A Segurança dos Documentos Eletrônicos (2ª Parte)

Desta forma, podemos dizer que a assinatura digitalizada não pode ser utilizada para substituir uma assinatura tradicional manual. Não se pode confundir as formas de "assinaturas", as *digitalizadas e as digitais*, principalmente porque a primeira não se modifica, ao passo que na segunda cada documento possuirá uma assinatura diferente, pois o conteúdo da mensagem adicionado à sua chave privada formam um *digesto* de mensagem.

O segundo mecanismo utilizado é chamado de firmas biométricas, as quais fazem o reconhecimento de dados únicos de um ser humano (chamados biométricos) tais como a impressão digital, a íris dos olhos, que sabemos se tratar de dados individuais.

Biometria é a ciência que estuda formas de identificar seres humanos pelas partes de seu corpo. Uma firma biométrica é uma tecnologia recente que permite reconhecer pessoas por suas características físicas como a íris dos olhos ou impressões digitais.

A biometria é amplamente utilizada nos Estados Unidos, principalmente em indústrias e na área governamental, sendo uma novidade em nosso país.

Existem cinco modos básicos de identificação, todos eles ligados à análise de alguma parte do corpo: impressão digital, leitura da íris, escaneamento de retina, cálculo geométrico da face e reconhecimento da voz. Dos modos acima apresentados os mais utilizados são os que analisam o dedo e a voz.

Isso significa que se a pessoa não for cadastrada ou utilizar um dedo diferente para a identificação, seu acesso será negado.

O que ocorre é que uma firma biométrica, apesar de ser capaz de identificar perfeitamente o indivíduo que a originou, não apresenta nenhuma vinculação com o conteúdo do documento eletrônico, uma vez que está diretamente vinculada a dados subjetivos.

Não podemos esperar que uma firma biométrica nos forneça segurança aos documentos eletrônicos.

Como é cada vez maior o número de senhas que temos que memorizar, o uso da autenticação biométrica é encarado como vantajoso, pois mantém um suporte técnico para grande número de pessoas que esquece os números e letras de acesso, as empresas não terão que gastar com tecnologia e recursos humanos para garantir o fornecimento e a troca regular de senhas, para manter esse sistema funcionando com segurança.

Com o intuito de proporcionar ao comércio eletrônico um maior crescimento, as empresas pontocom estão investindo nessa tecnologia; e, como exemplo, podemos mencionar a Microsoft, que nas versões futuras do Windows promete disponibilizá-la. Já existem teclados com sensores digitais, chips biométricos embutidos no *mouse* e nos monitores.

O uso de espécies de senhas é o terceiro modo que visa suprir as mesmas finalidades exigidas de uma

assinatura tradicional, sendo elas o PIN (*Personal Identification Number* ou Número de Identificação Pessoal), a *password* (palavra de passagem ou de aprovação) e a *passphrase* (frase de passagem ou de aprovação).

A última forma é a menos conhecida, mas as duas primeiras são utilizadas em larga escala nos dias atuais, como por exemplo, os terminais de caixas bancários automáticos, fechaduras eletrônicas, acionamento de alarmes etc.

Seus resultados não diferem em muito das firmas biométricas, pois se tratam de senhas que têm função de reconhecimento de seu portador.

Um PIN nada mais é do que um simples número, com aproximadamente quatro dígitos ou mais; um *password*, como o próprio termo já nos diz é uma palavra, já a *passphrase*, é formada por um conjunto de palavras separadas, como se fosse uma frase (podemos entendê-la como o conjunto de várias *passwords*).

O funcionamento de tais senhas se dá de maneira simples e fácil: uma vez que a pessoa tenha um código de acesso válido, e demonstre isso informando-lhe um sistema qualquer de verificação, ela adquire legitimidade para efetuar as ações restritas a pessoas autorizadas.

A diferença entre as firmas biométricas e as senhas é que as primeiras não constituem um segredo as qualidades físicas de determinada pessoa e sim simplesmente um meio capaz de identificar perfeitamente o indivíduo que a originou, já as segundas têm caráter sigiloso.

3.3. Assinatura digital

Um documento digital não pode ser assinado no modo tradicional, através do qual o autor se identifica por meio de sua assinatura manuscrita; contudo, surge uma forma nova de assinar, sendo ela conhecida como assinatura digital.

Os documentos eletrônicos, como todos sabem, possuem as características de alterabilidade e fácil falsificação, mas mesmo com todas estas implicações podem ter validade jurídica, desde que preencham os requisitos necessários.

Essa “assinatura” tem função de lacrar o conteúdo do documento, fazendo com que este permaneça íntegro, ou se for minimamente alterado, que isso possa ser constatado; também garante a autenticidade e a tempestividade.

Bill Gates, com total propriedade, explica o fenômeno da assinatura digital:

“*Quando você mandar uma mensagem pela estrada da informação, ela será “assinada” pelo seu computador, ou outro dispositivo de informação, com uma assinatura digital que só você será capaz de aplicar, e será codificada de forma que só seu destinatário real será capaz de decifrá-la. Você enviará uma mensagem, que pode ser informação de qualquer tipo, inclusive voz, vídeo ou dinheiro digital. O destinatário poderá ter certeza quase absoluta de que a mensagem é mesmo sua, que foi enviada exatamente na hora indicada, que não foi nem minimamente alterada e que outros não podem decifrá-la*

“.*(18)*

Ressalta-se que o objetivo da assinatura digital não é o de tornar a mensagem ilegível, pois ela em si não é encriptada, é apenas acrescentada à mensagem eletrônica, mantendo-a ilesa. Assim, podemos dizer que sua função precípua é a de elevar o estado de segurança do documento assinado.

Ao analisarmos os documentos tradicionais, podemos constatar que os requisitos essenciais que comprovam seu efeito probatório estão de modo notável apostos em um suporte material; já os documentos eletrônicos não necessitam obrigatoriamente de um continente, sendo que sua própria substância ou conteúdo já o comprovam.

A autenticidade pode ser garantida pela chave codificadora, como nos ensina Bill Gates:

“*A chave codificadora permite mais do que privacidade. Ela pode também garantir a autenticidade de um documento, porque a chave privada pode ser usada para codificar uma mensagem que só a chave pública pode decodificar. Funciona assim: se eu tenho uma informação que quero assinar antes de mandar de volta para você, meu computador usa minha chave privada para codificá-la. Agora a mensagem só pode ser lida se minha chave pública-que você e todo mundo conhece – for usada para decifrá-la. Essa mensagem é com certeza minha, pois ninguém mais tem a chave privada capaz de codifica-la dessa forma*“.*(19)*

3.4. Criptografia como segurança de dados

A criptografia está intimamente relacionada com a segurança dos dados, assumindo um papel cada vez mais importante devido à grande quantidade de informações que são movimentadas e a utilização crescente da rede de computadores.

Davi Monteiro Diniz nos ensina que “*criptografia consiste em uma escrita que se baseia em um conjunto de símbolos cujo significado é conhecido por poucos, permitindo com isso que se criem textos que serão incompreensíveis aos que não saibam o padrão de conversão necessário para a sua leitura*“. *(20)*

Desta forma, uma mensagem só será criptográfica se tiver sido gerada a partir de um sistema metalinguístico e, ainda, tiver uma intenção enigmática.

Ângela Bittencourt Brasil esclarece que a técnica de assinatura feita através da criptografia e da criptoanálise “consiste numa mistura de dados ininteligíveis onde é necessário o uso de duas chaves, a pública e a privada, para que ele possa se tornar legível”. Compara a criptografia como sendo semelhante ao segredo de um cofre forte. Esclarece, ainda, que essa assinatura é formada por uma série de letras, números e símbolos e é feita em duas etapas, sendo que na primeira o autor, através de um software que contém um algoritmo próprio, realiza uma operação e faz um tipo de resumo dos dados do documento que quer enviar, também chamado de função hash. Em um segundo momento, ele utiliza a chave privada, a qual irá encriptar esse resumo e o resultado desse processo, que é a assinatura digital. Em conclusão, aponta a mesma autora que a assinatura eletrônica, diferentemente da assinatura real, se modifica a cada arquivo transformado em documento, fazendo com que seu autor não a repita, como faz

com as assinaturas apostas nos documentos reais. *(21)*

Existem essencialmente duas grandes técnicas de criptografia, denominadas simétrica e assimétrica. A criptografia simétrica, também conhecida como chave secreta ou tradicional, é a mais antiga. Utiliza-se somente de uma chave, a qual está vinculada ao processo de cifragem e decifragem. Em se tratando de criptografia assimétrica, também conhecida como chave pública, é utilizado um par de chaves, uma delas a pública, podendo ser amplamente conhecida, e a outra, a chave privada, conhecida apenas por seu proprietário. Aqui as chaves são totalmente independentes entre si; porém, uma chave completa a outra.

Conclui-se desta forma que a mensagem que é cifrada por uma chave privada somente poderá ser decifrada por uma chave pública correspondente.

Podemos contar com duas formas distintas de criptografia, a simétrica e a assimétrica. A criptografia simétrica tem se revelado mais rápida que a assimétrica. Por isso, se o trabalho envolver um volume grande de dados, sua utilização será apropriada. Contudo, se o que é visado é a segurança da mensagem, a técnica a ser utilizada é a assimétrica.

Temos que visualizar que o primeiro grande efeito da autenticação eletrônica é o aprimoramento do comércio eletrônico, proporcionando aos usuários uma maior segurança nas celebrações dos diversos negócios jurídicos, pactuados na Internet. A certificação eletrônica tem a função de garantir a origem e a identidade do signatário do documento digital, permitindo a autenticidade da operação, reconhecendo as assinaturas eletrônicas, as quais são fornecidas por uma Autoridade Certificadora.

3.5. A autoridade certificadora

A autoridade certificadora tem a função de fornecer aos usuários os pares de chaves utilizados tanto para a assinatura digital como para a criptografia. É ela que fornece os certificados digitais, os quais podem ser definidos como um arquivo de computador que identifica quem você é para as outras pessoas, além de evitar o repúdio.

De uma forma simples, Ângela Bittencourt Brasil conceitua autoridade certificadora como sendo:

"*A pessoa encarregada de fornecer os pares de chaves. Essa autoridade é uma entidade independente e legal habilitada para exercer as funções de distribuidor das chaves e pode ser consultada a qualquer tempo, certificando que determinada pessoa é a titular da assinatura digital da chave pública e da correspectiva chave privada*". *(22)*

A identificação e a autenticação das pessoas que assinam os documentos eletrônicos serão feitas pela Autoridade Certificadora, passando a intermediar a relação entre os usuários, por meio do sistema cifrado de comunicação assimétrico.

Recentemente, foi expedida a Medida Provisória nº 2.200, de 28 de junho de 2001, que dispõe sobre a Infra-Estrutura de Chaves Públicas Brasileiras- ICP- Brasil, que institui o Comitê Gestor de Políticas

como órgão apto a fornecer os certificados eletrônicos, que irão garantir a segurança e demais aspectos já delineados dos documentos digitais.

O presidente da OAB-SP, Carlos Miguel Aidar, em crítica à medida provisória acima citada, argumenta que o presidente da República mais uma vez utilizou tal instituto de forma arbitrária, posto que ignorou toda uma discussão sobre a matéria, que vem sendo feita pela sociedade, pelo Congresso, etc. *(23)*

O mesmo autor enfatiza que a MP acima citada viola os princípios de liberdade de empresa e liberdade de contratação, haja vista ter colocado apenas como autoridade certificadora um órgão público, deixando de prever a possibilidade de empresas privadas atuarem na mesma função, como ocorre em muitos os outros países.

Concordamos com o posicionamento acima, uma vez que cabe aos usuários a escolha da empresa que fará a certificação de seus documentos, não ficando restritos a um órgão público, o único dotado de poder para tanto, ferindo, assim, o princípio da livre contratação.

3.6. Regulamentação do documento digital

No Brasil inexiste uma definição legal de documento eletrônico e, da mesma forma, não há uma legislação específica que ampare as negociações cibernéticas. Essa nova realidade faz com que busquemos nos adaptar à tecnologia crescente e regulamentar a questão, de forma a não permitir a estagnação econômica do país.

Antônio de Andrade e Silva, diretor do Centro Nacional de Desenvolvimento do Gerenciamento da Informação (Cenadem), afirma que "*a lei brasileira ainda falha no reconhecimento do documento digital e por isso as empresas têm de guardar cópias impressas do que já está armazenado nos CDs*". *(24)*

Maristela Basso, em sugestão de como deve ser a legislação brasileira a respeito do tema, afirma que não é preciso que a lei seja detalhista e queira, de uma só vez, disciplinar todos os aspectos envolvidos no comércio eletrônico. Tal finalidade geraria um erro em razão da dinamicidade das trocas eletrônicas e a constante evolução dos meios de comunicação e de segurança empregados. Em proposta, argumenta que a legislação deverá ser feita de forma consentânea com os parâmetros internacionais na "Lei Modelo da Uncitral" *United Nations Commission on International Trade Law* (Lei Modelo sobre Comércio Eletrônico aprovada pela Comissão das Nações Unidas para o Direito Comercial Internacional) o que pode ser feito observando-se as regras internas brasileiras de incorporação e os princípios de ordem pública local. *(25)*

O projeto de lei que existe busca regulamentar a Internet, equiparando a assinatura digital àquela convencionalmente aposta em um suporte físico, com o escopo de que as relações *on line* possam ter a mesma eficácia das tradicionais.

Em respeito a todas essas funções que o documento em papel proporciona, a lei modelo da Uncitral estabelece que os registros eletrônicos, para que recebam o mesmo nível de reconhecimento legal, devem satisfazer, no mínimo, o mesmo grau de segurança que os documentos em papel oferecem, o que

deve ser alcançado por de uma série de recursos técnicos. Em suma, a lei modelo estabelece uma série de requisitos para que um documento eletrônico alcance uma função equivalente ao documento escrito, assinado e original.

Em se tratando de documento eletrônico, a ordem jurídica nacional não se ajustou à nova realidade existente em nosso país,visto que até o presente momento, o assunto em questão não recebeu tratamento jurídico.

Rosana Ribeiro da Silva, com fundamento no dinamismo e na evolução social, entende que o direito, ao visar regular os hábitos e atividades sociais, deve necessariamente acompanhar a evolução desta, alterando ou dando novas interpretações às regras jurídicas existentes. Acrescenta, ainda, que compete ao direito regular as relações entre indivíduos, dando-lhes segurança e estabilidade nas relações jurídicas que os mesmos estabelecem, o que abrangeria também as relações que se originam da internet. *(26)*

4. Conclusão

1. Com o questionamento da segurança da nova forma de documentação, surgem mecanismos informáticos que nos garantem a autenticidade, a integridade e a tempestividade do documento eletrônico. Quanto à possibilidade dos documentos digitais serem equiparados aos tradicionais, podemos dizer que havendo uma lei específica que os regulamente, não há que se falar em repúdio. Assim, serão plenamente válidos se todos os requisitos inerentes a eles forem observados.

2. Referentemente aos documentos tradicionais, podemos concluir que a idéia de sua materialização é relevante na sua conceituação para a maioria dos autores; de tal modo, o conteúdo do documento está intimamente ligado ao seu continente. Existem conceitos de documentos tradicionais que ressaltam sua materialidade; porém, também podemos encontrar quem leva em consideração seu conteúdo, dando ênfase ao seu elemento espiritual. Modernamente, devemos permitir a separação de seus elementos, uma vez que são distintos e, por isso, não podemos confundir seu conteúdo com seu instrumento de apresentação.

3. Verificando as limitações que os documentos tradicionais, apostos em papel, nos apresentam quanto à rapidez e agilidade na circulação das informações, devemos repensar seu conceito. Com esse intuito, caminha a doutrina para uma maior flexibilização, visando adaptar aos conceitos de documento a qualidade de dados digitais, não relacionados à materialização. Diante desse entendimento, podemos concluir que não importa sua forma de apresentação, não prosseguindo a dependência de seu conteúdo com seu elemento continente. Alguns pontos devem ser revistos, pois o que realmente tem relevância é que o documento cumpra sua finalidade.

4. O documento digital é aquele que nos representa um fato, mas para termos acesso a ele é necessária a intervenção de um programa de computador. Assim, podem ser conceituados como aqueles que se encontram arquivados em formato digital, não podendo ser percebido pelo homem sem o auxílio de um computador. É ele uma seqüência de bits, que, traduzida, nos representará um fato. Devem ser encarados abstratamente. A vantagem desse novo modelo de documentação é que sua transmissão é mais rápida e

seu armazenamento mais bem administrado.

5. Para que o documento digital tenha validade jurídica é necessário que atenda a alguns requisitos, tais como a integridade, a autenticidade e a tempestividade. É muito importante podermos identificar a paternidade do documento, se foi ou não alterado seu conteúdo, bem como o tempo em que foi criado.

6. Com o fim de igualar os documentos digitais aos tradicionais, a informática nos apresenta uma maneira inovadora de assinar, que é a assinatura digital, visando a aumentar a confiança de seus usuários, garantindo, assim, que os requisitos inerentes a eles sejam verificados. Com a assinatura digital, seu usuário tem certeza de que o documento não será modificado, sem deixar vestígios e também o destinatário poderá confiar que a mensagem é mesmo de seu autor e que foi enviada exatamente na hora indicada. A cada mensagem a assinatura será diferente, pois ela utiliza o conteúdo do texto e sua chave privada, formando o que chamamos de digesto de mensagem. Conseqüentemente, cada documento terá uma assinatura diferente, pois seus conteúdos são diferentes, não tendo em hipótese alguma intenção de torná-la ilegível. Sua finalidade precípua é elevar a segurança do documento assinado.

7. Ligada diretamente à segurança do documento digital encontramos a criptografia, que é o mecanismo utilizado para tornar a mensagem ilegível para aqueles que não conheçam seu critério de transformação. Aqui sim existe intenção enigmática, diferentemente da assinatura digital. São utilizadas duas chaves, uma pública e a outra privada, sendo que somente desta forma o documento passará a ser legível pelo destinatário. O que uma chave desse par cifrar, somente a outra chave do mesmo par poderá decifrar.

8. Com intuito de proporcionar aos documentos digitais validade jurídica, devem ser criadas autoridades certificadoras, que fornecem aos usuários os pares de chaves. Essas autoridades têm responsabilidade quanto aos dados que confirmam, como também quanto à identificação e autenticação que fazem, ao intermediar relações entre as pessoas. Com a Medida Provisória nº 2.200, de 28 de junho de 2001, a matéria referente às Autoridades Certificadoras foi regulamentada. A respeito da MP, concluímos que o Presidente da República não poderia ter instituído o privilégio exclusivo ao Poder Público de autenticar os documentos digitais, ferindo, assim, os princípios da liberdade contratual e de empresa.

9. Por inexistir uma lei específica abordando o comércio eletrônico, o documento eletrônico e a assinatura digital não recebem, por enquanto, validade jurídica, mas alguns países, como os E.U.A, já o fizeram. Temos que nos adaptar à nova forma de documento, pois a tecnologia cresce a cada dia e não podemos permanecer estáticos frente às transformações. Devemos seguir os parâmetros fornecidos pela Lei Modelo da Uncitral, visando a uma uniformização das leis referentes ao tema. Essa futura lei deverá estabelecer que os registros eletrônicos satisfaçam o grau de segurança que os documentos em papel nos oferecem, o que deve ser alcançado por meio de uma série de recursos técnicos. Da mesma forma, deverá conter o conceito de todos os itens relacionados com o comércio eletrônico. Nossa futura legislação, destarte, deverá regulamentar de forma clara as questões relativas à segurança nas transações feitas com o auxílio da Internet.

Referências bibliográficas

ALVIM, Arruda. *Manual de Direito Processual civil*. 6. ed. São Paulo: Revista dos Tribunais, 1997, v. 2.

BASSO, Maristela. (2000) *Prudência no comércio eletrônico*

Site www.jus.com.br/doutrina/comerc2.html

BRASIL, Ângela Bittencourt. (2000) *Assinatura digital não é assinatura formal* Site www.jus.com.br/doutrina/assidig2.html

e (2001) *Assinatura Digital*

Site www.jus.com.br/doutrina/assigi.html

CHIOVENDA, Giuseppe. *Instituições de Direito Processual civil*. Campinas: Bookseller, 1998, v. 3.

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

DRUCKER, Peter.*Revista Exame Digital*, São Paulo: Abril, ed. 710, ano 34, n. 6, mar. 2000.

FERREIRA, Aurélio B. de Holanda. *Novo dicionário da língua portuguesa*. Rio de Janeiro: Nova Fronteira, 1996.

FOLGLIETTI, Felice. *E o fim da papelada?* Infoexame, São Paulo: Abril, jan. 2001.

GATES, Bill. *A estrada do futuro*. São Paulo: Companhia das Letras, 1995.

MARCACINI, Augusto Tavares Rosa. (2000) *O documento eletrônico como meio de prova*

Site www.advogado.com/internet/zip/tavares.htm

MARQUES, Jose Frederico. *Manual de processo civil* Campinas: Bookseller, 1997, v. 2.

NASCIMENTO, Amauri Mascaro. *Curso de Direito Processual do trabalho* 16ª ed. ampl. atual. São Paulo: Saraiva, 1996.

NOTÍCIAS OABSP. (2000) Site www.oabsp.org.br/main3.asp?pg=3.2&pgv=a&

id_noticias=963

SANTOS, Moacyr Amaral. *Primeiras linhas de Direito Processual civil*. 18. ed. São Paulo: Saraiva, 1997, v. 2.

SILVA, Rosana Ribeiro da. (2001) Contratos Eletrônicos. *http://www.jus.com.br/doutrina/contrele.htm*

THEODORO JUNIOR, Humberto. *Curso de Direito Processual civil*. 36. ed. Rio de Janeiro: Forense, 2001, v. 1.

VELHO, Adriana Haack. .A. validade do documento eletrônico (2000) *http://www.buscalegis.ccj.ufsc/a_validade_do_documento_eletrônico.htm*

VIEIRA, Eduardo. *Infoexame*, São Paulo: Abril, ano 15, n. 175, out. 2000.

Notas de rodapé

1 *Revista Exame Digital*. São Paulo: Abril, edição 710, ano 34, n. 6, mar. 2000, p. 113.

2 Apud VIEIRA, Eduardo. E o fim da papelada? Infoexame, São Paulo: Abril, ano 15, n. 175, out. 2000, p. 84.

3 A estrada do futuro. São Paulo: Companhia das Letras, 1995, p. 145.

4 Idem, ibidem, p. 173.

5 Novo dicionário da língua portuguesa. 2. ed. rev. Rio de Janeiro: Nova Fronteira, 1996, p. 605.

6 Manual de processo civil. 1. ed. atual. Campinas: Bookseller, 1997, v. 2, p. 233.

7 Instituições de Direito Processual civil. 1. ed. Campinas: Bookseller, 1998, v. 3, p. 151.

8 Primeiras linhas de Direito Processual civil. 18. ed. São Paulo: Saraiva, 1997, v. 2, p. 385.

9 Manual de Direito Processual civil. 6. ed. São Paulo: Revista dos Tribunais, 1997, v. 2, p. 492.

10 Curso de Direito Processual civil 36. ed. Rio de Janeiro: Forense, 2001, v. 1, p. 393.

11 Curso de Direito Processual do trabalho. 16. ed. ampl. atual. São Paulo: Saraiva, 1996, p. 262.

12 MARCACINI, Augusto Tavares Rosa. (2000) O documento eletrônico como meio de prova. http://www.advogado.com/internet/zip/tavares.htm

13 Opus cit., p.148.

14 (2000) http://www.advogado.com/internet/zip/tavares.htm.

15 (2000) http://www.advogado.com/internet/zip/tavares.htm

16 (2000) http://www.advogado.com/internet/zip/tavares.htm.

17 Opus cit., p.452.

18 Opus cit., p.138.

19 Opus cit., p.142

20 Documentos eletrônicos, assinaturas digitais: da qualificação jurídica dos arquivos digitais como documentos. São Paulo: LTr, 1999, p. 28.

21Assinatura digital não é assinatura formal. (2000) http://www.jus.com.br/doutrina/assidig2.html

22 Assinatura Digital. (2001) http://www.jus.com.br/doutrina/assidi.html

23 NOTÍCIAS OABSP.(2001) http://www.oabsp.org.br/ main3asp?pg= 3.2&pgv =a&id_noticias = 963

24 Apud VIEIRA, Eduardo. Opus cit., p. 86.

25 Prudência No Comércio Eletrônico (2000) http://www.jus.com.br /doutrina/ecomec2.html

26 Contratos Eletrônicos. (2001) http://www.jus.com.br/ doutrina/co

Date Created
15/05/2002