - realmente é só uma diferença na terminologia.) é um algoritmo de chave pública, mas só pode ser usado para assinaturas digitais.

[5] Um algoritmo baseado em exponenciação e aritimética modular. El Gamal é usado para criptografia e assinatura digital de maneira similar ao algoritmo RSA. Chaves grandes são geralmente consideradas mais seguras.

que não poderiam ser livremente escolhidas pelo usuário, devendo ser calculadas pelo computador.

Outro fator importante da criptografia assimétrica é que ela se utiliza de funções matemáticas que não tem retorno, isto é, não existe uma operação inversa. As conhecidas funções de adição, subtração, multiplicação ou divisão não passam nem perto do algoritmo utilizado. Os métodos da criptografia assimétrica são sofisticados e tanto as operações matemáticas da fórmula como a escolha das chaves são feitas a partir de complexos cálculos. Vale salientar que este método de criptografia, mesmo utilizando complexos cálculos matemáticos, não se trata de um obstáculo para a utilização pela população em geral, pois há diversos programas de computadores que realizam estas operações mirabolantes de forma transparente para o usuário. Tais programas codificam, decodificam e assinam a mensagem sem que o usuário faça um simples cálculo.

Uma característica da criptografia assimétrica é que a fórmula ou função é sempre a mesma, tanto para encriptar como para decifrar. O que muda, nas funções de cifrar e decifrar a mensagem, é a chave. Encriptando a mensagem com a chave pública, gera-se uma mensagem cifrada que não pode ser decifrada com a própria chave pública que a gerou e deve-se utilizar, para decifrar, a chave privada. O contrário também ocorre. Se a mensagem for cifrada com a chave privada, necessariamente deve-se utilizar a chave pública para decifrar. Se tentar utilizar a mesma chave que cifrou a mensagem para decifra-la, na realidade, o resultado será uma mensagem cifrada novamente, isto é, a mensagem será cifrada duas vezes.

Um aspecto relevante a ser discutido é a própria segurança da criptografia. A consistência do algoritmo e o tamanho das chaves estão diretamente relacionados à segurança da criptografia simétrica e assimétrica. Com relação a consistência do algoritmo, é importante

que um programa de criptografia utilize um algoritmo público e conhecido, isto é, a sua fórmula esteja disponível pra todos os interessados, bem como a comunidade científica. Parece ilógico, mas esta fórmula ficando disponível, ela está sujeita a estudos que podem testa-la e certamente divulgar uma eventual falha de segurança. Importante salientar que nenhum fornecedor de criptografia poderá colocar códigos ou funções que o favoreçam ou que impliquem quebra do sigilo das chaves do usuário.

Esta certeza de segurança do algoritmo advém do estudo prolongado das operações matemáticas envolvidas, na tentativa de encontrar meios de decifrar a mensagem sem conhecer a senha ou chave privada. Mesmo no que toca os algoritmos conhecidos e considerados seguros, esta segurança provém do fato de que, após anos e anos de investigação, não se encontrou uma maneira viável de quebrar o código.

De outro lado, um algoritmo novo ou mantido em segredo, não terá sido testado suficientemente para que se possa atestar o seu grau de segurança. Se mantido em segredo o algoritmo, sempre paira, entre os especialistas, um aspecto de insegurança, pois se fosse suficientemente bom, não seria necessário o sigilo sobre o seu funcionamento.

Para a criptografia moderna, fundada em conceitos matemáticos, um algoritmo só pode ser considerado seguro se, apesar de conhecidos todos os cálculos empregados, seus cifrados permanecerem sem sentido aos olhos dos que não detenham a chave. Muitas outras questões são importantes quando se trata da segurança dos dados, seja o processo de geração das chaves, seja o modo de armazená-las, ou mesmo a maneira como o programa irá implementar o algoritmo de criptografia. Por estas razões, considera-se que também o software de criptografia, para ser considerado seguro, deve ter o seu código-fonte conhecido. È uma forma de aferir se não há falhas de implementação, ou mesmo se não existe código malicioso inserido no sistema.

Um outro fator a considerar, no que diz respeito à segurança da criptografia, é o tamanho das chaves utilizadas pelo algoritmo. De acordo com este tamanho, pode-se afirmar que a criptografia é forte ou fraca. Ao tratar do tamanho das chaves, torna-se necessário distinguir o tamanho das chaves da criptografia simétrica da criptografia assimétrica. O tamanho das chaves é normalmente indicado em números de bits[6]: as chaves são números e a quantidade de bits indica quantos algarismos tem estes números, em notação binária. Assim, por exemplo, com oito bits pode-se representar um número entre 0 e 255 (respectivamente 00000000 e 11111111, em notação binária). Com dez bits, representa-se um número entre 0 e 1023.

Na criptografia simétrica, se o algoritmo for consistente e não houver falhas de implementação, uma forma de tentar decifrar a mensagem é pelo método da força bruta, isto é, testando-se todas as possíveis combinações de chaves. Chaves de criptografia simétrica com 128 bits, que representa um número com 39 algarismos em base decimal, são consideradas atualmente bastante seguras. Para se ter uma idéia deste número, se forem utilizados um bilhão de computadores, durante 24 horas por dia, cada um com velocidade para testar um trilhão de chaves por segundo, serão necessários mais de 10 bilhões de anos. Pode ser que a chave certa seja encontrada na metade do tempo, mas é muito improvável. Vale citar alguns algoritmos de criptografia simétrica considerados seguros, tais como o DES[7], o Triple-DES[8], o IDEA[9], o RC4[10], o RC5, o RC6 e o Blowfish[11].

---

[6] Menor informação que o computador pode processar. Possui valor numérico igual a 1 ou 0

[7] Data Encryption Standart - Exemplo do mais difundido cifrador computacional de chave única.

[8] Algoritmo que utiliza o DES e faz o processo de criptografia três vezes.

[9] Internation Data Encryption Algorithm - Desenvolvido em Zurique por James L. Massey e Xuejia Lai e publicado em 1990. IDEA usa chaves de 128 bits e é muito forte.

[10] Rivest Cipher - Ronald Rivest, da RSA Data Security INC., projetou essas cifras com tamanho de chaves variável para proporcionar uma criptografia em alto volume que fosse muito rápido. Um pouco mais rápido do que o DES, essas cifras podem se tornar mais seguras escolhendo-se um tamanho de chave mais longo, eles permitem chaves com o tamanho entre 1 e 2048 bits.

[11] O algoritmo blowfish, utiliza cifra de bloco de 64 bits com uma chave de até 448 bits de comprimento, é projetado por Bruce Schneier.

Quando analisamos a criptografia assimétrica, o tamanho das chaves deve ser bem maior, pois a partir da chave pública é possível obter a chave privada. Como os algoritmos são conhecidos e a chave pública também, a partir cálculos matemáticos, como a fatoração no algoritmo RSA, pode-se achar a chave privada correspondente. Fatorar um número, consiste em encontrar os números primos que multiplicados, geram o respectivo número, ou seja, como exemplo, o número 187 é encontrado a partir dos números primos 11 e 17 multiplicados. Tendo os números, torna-se fácil encontrar o produto, mas tendo apenas o produto, já não é tão fácil encontrar os dois números primos.

Atualmente a criptografia assimétrica é considerada segura utilizando par de chaves de 1024 bits, mas de todo modo, os softwares atuais permitem utilizar chaves muito maiores de até 8192 bits. Alguns algoritmos conhecidos de criptografia assimétrica, tais como o RSA, o Diffie-Hellman, o DSA, o El-Gamal, têm se mostrado resistentes às provações da comunidade científica.

Como se pode verificar da dificuldade em obter as chaves, seja a chave da criptografia simétrica, seja a chave privada da criptografia assimétrica, através de tentativas computacionais de cálculos e testes, talvez a forma mais rápida seria através da insegurança da guarda desta chave. A chave privada deve ser guardada da forma mais segura possível, sendo em arquivos criptografados simetricamente com frases senhas ou em dispositivos eletrônicos pessoais. Quem tem o maior interesse em guardar a chave privada é o próprio usuário, pois se alguém se apoderar de sua chave, poderá abrir seus documentos cifrados ou assinar documentos eletrônicos como se fosse o verdadeiro titular das chaves.

Criptografia assimétrica, pois, não é uma tecnologia passageira. A expressão tecnologia estaria mais adequada se referisse às técnicas pelas quais a criptografia assimétrica

pode ser implementada: os algoritmos RSA, DSA e El-Gamal poderiam ser chamados de tecnologias.

Criptografia assimétrica, portanto, é um modelo, um conceito, que pode ser implementado de maneiras - ou tecnologias - diferentes, e que tem suas bases em teorias matemáticas longamente experimentadas e desenvolvidas. Algumas tecnologias que se esboçam como alternativa à criptografia assimétrica, ou distorcem a essência do conceito de documento, ou mistificam técnicas que não são apropriadas para gerar assinaturas. Assim, enviar o documento para uma terceira pessoa, que ficaria encarregada de receber, por meio de alguma nova tecnologia, a aprovação do outro interlocutor, como alguns já chegaram a propor, é uma idéia que, mesmo realizada de modo seguro, torna o processo oneroso demais e impraticável quando se tratar de comunicação em massa.

Do ponto de vista econômico, vale a pena ressaltar que a utilização da criptografia assimétrica é hoje algo muito barato, gratuito até, considerando que os algoritmos RSA, DSA e El-Gamal têm uso liberado, sem reserva de direitos ou patentes, e existem diversos *softwares* livres, de código aberto, que implementam eficientemente as funções de cifrado, assinatura e gerenciamento de chaves. E, aliás, por terem seu código-fonte aberto, estão sujeitos a exame por especialistas em segurança de todo o mundo, sendo certamente mais seguros do que os programas de criptografia comerciais, que têm o código-fonte fechado.

2.2 Assinatura Digital

Inicialmente é relevante abordar o que não é assinatura digital. A imagem digitalizada de uma assinatura manual não é assinatura digital. Trata-se apenas de um arquivo gráfico que pode ser apensada em qualquer documento, sem implicar que o mesmo foi escrito ou gerado pelo assinante. Trata-se de um recurso computacional simples, onde qualquer pessoa pode digitalizar (transformar em imagem digital no computador) a imagem da assinatura em um documento e inseri-la em outro documento eletrônico. Uma senha de acesso, que é utilizada para entrar em sistemas, acessar a internet ou mesmo a caixa postal do correio eletrônico, também não é uma assinatura digital.

A criptografia assimétrica é a base da assinatura digital. O algoritmo Diffie-Hellman não produz assinaturas digitais, servindo apenas para seus propósitos originalmente desejados, o estabelecimento de comunicação sigilosa sem compartilhamento da chave de decodificação. Entretanto, em 1977, três outros matemáticos descobririam um algoritmo de criptografia assimétrica que, além de cifrar com a chave pública e decifrar com a privada, também "funciona" no caminho inverso, isto é, cifra com a chave privada e decifra com a pública. Nasce o conceito de assinatura digital. Este algoritmo, conhecido pelas iniciais de seus criadores – RSA – é o mais utilizado nos dias de hoje, embora outros poucos tenham sido posteriormente descobertos para também gerar assinaturas digitais. Um episódio profundamente controverso protagonizado por este algoritmo – mas permitido pela generosa legislação de patentes norte-americana – foi a obtenção de uma patente deste algoritmo pelos seus criadores, válida ao menos nos limites territoriais dos Estados Unidos - EUA. A possibilidade de patentear operações matemáticas, fundadas em conhecimentos antigos, públicos e sedimentados desta ciência, não deixou de ser recebida com críticas por cientistas e

pesquisadores ao redor do mundo. Mas, como o prazo desta patente já expirou, o algoritmo RSA hoje pertence ao domínio público também nos Estados Unidos.

A assinatura digital nada mais é do que o cifrado obtido neste "caminho inverso", em que o documento eletrônico é cifrado com a chave privada. Embora somente quem possua a chave privada possa chegar neste resultado cifrado, qualquer um que conheça a chave pública pode decifrá-lo, isto é, conferir a assinatura. Por caminhos muito diversos, reproduziu-se no mundo dos *bits* as propriedades da assinatura autógrafa: somente nossa mão é capaz de desenhá-la no papel, mas quaisquer terceiros que conheçam previamente nossos traços são capazes de identificar a assinatura como sendo nossa. Já a exclusividade da assinatura digital decorre do fato de que a posse da chave privada esteja restrita ao seu titular, de modo que somente ele seja capaz de produzir um cifrado que possa ser decodificado com a chave pública correspondente.

Sendo assim, a assinatura digital é o resultado de uma operação matemática, utilizando a criptografia assimétrica.

A assinatura digital, no caso, é produzida cifrando-se a mensagem com a chave privada, de modo a poder ser conferida com a chave pública; isto é, se a chave pública decifrar a mensagem, isto significa que ela provém daquele que detém a chave privada.

Na realidade, a mensagem toda não é criptografada, mas sim o resultado da aplicação de uma outra função matemática sem retorno, conhecida como *hash function*[12] ou "função digestora", sobre a mensagem. Isso se deve ao fato de que, criptografar mensagens curtas não representa nenhum problema computacional, mas criptografar arquivos extensos,

[12] Uma função matemática que não possui inversa e assim não se pode chegar ao valor inicial da expressão, mesmo tendo o valor final e a própria função.

documentos grandes, arquivos de imagens, planilhas, enfim, qualquer tipo de arquivo, demandaria elevados recursos computacionais, além de muito tempo pra assinar tais arquivos.

Na sistemática adotada, aplica-se sobre um documento editado ou confeccionado, um algoritmo de autenticação conhecido como *hash*. A aplicação do algoritmo *hash* gera um resumo do conteúdo do documento conhecido como *message digest*, com tamanho em torno de 128 *bits*. Aplica-se, então, ao *message digest*, a chave privada do usuário, obtendo-se um *message digest* criptografado ou codificado. O passo seguinte consiste um anexar ao documento em questão a chave pública do autor, presente no arquivo chamado certificado digital.

Como forma de melhor visualizar este processo, e compreender a funcionalidade da *hash function*, tome-se como exemplo o dígito de controle do Cadastro de Pessoa Física – CPF da Receita Federal. Os dois números de controle do CPF são obtidos através de cálculos matemáticos e a simples troca de um dos números acarretaria em outro dígito de controle, isto é, não coincidiria o número original com os dois números de controle.

Com a "função digestora" ocorre algo parecido, onde a partir da mensagem ou documento ou arquivo, é produzido um número de controle de 128 *bits*, isto é, um número com 39 casas decimais. Tal número torna inviável que se consiga encontrar duas mensagens que gerem o mesmo número de controle. Esse número de controle, o *message digest*, ou seja, o resumo da mensagem, é um número estatisticamente único que representa a mensagem. Este resumo da mensagem é que será criptografado com a chave privada ou a chave pública, dependendo do destinatário da mensagem.

Podemos dizer que assinatura digital de um documento eletrônico consiste nestes três passos: a) geração do *message digest* pelo algoritmo *hash*; b) aplicação da chave privada

ao *message digest*, obtendo-se um *message digest* criptografado e c) anexação do certificado digital do autor (contendo sua chave pública).

Ao chegar ao seu destino, o documento ou mensagem será acompanhado, como visto, do *message digest* criptografado e do certificado digital do autor (com a chave pública nele inserida). Se o sistema utilizado pelo destinatário suportar documentos assinados digitalmente, ele adotará as seguintes providências: a) aplicará o mesmo algoritmo *hash* no conteúdo recebido, obtendo um *message digest* do documento; b) aplicará a chave pública (presente no certificado digital) no *message digest* recebido, obtendo o *message digest* decodificado e c) fará a comparação entre o *message digest* gerado e aquele recebido e decodificado. A coincidência indica que a mensagem não foi alterada, portanto mantém-se íntegra. A discrepância indica a alteração/violação do documento depois de assinado digitalmente. Os principais algoritmos de *hash* são: o MD4[13], o MD5, e o SHA[14].

É justamente este o mecanismo utilizado para viabilizar as chamadas conexões seguras na Internet (identificadas pela presença do famoso ícone do cadeado amarelo). Para o estabelecimento de uma conexão deste tipo, o servidor acessado transfere, para o computador do usuário, um certificado digital (com uma chave pública). A partir deste momento todas as informações enviadas pelo usuário serão criptografadas com a chave pública recebida e viajarão codificadas pela Internet. Assim, somente o servidor acessado, com a chave privada correspondente, poderá decodificar as informações enviadas pelo usuário.

O sistema de criptografia assimétrica permite o envio de mensagens com total privacidade. Para tanto, o remetente deve cifrar o texto utilizando a chave pública do

---

[13] Umas das *message digest* mais usada é o MD4 e o MD5, que foi desenvolvido por Ronald Rivest da RSA Data Security, e pose ser usado livremente.

[14] SHA (Security Hash Algorithm) foi desenvolvido pelo NITS com a assistencia dp NSA (National Security Agency). Este algoritmo é similar ao algoritmo MD4, exceto que o SHA produz uma saida de 160 bits e o MD4 uma saida de 128 bits

destinatário. Depois, ele (o remetente) deverá criptografar o texto com a sua chave privada. O destinatário, ao receber a mensagem, irá decifrá-la utilizando a chave pública do remetente. O passo seguinte será aplicar a própria chave privada para ter acesso ao conteúdo original da mensagem.

A assinatura digital possibilita que o documento eletrônico possa suprir esta última funcionalidade do papel, acima referida. Um documento eletrônico assinado digitalmente, conquanto continue a ser uma seqüência de *bits* sem qualquer apego a um suporte físico, propicia as mesmas funcionalidades do papel como demonstração da verdade. A assinatura digital mantém um elo lógico de ligação com o documento assinado, de modo que, além de ser única para aquele documento, fique invalidada se houver qualquer alteração posterior. Com isso, o documento eletrônico assinado digitalmente por A, pode ser totalmente entregue a B, que o guardará como quiser, em seu computador, em discos compactos, *Compact Disks* - CDs ou outra mídia de armazenamento sob seu exclusivo controle. Ainda assim, B poderá apresentar o documento eletrônico a um terceiro C, que terá meios para acreditar que o documento provém de A, bem como que não foi adulterado posteriormente. Assim, um documento eletrônico com sua correspondente assinatura pode, na grande maioria das situações, substituir o papel como meio de prova, assumindo a função de prova documental.

A assinatura digital não é nada que se assemelhe a uma assinatura manuscrita. É muito difícil para nossa sociedade, no entanto, livrar-se do conceito de assinatura como algo exclusivamente relacionado a traços manuscritos. A imagem digitalizada de uma assinatura autógrafa nenhum significado apresenta em meio digital, posto que não confere qualquer segurança. No papel, cada assinatura autógrafa é única, posto que os átomos da tinta se misturaram aos átomos do papel, não havendo como reaproveitar aquela tinta, e seu exclusivo

desenho, noutros documentos. *Bits*, contudo, não são únicos. São, ao contrário, facilmente reproduzíveis, daí a assinatura manuscrita digitalizada ser algo absolutamente imprestável nos meios eletrônicos para os fins de se atribuir certeza da autoria de um documento.

Subsiste, entretanto, o problema da autenticidade (autoria). Portanto, a sistemática da assinatura digital (baseada na criptografia assimétrica) necessita de um instrumento para vincular o autor do documento ou mensagem, que utilizou sua chave privada, a chave pública correspondente. Em conseqüência, também o problema da segurança ou confiabilidade da chave pública a ser utilizada precisa ser resolvido. Esta função (de vinculação do autor a sua respectiva chave pública) fica reservada para as chamadas entidades ou autoridades certificadoras.

Assim, a função básica da entidade ou autoridade certificadora está centrada na chamada autenticação digital, onde fica assegurada a identidade do proprietário das chaves. A autenticação é provada por meio daquele arquivo chamado de certificado digital. Nele são consignadas várias informações, tais como: nome do usuário, chave pública do usuário, validade, número de série, entre outros. Este arquivo, também um documento eletrônico, é assinado digitalmente pela entidade ou autoridade certificadora.

A assinatura digital aposta em um documento eletrônico ou mensagem eletrônica, enfim, é o resultado de uma operação matemática que utiliza duas variáveis: o documento ou a mensagem a assinar e um dado sigiloso, conhecido no jargão técnico como chave privada. A chave pública acompanha a assinatura como forma de se verificar *a posteriori* a autenticidade do documento assinado.

2.3 Certificado Digital

Como visto, a assinatura eletrônica produzida por criptografia assimétrica permite reproduzir no meio eletrônico a mesma funcionalidade proporcionada pelo papel assinado à tinta. A assinatura de documentos eletrônicos, em si, pode ser produzida e conferida com o uso das chaves privada e pública, respectivamente, não sendo a certificação um dado essencial para a realização destas tarefas. A certificação eletrônica se constitui apenas em um *plus* que pode ou não ser agregado neste processo, para conferir mais segurança acerca da autenticidade das assinaturas assim produzidas.

A assinatura digital é o resultado de uma operação matemática, totalmente feita por computador, que utiliza como variáveis o documento eletrônico e a chamada chave privada do "signatário". Esta chave privada nada mais é do que um número, como aliás, também o é o documento, aos olhos do computador. Toda informação, para o computador, é tratada como um número. E este número que chamamos de chave privada, em oposição ao que a lógica leiga pode pensar, não está de forma alguma vinculado ao corpo do titular, nem deve estar. Ao contrário, toda a segurança de um mecanismo assim parte do pressuposto inicial de que estas chaves sejam geradas da forma mais aleatória possível, uma vez que a existência de algum ponto de partida conhecido pode permitir a um fraudador calcular a chave privada de outras pessoas, de modo que possa fazer-se passar por elas.

Sendo assim, o que relaciona um par de chaves a uma dada pessoa, de modo que se possa dizer que estas chaves lhe pertencem? A resposta é: confiança.

Se isso parece muito frágil, é de se notar que o reconhecimento de alguém como sendo ele mesmo é um problema muito anterior aos computadores. Em um corpo humano, em suas células, em suas características físicas, não se encontra nenhum vestígio do nome desta

pessoa, de seu CPF, ou outro identificador social. O nome e identidade são relacionados à pessoa por uma série de registros e documentos em que costumeiramente se confia, mas que nem sempre são fidedignos.

Enfim, que não se pense que a informática vai resolver de modo automático este problema humano de identificar alguém como sendo ele mesmo. Esta é uma premissa muito importante, para não se atribuir às assinaturas digitais e à certificação eletrônica uma fé mágica muito maior do que elas permitem conferir às relações humanas. O mérito das assinaturas digitais é o de atribuir aos arquivos eletrônicos funcionalidades que só o papel logrou produzir, ao longo de séculos, como exposto acima. Em alguns aspectos, chega a produzir vantagens, como a instantânea possibilidade de constatar a adulteração do documento. Em outros, acarreta dificuldades antes inexistentes, como o problema da guarda segura destas chaves privadas, aspecto fundamental da segurança das assinaturas digitais. Não vão obviamente solucionar todos os problemas de falsidade de identidade ou de declaração, pois estas são questões muito mais complexas do que um algoritmo matemático. O que a assinatura digital permite concluir pode ser resumido no seguinte:

Se uma assinatura digital foi conferida corretamente com uma dada chave pública, é matematicamente certo que:

a) quem produziu a assinatura digital tinha em seu poder a chave privada que corresponde a esta chave pública utilizada na conferência, vez que estas duas chaves do par são matematicamente relacionadas;

b) o documento eletrônico não foi alterado depois que a assinatura digital foi produzida, posto que qualquer alteração, mínima que fosse, invalidaria a assinatura.

Atribuir a uma pessoa a titularidade desta chave pública – e, portanto, da privada – é ato de fé, que pode estar respaldado em fatos mais ou menos confiáveis. Valorar o quanto esta relação chave-sujeito é suficientemente confiável para que se possa dizer que a assinatura é mesmo de tal sujeito é resultado do juízo humano.

O uso de certificados eletrônicos é uma forma de contribuir com a certeza acerca desta relação chave-sujeito, utilizando-se, também, de meios eletrônicos. Não deve ser vista, no entanto, como uma prova absoluta, pois deve ter ficado claro que tais certificados são, antes de mais nada, um ato declaratório de um outro sujeito, que, seja ele quem for, não tem o poder absoluto de vincular um número aleatório a uma pessoa. No entanto, é comum repetir-se, sem qualquer reflexão, que assinaturas digitais contariam com a propriedade do "não-repúdio", algo como um pó mágico capaz de impedir toda e qualquer discussão acerca da veracidade do documento ou da assinatura digitais. Esta expressão, na verdade, era utilizada no jargão técnico-científico para expressar que as operações matemáticas, insistentemente testadas pela comunidade científica, se mostravam "inquebráveis"; isto é, que a correta decodificação com a chave pública permite irrefutavelmente concluir que esta codificação foi feita por quem tinha a chave privada. Esta é a única verdade matemática que pode ser concluída, não sendo adequado estendê-la a todos os demais fatos que rondam o documento eletrônico.

Desmistificando a dourada certificação eletrônica, então, o certificado eletrônico pode bem ser comparado a uma carteira de identidade, que goza de maior ou menor fé na sociedade a depender de quem a emitiu. O número do Registro Geral "RG", a carteira da OAB e outros documentos públicos são presumivelmente verdadeiros, presunção esta que nunca é absoluta, como todos bem compreendemos sem qualquer dificuldade quando se tratam de documentos físicos. Carteirinhas de clube, de membro de torcida organizada ou de

escola também são documentos hábeis a demonstrar a identidade de alguém em comunidades fechadas, e embora sejam menos aceitas para este fim pela sociedade em geral, dentro do âmbito a que se destinam podem ser mais importantes do que os próprios documentos emitidos por órgãos públicos. Tentem entrar nas dependências do seu clube sem a tal carteirinha, exibindo apenas seu RG ao porteiro.

O certificado eletrônico, então, nada mais é do que a versão eletrônica destes documentos de identidade. O fato de usar tecnologia moderna não pode esconder que há, por trás de tudo isso, uma declaração – e declaração é sempre fruto do pensamento humano – acerca da identidade de alguém. Declaração que pode representar os mais diferentes efeitos e significados, conforme a intenção daquele que presta a declaração e os fins que se quer alcançar com ela.

Assim, o certificado eletrônico é um documento eletrônico assinado digitalmente, que declara a identidade de alguém e lhe atribui a titularidade de uma chave pública. A Carteira de Identidade de Advogado – a de papel, por ora – representa uma declaração da Ordem dos Advogados do Brasil de que uma pessoa com a aparência da fotografia ali retratada relaciona-se com o nome e demais dados nela descritos, assina da forma ali exibida e está inscrita no quadro dos advogados da entidade sob um determinado número.

Um certificado eletrônico pode conter tudo isso, além da informação principal a que ele se presta a declarar: qual é a chave pública do titular. Deste modo, o ente certificante – que emite o certificado – está prestando uma declaração acerca de dados pessoais e da titularidade de uma chave pública. E com esta chave pública certificada, pode-se conferir as assinaturas digitais do sujeito certificado.

No entanto, é de se ver que a certificação é um meio de prova acerca da titularidade de uma chave pública, mas não é o único possível. A titularidade de uma chave pública é fato que pode ser provado por outros meios, como a confissão, prestada verbalmente ou por escrito, até mesmo em um instrumento em papel, antes ou depois da assinatura digital ter sido produzida. Se é claro que a certificação eletrônica pode facilitar em muito a conferência, pois permite uma automação do procedimento, isso não significa que seja ela a única forma de se atestar a titularidade de uma chave pública, nem tão pouco que represente uma prova absoluta desta titularidade.

O equívoco de se pensar na certificação eletrônica como pólo metodológico do estudo da prova eletrônica, ou até da contração eletrônica, faz com que, por vezes, a discussão sobre o tema se distancie da relação material que se quer demonstrar. Invocam-se tantas regras, formas e argumentos pseudo-tecnológicos, que se esquecem de que o problema jurídico central verdadeiramente relevante é a demonstração da verdade de um fato que, antes desta parafernália toda ser criada, na grande maioria das vezes poderia ser demonstrado por todos os meios de prova.

Ora, antes de tudo, há pessoas realizando um ato jurídico qualquer, ato este que em regra sequer depende de forma determinada para ser *válido*. Se o ato foi instrumentalizado por documento eletrônico, surge a questão da confiabilidade deste, pelas razões expostas acima, posto que, nesta forma eletrônica, uma das partes pode facilmente adulterar documento verdadeiro, ou criar um documento totalmente falso. O uso de assinatura digital é o mecanismo que permite atribuir ao documento eletrônico as conhecidas propriedades do papel, mas isto pode conduzir a uma outra questão: a chave utilizada na conferência é verdadeiramente do suposto "signatário" do documento eletrônico? Uma das maneiras –

possivelmente a mais prática – de se identificar o titular destas chaves seria por meio da certificação eletrônica, notadamente quando se tratarem de pessoas que não se conhecem.

Mas este último fato pode, sem dúvida, ser demonstrado de outras maneiras, em especial entre pessoas que tenham relacionamento cotidiano. Os fatos representados no documento não serão mais ou menos verdadeiros pelo fato deste documento ser físico ou eletrônico, este assinado digitalmente com chaves certificadas. A vantagem da assinatura digital, insista-se, não está em incrementar nosso conhecimento acerca da verdade, mas tão somente em permitir a substituição da funcionalidade probante do papel, o que já não é pouco e representa uma revolução sem precedentes.

Um documento, um instrumento contratual, por exemplo, ao invés de ser redigido em papel e assinado de próprio punho, pode perfeitamente ser mantido em formato eletrônico, com assinaturas digitais dos contratantes. Mas imaginemos que, em uma contratação à distância, cada contratante enviasse aos outros, junto com a minuta assinada em papel, o seu próprio documento de identidade, para que cada um deles pudesse confrontar as assinaturas alheias lançadas no instrumento com a que consta da cédula de identificação. Em relação às assinaturas digitais, o certificado eletrônico realiza exatamente uma função análoga a essa (que jamais se procederia no "mundo físico"), além de dispensar conhecimentos grafotécnicos necessários para a tal conferência, já que o computador a realiza de modo automático. Esta, enfim, é a função do certificado eletrônico.

É de se lembrar, porém, que os mesmos certificados eletrônicos podem ter finalidades técnicas que nenhuma relação mantêm com documentos e assinaturas eletrônicas. Nisto residem outras tantas confusões sobre o tema. Como já expresso acima, a criptografia é originalmente uma forma de se escrever em código, para proteção do sigilo da comunicação.

Todas as páginas da internet que pedem ao usuário o envio de alguma informação confidencial (dados pessoais, número de cartão de crédito, senha bancária, etc.) são normalmente protegidas por criptografia, sendo o servidor identificado por um destes certificados. O servidor que alimenta esta página da internet envia ao usuário a sua chave pública, para que este codifique os dados a serem enviados, tarefa que o *software* navegador faz de modo transparente. Atualmente, é este o uso mais comum destes modelos de certificação, mas não se deve confundir este procedimento de identificação do servidor *web* com a produção de documentos eletrônicos assinados.

2.4 A infra-estrutura de Chaves Públicas

Uma infra-estrutura de chaves públicas (ICP) pode ser conceituada como um sistema que tem por finalidade precípua, mas não exclusiva, atribuir certificados digitais, e conseqüentemente assinaturas digitais, a um universo de usuários. Além de fornecerem estes documentos eletrônicos às pessoas naturais, aos órgãos e às entidades públicas e privadas, os entes que compõem uma ICP, desempenham a tarefa de gerenciar o ciclo de vida dos certificados, como no caso de comprometimento da chave privada de determinado titular de um determinado certificado digital em virtude roubo ou fraude.

Uma infra-estrutura de chaves públicas pode ser configurada basicamente em dois modelos: o hierárquico e o de confiança distribuída. O primeiro é configurado numa hierarquia, na forma de uma pirâmide ou árvore invertida, situando-se no topo uma entidade na qual todos devem confiar. A confiança de dissemina de cima para baixo. A entidade localizada no ápice da hierarquia é denominada Autoridade Certificadora Raiz, emite um

certificado para uma autoridade certificadora de segundo nível e esta emite para o usuário final. No modelo de confiança, cada autoridade certificadora constitui uma hierarquia independente, não havendo, a princípio nineis intermediários.

Um conceito importante a ser desmistificado aqui é o da interoperabilidade. Faz parte da infra-estrutura de chaves públicas também e pode ser definida como a capacidade que possuem os aparelhos ou equipamentos, que fazem parte da infra-estrutura, se comunicarem entre se, independentemente de sua procedência ou fabricante. Num sistema de telefonia celular, a interoperabilidade permite que um usuário com aparelho X de uma operadora A mantenha conversa com outro usuário utilizando aparelho Y da operadora B. O mesmo princípio aplica-se a infra-estrutura de chaves públicas, onde um usuário poderá comunicar-se com outro usuário independentemente dos seus certificados digitais ou equipamentos utilizados.

Um aspecto abordado pela doutrina com relação à tecnologia adotada para a assinatura digital é a questão da "neutralidade tecnológica". As manifestações sobre o assunto dispõem na seguinte conclusão: a lei deve ser tecnologicamente neutra para ser adequada. A questão da neutralidade tecnológica implica em duas vertentes de pensamento. Ser tecnologicamente neutro é o atributo conferido principalmente às legislações, e significa não se privilegiar determinada tecnologia em detrimento de outra. Outra forma de neutralidade seria a de que as legislações neutras teriam mais longevidade, não precisando de alterações de acordo com as inovações tecnológicas. Assim seria tecnologicamente neutro especificar "assinatura eletrônica" pois não explicita nenhuma tecnologia específica, enquanto que "assinatura digital", que é uma espécie de assinatura eletrônica, determina o modelo da criptografia assimétrica.

A neutralidade tecnológica prega a maior abertura possível e acaba, na realidade, deixando um vazio apto a ser preenchido por qualquer procedimento ou modelo tecnológico não consolidado ou aprovado pela comunidade científica. Esse vazio pode prejudicar principalmente uma das características mais cruciais de uma infra-estrutura de chaves públicas, que é a interoperabilidade. Conforme afirma Fabiano Menke[15]: "Se tudo for possível, pode ser que nada seja realizável.A pretexto da viabilização de uma simpática abertura, o caos poderá imperar". Contrapondo-se à questão de que a lei deve ser tecnologicamente neutra, há a questão da insegurança da aplicação de regras vagas, da falta de uma regra específica, que utilize um padrão já aprovado pelo mercado ou sociedade.

No Brasil, a infra-estrutura de chaves públicas é albergada na ICP-Brasil, estrutura de certificação baseada no modelo hierárquico, instituída pela Medida Provisória 2.200, de 28 de junho de 2001.

Inicialmente, em 5 de setembro de 2000, foi instituída a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal, a denominada ICP-Gov, com objetivos de atender somente à certificação eletrônica dentro da Administração Pública. A Medida Provisória veio em seguida e criou a ICP-Brasil, através da MP 2.200 de 28 de junho de 2001, agora com incidência sobre qualquer usuário que tentasse obter um certificado digital.

A nova norma veio não apenas para instituir a infra-estrutura técnico-administrativa dos agentes que regularão e forneceram os certificados digitais, mas também versou sobre os efeitos jurídicos produzidos por uma declaração de vontade assinada digitalmente com certificado emitido no âmbito da ICP-Brasil bem como sobre os efeitos jurídicos emanados de outros meios de comprovação de autoria. Com isso, o texto lega brasileiro elegeu a política legislativa de intervenção estatal no controle e supervisão da

[15] MENKE, Fabiano. Assinatura Eletrônica: aspectos jurídicos no direito brasileiro – São Paulo: Editora Revista dos Tribunais, 2005 p. 62

atividade dos prestadores de serviços de certificação, designando uma autarquia federal como responsável por tais atribuições.

No que toca à infra-estrutura normativa e técnico-administrativa, o Comitê Gestor é a autoridade gestora de políticas da ICP-Brasil e tem por atribuição principal coordenar a sua implantação e o seu funcionamento, a partir de critérios e das normas para o credenciamento das entidades que integram a cadeia de certificação. Dentre as resoluções aprovadas pelo Comitê Gestor, estão as, denominadas de núcleo duro, Resoluções no. 1, 2, 7 e 8 (respectivamente, Declaração de Práticas de Certificação da AC Raiz, Política de Segurança da ICP-Brasil, Requisitos mínimos para as Políticas de Certificados e Requisitos mínimos para as Declarações de Práticas de Certificação).

A Autoridade Certificadora Raiz – AC Raiz é um dos pilares da infra-estrutura de chaves públicas brasileira. A função da AC Raiz é desempenhada pelo Instituto Nacional de Tecnologia da Informação – ITI, autarquia federal vinculada à Casa Civil da Presidência da República. A AC Raiz é a primeira autoridade da cadeia de certificação, consoante dispõe o art 5° da Medida Provisória 2.200. As normas de funcionamento da AC Raiz estão dispostas na Resolução 1 do Comitê Gestor, denominada Declaração de Práticas de Certificação (DPC).

A função fundamental da AC Raiz é funcionar como "âncora de confiança" da hierarquia, emitindo, revogando e gerenciando os certificados digitais das Autoridades Certificadoras situadas em nível imediatamente subseqüente ao seu. Em infra-estruturas onde não existe a figura do "âncora de confiança", os fornecedores de certificados emitem seus certificados auto-assinados, com multiplicação de hierarquias, onde não é possível se chegar a um certificado raiz com confiabilidade.

Por determinação legal a AC Raiz não emite certificados para os consumidores, usuários finais. Na realidade há um processo para credenciar entidades a Autoridades Certificadoras – AC, que consiste num procedimento complexo que prevê pormenorizada auditoria das instalações, rotinas, documentos e práticas das entidades interessadas.

As Autoridades Certificadoras – AC são as principais fornecedoras da ICP-Brasil, pois emitem certificados digitais para os usuários finais. Os requisitos para uma entidade se tornar AC estão dispostos num conjunto de resoluções, onde se destacam: 1) habilitação jurídica; 2) regularidade fiscal; 3) qualificação econômico-financeira; 4) qualificação técnica. Esta última é primordial para o exercício das atividades de uma AC.

Da mesma forma da AC Raiz, as autoridades certificadoras devem dispor de ambiente altamente seguro onde realizarão atividades de emissão e de revogação de certificados. Esse ambiente seguro deverá ter seis (6) níveis de ambientes, compartimentos não identificados com pelo menos quatro(4) níveis de acesso físico ao ambiente da AC e mais dois(2) níveis relativos à chave privada, conforme item 5.1.2.1 da Resolução 8 da ICP-Brasil. Há diversos outros cuidados, entre eles está o da publicação da lista dos certificados revogados (LCR) através da na internet para consulta por parte de qualquer interessado.

Um dos pilares da ICP-Brasil, e de qualquer infra-estrutura de chaves públicas que pretenda ser segura o suficiente é o requisito da identificação do interessado mediante presença física perante uma Autoridade de Registro – AR, que é a entidade que opera na ponta inferior da cadeia, aquela que atinge o usuário final, recebendo as solicitações de emissão de certificados digitais. Os serviços de autoridade de registro poderão ser desempenhados por órgãos ou entidades públicos, ou pelas pessoas de direito privado. As AR serão sempre vinculadas a determinada autoridade certificadora, e no âmbito da ICP-Brasil,

submetem-se à auditoria prévia da AC Raiz, que as credenciará na hipótese de requisitos normativos.

Os pilares jurídicos da Infra-Estrutura de Chaves Públicas brasileira são os §§1° e 2° do art. 10 da MP 2.200. O §1° dispõe que "As declarações constantes nos documentos em forma eletrônica produzidos com a utilização do processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiras em relação aos signatários, na forma do art. 131 da Lei 3071, de 1° de janeiro de 1916 – Código Civil". Este parágrafo tem por escopo atribuir uma presunção de veracidade às declarações de vontade realizadas no ambiente virtual, mediante a utilização de assinatura digital obtida perante uma das certificadoras credenciadas pela AC Raiz da ICP-Brasil. Vale ressaltar que o art. 131 do Código Civil de 1916 foi reproduzido integralmente no art. 219 do Código Civil de 2002.

Este texto legal está tratando da autoria de documentos eletrônicos e determinadno que a assinatura digital aposta a partir de uma chave privada relacionada a uma chave pública inserida em certificado digital obtido no âmbito da ICP-Brasil será equiparada à assinatura de próprio punho.

O §2° do art. 10 da MP 2.200, dispõe que " o disposta na Medida Provisária não obsta a utilização de outro meio de comprovação de autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitidos pelas partes como válido ou aceito pela pessoa a quem for aposto o documento". Foi incluído na primeira reedição da MP e depois consolidado na versão que vige até hoje, por força da Emenda Constitucional (EC) número 32 de 11 de setembro de 2001, onde as Medidas provisórias editadas antes desta EC, não teriam sua eficácia atingida e nem perderiam sua validade. A finalidade do comando é flexibilizar a utilização dos métodos de comprovação de autoria, de maneira a não se tornar obrigatório o uso de certificados

digitais baseados no ICP-Brasil. É uma forma de enfatizar a autonomia da vontade bem como demonstrar a neutralidade tecnológica também da norma.

3 CONSULTA POPULAR VIA INTERNET

3.1 Iniciativa Popular, Plebiscito e Referendo

A forma pela qual os cidadãos participam das deliberações que interessam à coletividade origina três tipos de democracia, que podem ser classificadas em direta, indireta (ou representativa) e semidireta (ou participativa). O termo democracia significou, inicialmente, democracia direta, isto é, uma forma de governo em que os cidadãos tomam as decisões, diretamente, com validade para todos.

Essa democracia pura, em que o povo se autogoverna, de fato, só foi praticada na antigüidade, em Atenas e Roma, mesmo assim com grandes diferenças em relação ao que hoje entendemos como democracia, principalmente em razão das barreiras que a estratificação social impunha a certas classes, como a dos escravos. A expressão democracia representativa significa, de um modo geral, que as deliberações coletivas são tomadas não diretamente pelos membros de uma determinada coletividade, mas por pessoas especialmente eleitas para essa finalidade. Essas pessoas, designadas como representantes, possuem duas características bem estabelecidas: a) por gozarem da confiança do corpo eleitoral, após eleitas não são mais responsáveis perante os próprios eleitores, e seu mandato, portanto, não é revogável; b) não são responsáveis diretamente perante os seus eleitores exatamente porque convocadas a tutelar os interesses gerais da sociedade e não os interesses particulares de uma ou outra categoria. Na democracia representativa, a participação popular é indireta, periódica e formal, e se organiza mediante regras que disciplinam as técnicas de escolha dos representantes do povo.

Todavia, não se trata apenas de uma questão de eleições periódicas, em que, por meio do voto, são escolhidas as autoridades governamentais. Além de designar um procedimento técnico para a designação de pessoas para o exercício de funções governamentais e legislativas, eleição significa a expressão de preferência entre alternativas, a realização de um ato formal de decisão política.

Realmente, nas democracias de partido e sufrágio universal, as eleições tendem a ultrapassar a pura função designatória, configurando um instrumento por meio do qual o povo manifesta sua aprovação a uma política governamental e confere seu consentimento e, por conseqüência, legitimidade às autoridades governamentais, participando na formação da vontade do governo e no processo político.

A idéia de que a democracia se realiza de modo mais amplo e legítimo por meio de constantes consultas populares sobre assuntos políticos, e que se exprime, no caso concreto, como exigência de que a democracia representativa seja complementada e, em alguns casos, substituída pela democracia direta, não é recente, nem se restringe ao Brasil.

O avanço das comunicações e da informática reforça a idéia de que seja possível manter em funcionamento um processo permanente de consulta à população sobre pontos importantes da política. Também no processo eleitoral, com a introdução do sistema eletrônico de votação, estamos dando passos importantes no sentido de facilitar a participação do cidadão em decisões, estabelecendo pré-condições para que, num futuro não muito distante, os cidadãos possam se manifestar sem sair de casa.

Tal entendimento apóia-se no pressuposto de que todos os cidadãos estejam interessados numa participação constante nos assuntos públicos, o que não reflete a realidade política brasileira. Outro dado a se levar em conta é que os assuntos não surgem

espontaneamente, antes são formulados por alguém, que decide também o que vai ser objeto de consulta, quando ela vai ocorrer e o que vai ser feito com o resultado. Para que essas decisões sejam tomadas, não se dispensam os representantes, que estudam e discutem os assuntos, antes de submetê-los à consulta popular. Também em instituições representativas com menor número de participantes, a discussão e o debate prévios são necessários, e geralmente preparados em comissões temáticas, que os encaminham posteriormente à deliberação do grupo maior.

Assim, o processo de democratização, de que se fala atualmente, não consiste, como erroneamente muitas vezes se diz, na passagem da democracia representativa para a democracia direta, mas na passagem da democracia política em sentido estrito para a democracia social. Essa passagem se realiza mediante a ampliação do poder ascendente, que até então se situava quase exclusivamente no campo da grande sociedade política e de associações voluntárias, para o campo da sociedade civil nas suas várias organizações, da escola à fábrica, em que se processa a maior parte da vida dos membros de uma sociedade moderna.

A iniciativa popular consiste na possibilidade de apresentação, pelos cidadãos, de projetos de lei ao Legislativo, desde que subscritos por número razoável de eleitores (conforme determinam os arts. 14, III, e 61, § 2°); o projeto necessita da assinatura de, no mínimo, um por cento do eleitorado nacional, distribuídos pelo menos em cinco Estados, com não menos de três décimos por cento dos eleitores de cada um deles. A Constituição prevê, também, que a iniciativa popular, no processo legislativo estadual, será regulamentada por lei, enquanto que, em relação aos Municípios, estabelece que a sua lei orgânica adotará a iniciativa popular de leis de interesse específico do Município, da cidade ou de bairros, através de manifestação de, pelo menos, cinco por cento do eleitorado.

O referendo popular (previsto no art. 14, II) significa a submissão de projetos de lei aprovados pelo legislativo ao exame direto dos cidadãos, atendidos certos requisitos, tais como pedido de determinado número de eleitores, de certo número de parlamentares ou do próprio chefe do executivo. O projeto será considerado aprovado somente se receber votação favorável do corpo eleitoral. A Constituição estabelece que a autorização para a realização do referendo é da competência exclusiva do Congresso Nacional, conforme determina no art. 49, XV, mas não disciplina as condições de seu exercício. Assim, o Congresso Nacional fica livre para autorizá-lo, até mesmo em matéria constitucional, podendo, também, formular uma lei definindo os critérios e requisitos para o seu exercício.

No Brasil, a utilização do plebiscito para dar maior legitimidade às decisões do Congresso não tem sido prática comum na história constitucional brasileira. Sua primeira inclusão no texto constitucional chega a contradizer a tese, universalmente aceita, de que constitui importante instrumento de participação política popular no processo decisório, e, portanto, de exercício democrático. Com efeito, foi na Constituição de 1937, do Estado Novo, que ele surgiu pela primeira vez, para consulta à população, em quatro situações, a mais importante para dar legitimidade ao texto constitucional, mas sequer chegou a ser realizado em nenhuma delas. Não previsto na Constituição de 1946, o plebiscito foi introduzido pela Emenda Constitucional n° 4, de 1961, para conhecer a preferência do eleitorado sobre a continuidade do sistema parlamentar, que havia sido adotado sem consulta popular. Consultado em janeiro de 1963, por meio do plebiscito, o eleitorado decidiu pelo retorno do sistema presidencial.

Os textos constitucionais de 1967 e 1969 não admitiam o plebiscito como consulta sobre questões políticas, mas permitiam consulta prévia às populações locais para a criação de novos municípios. A forma de consulta prévia adotada pela Lei Complementar n° 1, de 1967,

foi o plebiscito. A Constituição de 1988 é inovadora, pois admite a utilização do plebiscito em quatro situações:

1. como exercício da soberania popular (art. 14, I);

2. como exercício do direito do cidadão de um Estado ou Território Federal a manifestar-se sobre a sua subdivisão, desmembramento ou anexação a outro (art. 18, § 3°);

3. como exercício do direito do cidadão de um município a manifestar-se sobre a criação, incorporação, fusão ou desmembramento desse município ou de parcela dele (art. 18, § 4°);

4. como exercício de sua soberania para a definição da forma e sistema de governo em data determinada – 7 de setembro de 1993 (art. 2° do ADCT).

Dessas quatro hipóteses, apenas uma, relacionada com a definição da forma e do sistema de governo, foi objeto de convocação constitucional, pois o art. 2° do Ato das Disposições Constitucionais Transitórias, que o instituiu, estabeleceu também a data para sua realização, 7 de setembro de 1993.

Assim, a cidadania encontra-se prestigiada, pois o cidadão dispõe de outros meios, além do sufrágio, para participar da vida política. Constitui atribuição exclusiva do Congresso Nacional a convocação de plebiscito, conforme dispõe o art. 49 da Constituição, em seu inciso XV. Tal entendimento não se enfraquece diante da exigência de norma para regulamentar o plebiscito, o referendo e a iniciativa popular, conforme estatui o art. 14 da Constituição. Com efeito, a lei referida no *caput* do artigo, no âmbito da expressão "nos termos da lei", significa, na verdade, a exigência de disciplinamento normativo que dê suporte legal para a realização das três modalidades de soberania popular, não de uma lei específica para regulamentar cada uma delas. Sua regulamentação, para cada caso, deve ser feita pelo Congresso Nacional, por meio de decreto legislativo.

3.2 A história do voto eletrônico no Brasil

Com o advento da eletrônica as máquinas de votar também estão sendo adaptadas a nova tecnologia. O Brasil saiu na frente neste campo da informatização do voto e, em 1996, tornou-se o primeiro país a implantar o voto eletrônico em toda a sua extensão, isto é, desde a identificação do eleitor até a finalização da apuração e totalização dos votos, passando pelo próprio ato de votar.

Experiências com o voto eletrônico têm sido desenvolvidas em outros países, inclusive nos mais ricos e mais avançados tecnologicamente, mas até agora em nenhum deles foi implantado o voto eletrônico de forma completa como no Brasil.

Em 1982, durante o Regime Militar de Exceção, aconteceu a primeira tentativa de informatização da totalização dos votos naquilo que ficou conhecido por Caso Proconsult. A informatização da totalização de votos continuou a se desenvolver nas eleições seguintes.

Em 1985 o lobby do Tribunal Superior Eleitoral - TSE no Congresso Nacional conseguiu a aprovação rápida da Lei 7.444/85 que ordenava a unificação do Cadastro de Eleitores com o uso da computação e dava ao TSE poderes de regulamentar o processo de recadastramento. O TSE decidiu, autonomamente, eliminar a foto do eleitor no Título Eleitoral criando, para alguns, enorme falha de segurança, possibilitando uma fraude simples em que qualquer pessoa pode votar utilizando o título de outra.

Em 1995, em novo lobby do TSE no Congresso Nacional, foi aprovado um projeto redigido seis meses antes por um de grupo de trabalho interno do TSE, resultando na

Lei 9.100/95, que permitia o uso de máquinas de votar eletrônicas e dava ao TSE o poder de regulamentar o seu uso. O TSE optou por usar máquinas de votar de gravação eletrônica direta (DRE) sem comprovante do voto conferido pelo eleitor. Optou ainda pela identificação do eleitor na própria máquina de votar Esta máquina passou a ser chamada de Urna Eletrônica.

Em 1996, 1/3 do eleitorado, aproximadamente 35 milhões de eleitores, votou nas novas urnas eletrônicas sem comprovante do voto conferido pelo eleitor. Em 1998, as urnas foram utilizadas por 2/3 dos eleitores e em 2000, por 100%. Em 1999, surgiu no Senado o primeiro projeto de lei que obrigava que maquinas de votar imprimissem o voto para a conferência do eleitor, criava a auditoria estatística de 3% das urnas a serem sorteadas depois da eleição, impedia a identificação do eleitor na mesma máquina onde fosse votar e obrigava o uso de software aberto nas urnas eletrônicas.

Os juízes-ministros do TSE voltaram a exercer forte lobby no Congresso Nacional e conseguiram, em apenas dois dias de 2001, aprovar 7 emendas no projeto de lei que criou a Lei 10.480/02 a qual adiava a aplicação do voto impresso conferido pelo eleitor para 2004, mandava sortear as urnas a serem auditadas antes das eleições, permitia a identificação do eleitor na máquina de votar e permitia ao TSE utilizar programas de computador fechados nas urnas eletrônicas utilizando assinatura digital.

3.3 Uma visão crítica da urna eletrônica

A utilização da urna eletrônica no Brasil trouxe à tona, principalmente na comunidade científica de segurança da informação, a questão da segurança do voto. Tais equipamentos são computadores que executam programas, muitas vezes ininteligíveis aos olhos dos que participam do processo eletivo, como o eleitor, os fiscais dos partidos, os mesários, que apenas executam os procedimentos repassados pelo corpo técnico do TSE.

Através de relatórios de análises das urnas eletrônicas e partindo de opiniões de técnicos e engenheiros, tudo disponibilizado em fóruns de debates na internet, constata-se que há divergências quanto a possibilidade de fraudes no processo de votação e apuração na utilização da urnas. Foram encontradas inúmeras fragilidades nos seus sistemas de segurança que permitiam, e que poderiam em tese ainda permitir, com grande facilidade a quem precisa manipulá-lo, a execução de mecanismos destinados a desviar ou identificar votos. E o que é pior, de forma também facilmente não detectável a qualquer auditoria *a posteriori* , o que por si só já é uma falha inadimissível.

Um dos pontos apontados como falha no processo seria a possibilidade de alteração dos programas gravados nas urnas de forma que eles pudessem manipular a votação bem como o processo de apuração. Isso se daria depois do prazo que o TSE dá para os partidos com os seus fiscais homologarem as urnas.

Outro fator apontado como falha seria a capacidade de vinculação do eleitor com o respectivo voto registrado o que contraria a inviolabilidade do voto, onde o tipo de máquina utilizada atualmente permitiria plenamente tal vinculação através do programa de votação.

Também é citado a questão da alteração da norma por parte do TSE que não permite a impressão do voto, o que se traduz em uma sensação de desconfiança da real efetivação do voto na urna.

4 CONSIDERAÇÕES FINAIS

Este tema é amplo e intrincado. Tem sido discutido dentro da Internet, no Brasil, pelo *Fórum de Debates do Voto Eletrônico*[16] e, no exterior, por várias listas de debate, como a *NZ Electronic Electoral Trial List* [17] da Nova Zelandia e a *VoteSite.com Mailing List* [18] no estado da Califórnia, EUA.

Na Nova Zelândia está em desenvolvimento um teste público de um sistema de "e-voting"[19], que ocorrerá em paralelo a uma eleição normal, patrocinado por agências governamentais e por universidades, para se avaliar se é possível se implantar um sistema seguro e satisfatório.

Na lista americana tem surgido algumas propostas de "e-voting" com a utilização de *cédulas de voto virtuais assinadas digitalmente* pelo eleitor. Comparando com a votação tradicional, isto equivaleria a imprimir a identificação do eleitor na cédula eleitoral do voto impresso, a inviolabilidade do voto pode ficar totalmente comprometida!

Dentro desta filosofia de segurança máxima até mesmo contra seus projetistas e administradores, o voto eletrônico exige um esquema de segurança muito complexo que esta é a grande barreira que tem impedido a adoção do voto eletrônico integral nos demais países do mundo com a utilização do atual mecanismo da urna eletrônica.

Atualmente o estágio avançado da tecnologia disponível via internet, bem como a a utilização da identificação com assinatura digital e disponibilização de softwares de código-

---

[16] Fórum do Debates do Voto Eletrônico: http://www.brunazo.eng.br/voto-e/forum.htm
[17] NZ Electronic Electoral Trial List: http://NZvotingtrial.listbot.com
[18] The VoteSite.com mailing list: http://votesite.com.listbot.com
[19] E-democracy in New Zealand elections: http://www.polemic.net/nzeet.html

fonte aberto e livres de patentes, acessos cada vez mais rápidos à rede mundial, permite aos brasileiros adentrar num mundo de pesquisa, tecnologia, serviços, opções inimagináveis há poucos anos atrás.

O atual estágio de maturidade tecnológica que se encontra o Brasil, bem como a participação cada vez mais ativa de suas instituições zeladoras do ordenamento jurídico, geram o embasamento para a utilização de um novo estágio da tecnologia no processo de votação no Brasil.

O ambiente da internet é perfeitamente utilizável para qualquer processo que se exija segurança máxima dos dados trafegados de forma a garantir a integridade, o sigilo, a autorização e a privacidade dos usuários.

Os órgãos públicos estão a cada dia aumentando a oferta dos seus serviços via internet e já utilizam numa escala considerável a identificação dos seus usuários com a assinatura digital dentro do padrão da ICP-Brasil. A intenção do Governo em patrocinar a "inclusão digital" proporcionando à população desassistida um acesso gratuito à rede virtual, vai incrementar mais ainda o número de usuários brasileiros na internet.

O TSE já possui em sua base tecnológica todo um acervo de sistemas de gerenciamento, apuração, controle das urnas, restando partir para softwares de controle de urnas virtuais que seriam disponibilizadas pela internet onde o eleitor correspondente àquela urna poderia depositar o seu voto e assinar a lista de presença de forma eletrônica.

O projeto de votação na internet visa inicialmente atender ao instituto da Consulta Popular apregoada pela nossa Constituição Federal para desta forma propiciar uma participação mais efetiva dos cidadãos na vida política na democracia brasileira.

5 REFERÊNCIAS BIBLIOGRAFICAS

A Verdade Absoluta. Criptografia. O algoritmo ElGamal. Disponível na internet no endereço http://www.absoluta.org/cripty/cripty_elgamal.htm.

A Verdade Absoluta. Criptografia. O algoritmo DES. Disponível na internet no endereço http://www.absoluta.org/cripty/cripty_des.htm

CASTRO, Edson de Resende. ***Teoria e Prática do Direito Eleitoral***. Belo Horizonte: mandamentos Editora, 2004.

Computer Emergency Response Team. Rio Grande do Sul. Autenticação. Disponível na internet no endereço http://www.cert-rs.tche.br/docs_html/autentic.html

FINKELSTEIN, Maria Eugênia. ***Aspectos jurídicos do comércio eletrônico***. Porto Alegre: Síntese, 2004.

Fórum Voto Eletônico. Amílcar Brunazo Filho. Página principal. Disponível na internet no endereço http://www.brunazo.eng.br/voto-e/

Fórum Voto Eletônico. Amílcar Brunazo Filho. Simpósio sobre segurança em Informática. A segurança do voto na urna eletrônica brasileira. Disponível na Internet no endereço http://www.iron.com.br/~kika/voto-e/textos/SSI99.htm

GRECO, Marco Aurélio; MARTINS, Ivens Gandra da Silva (coord.). ***Direito e Internet***: relações jurídicas na sociedade informatizada. São Paulo, Editora Revista dos Tribunais, 2001.

LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). ***Direito e Internet***: aspectos jurídicos relevantes. Bauru, Edipro, 2001.

MARCACINI, Augusto Tavares Rosa. ***Direito e Informática***. Ed. Rio de Janeiro: Forense, 2002.

MEIRELLES, Hely Lopes. Direito Administrativo Brasileiro. São Paulo: Malheiros, 1998.

MENKE, Fabiano. ***Assinatura eletrônica***: aspectos jurídicos no direito brasileiro. São Paulo: Editora Revista dos Tribunais, 2005.

MORAES, Alexandre de: ***Direito Constitucional***. São Paulo, Atlas, 2002.

PECK, Patrícia. ***Direito Digital***. São Paulo: Ed. Saraiva, 2002.

REINALDO FILHO, Demócrito (coord.). ***Direito da Informática***: temas polêmicos. Bauru, Edipro, 2002.

SERVE. A Security Analysis of the Secure Electronic Registration and Voting Experiment. Disponível na internet no endereço http://www.servesecurityreport.org/

UFLA. Departamento de Ciência da Computação. A criptografia RSA e o algoritmo chinês do resto. Disponível na internet no endereço

http://www.dcc.ufla.br/infocomp/artigos/v2.1/criptografiaRSA.pdf.