A assinatura digital como prova de autoria do documento eletrônico[1]

Mário Furlaneto Neto[2]

Giuliano Bellinetti[3]

Resumo: Para se investigar cientificamente a questão da assinatura digital como prova da autoria do documento eletrônico, fez-se necessário, inicialmente, através de uma revisão bibliográfica, abordar a conceituação de documento, desde sua origem etimológica, passando pela forma documental, até chegar ao conceito de documento eletrônico, para, posteriormente, dispor sobre a questão da assinatura digital. Assim, foram elencados aspectos como o código secreto, a assinatura digitalizada, a assinatura digital (criptografia simétrica e assimétrica) e a chave biométrica. Pode-se concluir ser a assinatura digital, por intermédio da criptografia assimétrica, meio hábil para garantir autenticidade, integridade e validade jurídica do documento eletrônico, porém, necessário se faz que a comunidade jurídica discuta cientificamente as resoluções e projetos de lei que abordam a matéria, como forma de contribuir para a melhoria do processo.

Palavras-chave: documento eletrônico, assinatura digital, criptografia assimétrica.

Abstract: In order to investigate the digital signature issue as an evidence of the responsibility for the electronic document, it has been necessary, initially, through a bibliographic review, to approach the document conceptualization, since its etymological origin, going through the documental form, until it gets to the concept of electronic document, to subsequently, deal with the digital signature issue. Therefore, it has been chosen aspects such as the hidden code, the digitized signature, the digital signature (asymmetrical and symmetrical cryptography) and the biometrical key. It can be concluded that the digital signature, through the asymmetrical cryptography, is a skilful way to guarantee the authenticity, integrity and legal validity of the electronic document. However, it's necessary that the juridical community discusses scientifically the resolutions and law projects which approach the issue as a way of contributing to the process improvement.

Keywords: electronic document, digital signature, asymmetrical signature.

1 O presente artigo surgiu no decorrer das discussões do NEPI – Núcleo de Estudos, Pesquisas, Integração e Práticas Interativas do UNIVEM – Centro Universitário Eurípides de Marília, mantido pela Fundação de Ensino "Eurípides Soares da Rocha".

2 Delegado de Polícia, Mestre em Ciência da Informação pela UNESP de Marília, Professor de Processo Penal do UNIVEM, membro e pesquisador do NEPI. E-mail: mariofur@flash.tv.br.

3 Graduando em Direito no UNIVEM e membro do NEPI. E-mail: gbellinetti@ig.com.br.

Resumen: Para investigar científicamente la cuestión de la firma digital, como prueba de la autoría del documento electrónico, se hizo necesario, inicialmente a través de una revisión bibliográfica, abordar la conceptualización del documento, desde su raíz etimológica, pasando por la forma documental, hasta llegar al concepto de documento electrónico, para , posteriormente, hablar sobre la cuestión de la firma digital. Por lo tanto, han sido catalogados aspectos como el código secreto, la firma digitalizada, la firma digital (criptografía simétrica y asimétrica) y la clave biométrica. Se puede concluir que la firma digital, por intermedio de la criptografía asimétrica, es un medio hábil para garantizar autenticidad, integridad y validez jurídica del documento electrónico. Sin embargo, es necesario que la comunidad jurídica discuta científicamente las resoluciones y los proyectos de ley que abordan el asunto, como manera de contribuir con la mejoría del proceso.

Palabras-clave: documento electrónico, firma digital, criptografía asimétrica.

Introdução

A *Internet* pode ser considerada o maior sistema de comunicação interativo com que a humanidade já se deparou. Em apenas 35 anos, já soma 600 milhões de usuários mundialmente interligados (Módulo Security – 9ª Pesquisa Nacional de Segurança da Informação).

Esse sistema de comunicação interativo fez surgir a cibercultura, definida por Lévy (1999, p. 17) como o "conjunto de técnicas (materiais e intelectuais) de práticas, de atitudes, de modos, de pensamentos e de valores que se desenvolvem juntamente com o crescimento do ciberespaço"[4].

Justamente neste contexto é que os empresários do setor comercial enxergaram um grande filão, o *e-commerce* ou comércio eletrônico.

Somente no Brasil, em um cenário de 30 milhões de usuários interligados à grande rede, estima-se que 3 milhões de internautas façam compras pela *Internet*, gerando um faturamento na ordem de 1,7 bilhões de reais (Módulo Security – 9ª Pesquisa Nacional de Segurança da Informação).

A título de exemplificação e voando em direção ao *e-commerce*, as companhias aéreas foram responsáveis por 13% do volume de transações no comércio eletrônico no mês de setembro de 2004, de maneira que, atualmente, Gol e Varig vendam cerca de 80% de seus bilhetes via *web* (Balieiro, 2005).

Segundo Sposito (2005), o portal Submarino estima um faturamento de 300 milhões de reais em 2004, contra 212 milhões no ano anterior, enquanto a rede varejista Magazine Luiza estimou um aumento de 100% nas vendas pela *Internet* em 2004, o que, atualmente, representa praticamente 12% da receita total da empresa.

Porém, ao mesmo tempo em que o comércio eletrônico cresce exponencialmente, os golpes digitais desenvolvem-se em um ritmo acelerado. Assim, o número de ataques a computadores de empresas aumentou 34% em apenas um ano, de maneira a alcançar a cifra de 400 milhões de reais de prejuízo em 2004 (Módulo Security – 9ª Pesquisa Nacional de Segurança da Informação).

Para atingir a boa-fé do usuário e ludibriá-lo, de forma a obter dados cadastrais importantes ou a vantagem indevida, os autores dos golpes digitais realizam as mais variadas condutas.

Assim, a arquitetura do golpe digital pode compreender o envio de um simples *e-mail*, denominado de *phishing scam* e intitulado por Fortes (2005) como a praga de 2004, a um *keylog*, programa malicioso instalado na máquina da vítima.

O *phishing scam* é uma mensagem fraudulenta, normalmente com características idênticas a de uma instituição financeira ou comercial, que visa a induzir o usuário a preencher formulários com seus dados cadastrais ou confirmar contas bancárias, senhas ou número do cartão de crédito. De posse dos dados, o agente consegue subtrair dinheiro da conta corrente do internauta, acessando-a por meio do *home banking*, ou mesmo fazer compras na *web* ou por telefone mediante o pagamento com o cartão de crédito da vítima.

Por sua vez, o *keylog* ou cavalo de tróia são pequenos programas maliciosos que são inseridos no computador do internauta, normalmente mediante *e-mail*, cuja finalidade é a de subtrair dados. Assim, quando o usuário acessa um *home banking* e digita sua senha e os dados de sua conta corrente, estas informações são monitoradas e

retransmitidas ao invasor, que de posse delas, poderá, igualmente, acessar a conta corrente da vítima e efetuar saques fraudulentos.

Diante do contexto de crescimento do comércio eletrônico e dos golpes digitais, necessário se torna a adoção de mecanismos para garantir confiabilidade e segurança nas transações eletrônicas, em cujo contexto se insere a prova da autoria da transação ou do documento eletrônico, motivo pelo qual, com o presente artigo, mediante uma revisão literária, pretende-se resgatar a questão da assinatura digital como prova de autoria do documento eletrônico.

Inicialmente, resgatar-se-á a conceituação de documento eletrônico como embasamento para tratarmos a questão da assinatura digital e os processos utilizados para a sua efetivação.

Documento: conceituação e tipologia[5]

Em um sentido etimológico, documento tem sua origem nos termos latim *doceo* e *disco*, que significam ensinar e aprender, bem como no termo *mentum*, instrumento. Portanto, seria o instrumento de ensinar ou para aprender.

Para López Yepes (1997, p. 12, tradução nossa), o documento possui duas facetas: a de "testemunho para ensinar e transmitir conhecimentos" e a de "testemunho como prova".

Conferindo um caráter mais amplo e geral ao conceito de documento, Núñez Contreras (1981, p. 32, tradução nossa) o define como "um objeto corporal, produto da atividade humana que lhe reflete e que conserva e transmite permanentemente a representação de um fato alheio, alheio ao próprio documento".

No mesmo sentido, Chiovenda (1965, apud Marcacini, 1999) salienta ser "toda representação material destinada a reproduzir determinada manifestação do pensamento, como uma voz, fixada duradouramente".

No dizer de Guimarães (1998, p. 99), "aos olhos da Diplomática[6], o documento atua como materialização de um ato jurídico-administrativo, de modo a surtir efeitos jurídicos". Segue o autor dizendo que "mais do que mero suporte de informação (como alude a Biblioteconomia) ou ainda meio de prova (como no Direito), o documento é enfocado a partir do contexto de seu órgão gerador, tendo, assim, uma função precípua (e originária)"[7].

Em termos de estrutura documental, autores como Bellotto (1991) e Núñez Contreras (1981) arrolam como elementos constitutivos o trinômio matéria, meio e conteúdo, denominados por Heredia Herrera (1988) como suporte, estrutura e conteúdo. Em um raciocínio inverso, tem-se que o conteúdo do documento (um texto biográfico, um testamento, um relato, etc) é representado por um meio (como por exemplo, sinais gráficos, pintura a óleo, etc) e sedimentados em uma matéria (suportes como a pedra, o pergaminho, o papel, etc).

Ao tratar sobre o meio ambiente de um documento tradicional, Duranti (*Interpares Project*, 2003, tradução nossa) delimita como seus componentes necessários básicos os seguintes:

1. meio: suporte material do conteúdo do documento;

2. conteúdo: os fatos narrados no documento;

3. forma: os modos pelos quais o conteúdo é manifestado, que podem ser físicos (características externas ou elementos extrínsecos do documento, tais como formato, cores, etc) ou inte-

lectuais (características de composição internas ou intrínsecas do documento, como configurações, articulações textuais e anotações);

4. pessoas: entidades reconhecidas pelo sistema jurídico como capazes para o ato, podendo ser físicas ou jurídicas.

5. atos: condutas de criação, manutenção, modificação ou extinção de situações, como por exemplo, o ato de transação, capaz de mudar a relação entre duas pessoas ou mais.

Em decorrência de o objetivo do presente artigo ser o de analisarmos mecanismos confiáveis de prova de autoria do documento eletrônico, necessário se faz conferirmos uma atenção especial ao elemento pessoa, pois segundo o *Interpares Project* (2003, tradução nossa), independentemente de serem físicas ou jurídicas, em todo documento necessariamente concorrem três pessoas:

a) Autor: pessoa competente para a criação do documento, ou seja, sua edição ou comando. Pode coincidir ou não com o autor da ação;

b) Destinatário: a pessoa para quem o documento é dirigido. O destinatário pode ou não coincidir com o destinatário da ação. O destinatário não é necessariamente a pessoa para quem um documento é remetido ou transmitido;

c) Escritor: a pessoa intelectualmente responsável pela origem do documento.

Existem outras duas pessoas que podem estar envolvidas com a criação do documento, mas não necessariamente existentes. São:

d) Subscritor ou Firmante: pessoa que valida a forma do documento, o procedimento de sua criação, ou seu conteúdo, como ocorre nos casos de fé pública do escrevente judiciário.

e) Testemunha: a pessoa que sinaliza o documento para o propósito de conferi-lo solenemente; autenticando a assinatura do autor, o conteúdo do documento, ou suas cópias; ou conferindo atos orais ou escritos que dependam de requisitos formais, como o juramento, feito em sua presença.

Os elementos do documento tradicional apontados por Duranti (1996) serviram de base para o *Interpares Project* (2003, tradução nossa) iniciar a pesquisa dos elementos essenciais para conferir a autenticidade de um documento eletrônico. Com o transcorrer da pesquisa, esses elementos foram revistos e ampliados, de forma a se propor os seguintes requisitos de identidade e integridade:

Quadro 1 – Elementos do documento eletrônico
A.1: Expressões dos atributos do documento e *linkage* para o documento:
A.1.a Identidade do documento:
A.1.a.i Nomes das pessoas que concorrem na formação do documento:
- nome do autor[8]
- nome do escritor[9] **(se diferente do autor)**
- nome do originador[10] **(se diferente do nome do autor ou escritor)**
- nome do destinatário[11]
A.1.a.ii Nome da ação ou matéria
A.1.a.iii Data da criação e transmissão:

- data cronológica[12]
- data do recebimento[13]
- data da transmissão[14]
A.1.a.iv Expressões de vinculo arquivístico[15] **(ex.: código de classificação, arquivo identificador)**
A.1.a.v Identificação de anexos
A.1.b Integridade do documento:
A.1.b.i Nome da instituição, departamento ou seção responsável pelo trâmite[16]
A.1.b.ii Nome do escritório de responsabilidade primária[17] **(se diferente do previsto no item anterior)**
A.1.b.iii Indicação dos tipos de anotações adicionadas no documento[18]
A.1.b.iv Indicação de modificações técnicas[19]
A.2 Privilégios de acesso: o criador definiu e efetivamente implementou privilégios de aceso concernentes à criação, modificação, anotações, relocação e destruição do documento
A.3 Procedimento de proteção: perda e adulteração do documento
O criador estabeleceu e efetivamente implementou procedimentos para prevenir, descobrir e corrigir perda ou adulteração de documentos.
A.4 Procedimentos de proteção: meio e tecnologia empregados
O criador estabeleceu e efetivamente implementou procedimentos para garantir a contínua identidade e integridade do documento contra meio deteriorado e através de mudanças tecnológicas
A.5 Estabelecimento de formas documentais: o criador estabeleceu formas documentais do documento associadas a cada produto de acordo com requisitos do sistema jurídico ou aqueles do criador
A.6 Autenticação do documento: se a autenticação é requisito para o sistema jurídico ou necessita de organização, o criador estabeleceu rotas específicas com referências aos documentos que podem ser autenticados, para quem, e o meio de autenticação
A.7 Identificação da Autoridade do documento: se existem múltiplas cópias de alguns documentos, o criador estabeleceu procedimentos que identifiquem quais documentos são autorizados.
A.8 Remoção e transferência de documentos relevantes: se há uma transição de documentos para o status ativo, semi-ativo ou inativo, quais envolvem a remoção de documentos de um sistema eletrônico, o criador estabeleceu e eficientemente implementou procedimentos para determinar que documentos devem ser removidos e transferidos para serem preservados.

Figura 1. Fonte: *Interpares Project* (2003).

Afora os elementos essenciais do documento diplomático, os diplomatas distinguiram caracteres extrínsecos e intrínsecos, como requisitos de autenticidade visando auxiliar e garantir a sua confiabilidade. Os primeiros se referindo à aparência externa, e os segundos ao modo pelo qual se articula a representação de seu conteúdo.

Para Núñez Contreras (1981, p. 39-40, tradução nossa), Belloto (1991, p. 33) e Heredia Herrera (1988, p. 92-93, tradução nossa) os caracteres externos são representados pela matéria (suporte), meio (escrita), formato com o que se representa a escrita na matéria e os sinais gráficos especiais, distintos da escrita, tais como os selos, carimbos, letras iniciais, etc, enquanto os caracteres internos estariam representados pela língua empregada e o teor documental, que no dizer de Bellotto (1991, p. 33) "[...] é o modo de articular o discurso segundo fórmulas determinadas e uniformes segundo a tipologia do documento".

Sob o ponto de vista da estrutura da análise crítica diplomática, Duranti (1996, p. 131-132, tradução nossa) apresenta uma metodologia de trabalho que foi incorporada por Nascimento (2002, p. 127) para a análise do documento jurídico eletrônico:

Quadro – 2 Elementos de forma documental

Elementos da forma documental	Elementos diplomáticos	Caracterização e função
Externos ou extrínsecos	Suporte Escritura Linguagem Signos especiais Selos Anotações	- caráter material do documento e sua aparência externa - podem ser examinados sem ler o documento - determina a disposição e articulação do discurso - estabelecer data, proveniência e provar autenticidade - verificar grau de autoridade e solenidade - verificar modo de edição e melhoria da documentação associada a um sistema eletrônico de informação.
Internos ou intrínsecos	Protocolo e subseções Texto e subseções Escatocolo e subseções	- todos os documentos da articulação intelectual (modo de apresentação do conteúdo ou partes que determinam o teor do conjunto); - Elementos reunidos em grupos com alguma relação de subordinação uns com os outros, denominados de substrutura ideal (protocolo, texto, escatocolo); - onde se localiza a parte central do documento (texto); - contém (protocolo) o contexto administrativo da ação (pessoas incluídas, tempo, lugar e assunto), fórmulas iniciais; - contém (texto) as considerações e circunstâncias que lhe deram origem e as condições relacionadas com seu cumprimento; como também uma manifestação de vontade; comunica natureza da ação e a de função do documento; - contém (escatocolo) o contexto da documentação da ação (enuncia os meios de validação, indica a responsabilidade com relação ao ato de documentação e fórmulas finais;

		- nos documentos contemporâneos, o intitulado é usualmente seguido pela data, indicando o lugar e/ou o momento da compilação do documento e/ou da ação concernente ao documento.

Figura 2. Fonte: Nascimento (2002, p. 127).

Assim, pode-se concluir que a assinatura digital estaria inserida no contexto dos elementos externos ou extrínsecos apontados por Duranti (1996 Apud Nascimento, 2002), com o objetivo de provar a autenticidade e autoria do documento eletrônico, gerando confiabilidade.

Superada a questão da forma documental, necessário se torna analisarmos o posicionamento doutrinário no que tange à conceituação de documento eletrônico.

Em uma abordagem sobre o valor probatório do documento eletrônico, Marcacini (1999), o define como "uma seqüência de *bits* que traduzida por um programa de computador, seja representativa de um fato" (grifo nosso). Verifica-se que o autor emprega o documento eletrônico como gênero, do qual o documento digital é espécie.

Em seu manual de direito de informática, Giannantonio (1994, p. 338 apud Trujillo, 2000) conceitua documento eletrônico ou informático como "o documento produzido pelo computador eletrônico. Distinguem-se documentos eletrônicos *stricto sensu*, memorizados em forma digital e não perceptíveis ao homem se não através do computador, e documentos eletrônicos *lato sensu*, isto é, todos os documentos formados pelo computador mediante dispositivos de saída".

López Yepes (1997, p. 21-22) apresenta, tipologicamente, a seguinte classificação de documento:

a) Pela forma de representação da mensagem no suporte físico:

1. Gráfico: livro, revista, etc.

2. Iconográfico: fotografia, pintura, etc.

3. Fônico: disco, fita magnética, etc.

4. Audiovisual: filme, vídeo, etc.

5. Plásticos: objetos.

6. Eletrônico: fita de vídeo.

7. Digital: disquete, disco óptico digital, etc.

b) Por nível de difusão:

1. Publicado: qualquer documento multiplicado em número suficiente de exemplares que permitem sua difusão pública.

2. Inédito: manuscrito ou documento de arquivo não publicado.

3. Reservado: documento manuscrito ou impresso, porém não difundido.

c) Pelo grau de originalidade em sua criação:

1. Fontes: os documentos mais próximos às informações ou acontecimentos que refletem o que constitui a matéria prima: documentos de época, crônicas, estatísticas, legislação, objetos de museu, etc.

2. Bibliografia: os documentos elaborados desde as fontes: monografia, artigo de revista, etc.

d) Pelo grau de modificação da natureza da mensagem como resultado da análise documental:

1. Primário: livro, artigo de revista, etc.

2. Secundário: ficha bibliográfica, repertório bibliográfico, resumos, etc.

e) Pelo grau de transformação da mensagem documentária registrada em um documento:

1. Mensagem documentada.

2. Mensagem marginal.

3. Mensagem referencial.

4. Mensagem documental.

f) Por sua situação no âmbito do sistema das ciências: político, econômico, demográfico, religioso, etc.

g) Pelo grau de permanência da mensagem ao longo do tempo:

1. Científico: monografia científica, teses de doutorado, artigo científico, etc.

2. Não científico: artigo de imprensa, ensaio, etc.

h) Pela natureza do código ou modo tecnológico de representação da mensagem:

1. Documento analógico: vídeo.

2. Documento eletrônico: vídeo.

3. Documento digital: CD-ROM.

Para o autor, há uma clara distinção entre documento eletrônico e digital, mormente quando o pontua sob o ponto de vista do modo tecnológico de representação da mensagem.

Verifica-se que a doutrina não é pacífica quanto aos conceitos de documentos eletrônicos e digitais. Ao que parece, para López Yepes (1997), o liame que separa os conceitos está na linguagem tecnológica empregada para a representação da mensagem aposta no documento, independentemente de seu suporte. Dessa forma, a seqüência de *bits* caracterizaria o documento digital e não o eletrônico, enquanto Marcacini (1999) e Giannantonio (1994) caracterizam o documento digital como espécie do gênero documento eletrônico.

Importa salientar que, pelas ementas de projetos de lei em tramitação na Câmara dos Deputados[20] e pela legislação em vigor[21], o legislador pátrio tem demonstrado uma preferência em adotar a terminologia documento eletrônico.

Após a análise do conceito de documento eletrônico, necessário se torna abordarmos a questão da assinatura digital como sua garantia.

3 Assinatura digital: a garantia da autoria do documento eletrônico

O avanço tecnológico proporcionado pela grande rede faz com que passemos a refletir sobre a autenticidade e veracidade do documento digital.

No entanto, "podemos dizer que a autenticidade de um documento depende do grau de confiabilidade que dele se pode extrair" (Gico júnior, 2000, p. 325 Apud Nascimento, 2002, p. 96).

Nesse contexto, Nascimento (2002) aponta a assinatura como elemento diplomático intensamente relacionado à autenticidade documental.

E como conferir confiabilidade em um documento eletrônico, se ele pode ser facilmente adulterado?

A resposta pode estar na adoção da assinatura digital. Vale lembrar que não estamos falando da digitalização da própria assinatura letrada ou assinatura autógrafa, normalmente apostas em documentos como, por exemplo, nos certificados de licenciamento anual de veículos automotores expedidos pelos Departamentos de Trânsito, ou mesmo em resultados de exames médicos disponibilizados pela *Internet*, mas sim, do resultado de complexos algoritmos criptográficos que cifram os *bits*, atribuindo segurança e confiabilidade ao documento.

A criptografia, a arte de escrever em código, tão antiga quanto à própria escrita, era utilizada por Júlio César, Imperador romano, que codificava suas mensagens alterando as letras que compunham uma palavra pela terceira letra seguinte do alfabeto. Também foi largamente empregada pelos alemães

na Segunda Guerra Mundial, que fabricaram a máquina enigma, considerada a ferramenta criptográfica mais importante da Alemanha nazista. O sistema foi desvendado pelo matemático polonês Marian Rejewski, o que resultou em um passo decisivo para os aliados vencerem a guerra.

O seu emprego oferece ao documento digital requisitos para a sua autenticidade e confiabilidade, de maneira que uma transação efetuada pela *Internet* consista, de fato, em uma expressão de vontade com validade jurídica e força probante.

Segundo Devegili (2001) o emprego da criptografia pode resultar em: confiabilidade, identificação, integridade e não repúdio.

Assim, preserva-se a autoria da mensagem e sua originalidade, de maneira que ela, cifrada, não poderá ser lida por terceiros, não tendo como o remetente negar o seu envio e tampouco o destinatário alegar o não recebimento.

Dentro desse contexto e a título de exemplo, imaginemos uma compra pela *Internet*. A informação objeto do negócio deve estar disponível, de maneira que o comprador possa acessá-la a qualquer hora. O objeto do negócio não pode ser alterado após a contratação, mantendo-se íntegro. A transação deve ser restrita, privativa aos contraentes, ensejando o controle de acesso, que por sua vez, oferece às partes a absoluta certeza de quem figura em ambos os pólos contratuais, caracterizando a autenticidade. Assim, o contrato transforma-se em um instrumento com validade jurídica, podendo ser usado como prova em futura ação, de forma que não poderá ser repudiado pelas partes, contraente e contratado.

Ao abordar sobre os processos tecnológicos *lato sensu* empregados para formalizar a assinatura eletrônica, Correia (1999) elenca suas formas:

1. código secreto: consistente no emprego de um *password*, fórmula numérica ou alfanumérica de conhecimento pessoal do proprietário, que deverá ser confirmada pelo gestor de sistemas ou da base de dados do sítio acessado.

2. assinatura digitalizada: reprodução da assinatura autógrafa do autor, por meio de *scanner*.

3. assinatura digital ou criptográfica: de acordo com o sistema em que se baseia, comporta duas modalidades:

3.1 criptografia com chave privada ou simétrica: a mesma chave serve tanto para criptografar o documento como para decodificá-lo. Assim, tanto o autor como o receptor são detentores da mesma chave.

2.2 criptografia com chave pública ou assimétrica: consiste no emprego de uma chave pública, capaz de decodificar a mensagem encriptada, e uma chave privada, que a codifica.

4. chave biométrica: fundamentada no reconhecimento de características físicas da pessoa, tais como, por exemplo, as impressões digitais e as da íris.

O código secreto ou *password,* largamente utilizado em *home banking,* não vem impedindo que internautas tenham suas senhas subtraídas e utilizadas por outrem, demonstrando ser um sistema bastante vulnerável.

A assinatura digitalizada por meio de *scanner* não impede, por exemplo, que de posse de um documento original, um terceiro digitalize a assinatura de seu autor e emita um outro documento, com conteúdo diverso, contendo a assinatura copiada, demonstrando, também, ser um processo sujeito a fraudes.

No que tange à criptografia simétrica, o processo permite que uma das partes emita um documento como se fosse de autoria da outra, já que a chave para codificar e decodificar é a mesma, de forma a também não ser confiável.

O processo de chave biométrica é preciso, porém extremamente caro, face aos equipamentos de ponta utilizados e em decorrência da necessidade de se ter uma grande base de dados com padrões originais fornecidos pelas partes, para servirem de confronto. Atualmente, é utilizado por empresas de grande porte para controlar o acesso restrito de pessoas.

Assim, por ser um processo menos expendioso e eficaz, a ICP-Brasil adotou como base a criptografia assimétrica, sem, contudo, proibir "a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, podendo inclusive ser(em) utilizados certificados não emitidos pela ICP-Brasil, desde que emitidos pelas partes como válidos ou aceitos pela pessoa a quem for oposto o documento" (Copalo, 2002).

Segundo Demócrito Filho (2000) a chave pública, "de conhecimento público, é usada para verificar se a assinatura digital aposta no documento eletrônico é mesmo dele (daquele determinado usuário), ou para criptografar um documento a ser-lhe enviado". Segue o autor dizendo que a chave privada "é o elemento do par de chaves assimétricas de uso exclusivo do usuário, mediante a qual ele apõe sua assinatura digital do documento eletrônico ou decripta uma mensagem que lhe foi enviada, previamente criptografada por um terceiro que utilizou a sua (dele, usuário) chave pública".

Conclui seu raciocínio ao afirmar que, diante disso, "a autoridade certificadora, responsável pela outorga dessas chaves, emite então um certificado eletrônico, uma espécie de garantia de autenticidade dos emissores e destinatários dos documentos que trafegam na rede de comunicação".

Vale lembrar que o par de chaves criptográficas será gerado sempre pelo próprio titular perante a autoridade certificadora e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Como garantia de segurança, Devegili e Santos (2003) salientam que o sistema não deve ser utilizado em qualquer computador, apenas naquele de uso pessoal do autor do documento. Para os autores, deve-se adotar o emprego de cartões inteligentes ou *smart cards* para o armazenamento das chaves, pois, em caso de extravio ou furto, pode-se facilmente cancelá-las junto à autoridade certificadora.

A preocupação com a autenticidade, integridade e validade jurídica do documento eletrônico tem contorno transnacional.

Tanto assim que, partindo do pressuposto de uma legislação uniforme em âmbito mundial, sem desrespeitar a soberania estatal, e procurando preservar a eficácia probatória dos documentos eletrônicos, a *United Nations Commission on International Trade Law* – Unicitral, elaborou a *Model Law on Eletronic Signatures* (2001) como diretriz a ser seguida sobre a temática.

Fazendo alusão ao direito comparado, Paiva e Cuervo (2002) citam as legislações dos Estados Unidos, México, Reino Unido, Espanha, Itália e Alemanha, de forma a traçar um paralelo com o direito pátrio.

No Brasil, a MP-2.200-2, de 24 de agosto de 2001, estatuiu a ICP-Brasil com o objetivo de garantir a autenticidade, a integridade e a validade jurídi-

ca do documento eletrônico.

Basicamente, a ICP-Brasil é composta por uma autoridade gestora política, no caso, o Comitê Gestor[22], bem como pela cadeia de autoridades certificadoras, composta pela Autoridade Certificadora Raiz – AC Raiz, pelas Autoridades Certificadoras – AC, e pelas Autoridades de Registro – AR.

Segundo o artigo 4º da MP-2.200-2, de 24 de agosto de 2001, compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

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

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

O Comitê Gestor da ICP-Brasil poderá delegar atribuições a AC Raiz, cuja competência originária é de emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas, sendo-lhe vedado emitir certificados aos usuários finais.

Entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete às AC emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Por sua vez, às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Importa salientar que o Comitê Gestor da ICP-Brasil poderá estabelecer critérios para credenciar como AC e AR, os órgãos e as entidades públicas e as pessoas jurídicas de direito privado,

sendo vedado a qualquer AC certificar nível diverso do imediatamente subseqüente ao seu, exceto em hipóteses excepcionais previamente aprovadas pelo Comitê Gestor da ICP-Brasil.

4 Conclusão

A criptografia assimétrica, adotada como padrão pela ICP-Brasil parece ser o processo mais confiável para se garantir autenticidade, integridade e validade jurídica do documento eletrônico.

Porém, para que todo o processo ganhe a confiança da sociedade, necessário se torna sua efetiva implementação.

Nessa seara, o Comitê Gestor da ICP-Brasil editou várias resoluções disciplinando o funcionamento da certificação digital e o Governo Federal apresentou, em regime de prioridade, o PL-2281/2003, visando instituir taxas de credenciamento, fiscalização e manutenção de credenciamento e multas relativas às atividades de certificação digital, que merecem o devido enfrentamento pela comunidade jurídica, como forma de contribuição para a melhoria de todo o sistema.

Bibliografia

Balieiro, Silvia. *Viagem pela internet*. São Paulo: Abril. Info Exame, n. 226, jan. 2005. p. 26-27.

Bellotto, Heloisa Liberalli. *Arquivos permanentes*: *tratamento documental*. São Paulo: T.A. Queiroz, 1991, 198p. ISBN 85-7182-006-6.

Brasil. Medida Provisória n. 2.200-2 de 24 de out. de 2001. Institui a Infra-Estruta de Chaves Públicas brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Disponível em: <http://wwwt.senado.gov.br>. Acesso em 6 fev. 2005.

_____. Decreto n.º 3872, de 18 de jul. de 2001. Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas brasileira – CGICP-Brasil, sua secretaria-executiva, sua comissão técnica executiva e dá outras providências. Disponível em: <http://wwwt.senado.gov.br>. Acesso em 6 fev. 2005.

_____. Projeto de lei n.º 1589, de 31 de ago. De 1999. Dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e dá outras providências. Disponível em: <http://www3.camara.gov.br>. Acesso em: 6 fev. 2005. (Autor: Luciano Pizzatto).

_____. Projeto de lei n.º 2281, de 10 de out. de 2003. Institui a Taxa de Credenciamento – TCD, a Taxa de Fiscalização e de Manutenção de Credenciamento – TFM, as multas que especifica, e dá outras providências. Disponível em: <http://www3.camara.gov.br>. Acesso em: 6 fev. 2005. (Explicação da ementa: Criando a TCD e a TFM relativas às atividades de certificação digital) (Autor: Luciano Pizzatto).

Carrascosa López, Valentin. *La regulación jurídica del fenómeno informático*. Mérida: Revista Iberoamericana Informática y Derecho. 1998. v. 19-22. p. 33-55. ISBN 84-88861-61-3.

Chiovenda, Giuseppe. *Instituições de Direito Processual Civil*, 2ª ed. vol 3. São Paulo: Saraiva, 1965. p. 127. Apud Marcacini, Augusto Tavares Rosa.

O documento eletrônico como meio de prova. *Augusto Marcacini*, São Paulo, nov. 1999. Disponível em: http://augustomarcacini.cjb.net/index.php/DireitoInformatica/DocumentoEletronico Acessado em: 06 fev. 2005.

Correia, Miguel Pupo. Sociedade de informação e direito: a assinatura digital. *Avocati Lócus*, São Paulo, jul. 1999. Disponível em: http://www.advogado.com/cd/cd-doutri.htm. Acessado em: 26 jan. 2005.

Copalo, Edilane Del Rio. ICP-Brasil: o sistema de certificação digital brasileiro. *Infojus*, Recife, mar. 2002. Disponível em: http://www.infojus.com.br/webnews/noticia.phd?id_noticia=1337&. Acessado em: 05 fev. 2005.

Devegili, Augusto Jun. Farnel: uma proposta de protocolo criptográfico para votação digital. 2001. Dissertação (Mestrado em Ciência da Computação) – Faculdade de Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2001. Disponível em: <http://www.inf.ufsc.br/~custodio/orientacao.html>. Acesso em: 09 jan. 2002.

Devegili, Augusto Jun; Santos, Aline Sueli de Salles. Conceitos de criptografia e sua relação com o direito: segurança e autenticidade. In: Kaminski, Omar (Org.) *Internet Legal: o direito na tecnologia da informação*. Curitiba: Juruá, 2003.

Duranti, Luciana. *Diplomática: usos nuevos para una antigua ciência*. Tradução Manuel Vázques. Carmona: S & C ediciones, 1996. 170 p.

Fernández Molina, Juan Carlos. Derecho de autor y privilegios de las bibliotecas: ¿es posible su mantenimiento en un entorno electrónico? *Revista Argentina de Bibliotecología*, Buenos Aires, n. 2, 1999, p. 39-48.

Fortes, Débora. A praga de 2004. São Paulo: Abril. *Info Exame,* n. 226, jan. 2005, p. 23.

Furlaneto Neto, Mário. *Pornografia infantil na internet: elementos diplomáticos como subsídio à caracterização do delito*. Marília, 2003. 144 f. Dissertação (Mestrado em Ciência da Informação) – Faculdade de Filosofia e Ciências, Universidade Estadual Paulista. Marília, 2003.

Giannantonio, Ettore. Manuale di Diritto dell'Informatica. Padova: Ed. Cedam, 1994, p. 338 ss. Apud Trujillo, Elcio. O Mercosul e a documentação eletrônica. *Avocaci Lócus*, São Paulo, fev. 2000. Disponível em: http://www.advogado.com. Acessado em: 06 fev. 2005.

Gico júnior, Ivo Teixeira. O arquivo eletrônico como meio de prova. Repertório IOB de Jurisprudência, caderno 3, 1ª quinzena, n.15, ago. 2000, p.321-329. Apud Nascimento, Lúcia Maria Barbosa do. *A dimensão diplomática do documento jurídico digital*. Marília, 2002. 180 f. Dissertação (Mestrado em Ciência da Informação) – Faculdade de Filosofia e Ciências, Universidade Estadual Paulista. Marília, 2002.

Guimarães, José Augusto Chaves. O caráter instrumental da Diplomática para o tratamento temático de documentos na área jurídica. *Cadernos da Faculdade de Filosofia e Ciências*, Marília, v. 7, n.1/2, p. 97-106. 1998.

Heredia Herrera, Antonia. *Archivísti-*

ca general: teoría y práctica. Sevilla : Diputación Provincial, 1988. p. 35-105.

Interpares Project. Internacional Research on Permanent Authentic Records in Eletronic Systems. The long-term preservation of authentic electronic records: findings of the InterPARES Project. Disponível em: <http://www.interpares.org/book/index.htm>. Acessado em: 18 jan. 2003.

_____. Requirements for assessing and maintaining the authenticity of electronic records. March, 2002. Disponível em: <http://www.interpares.org/book/index.htm>. Acessado em: 18 jan. 2003b.

Lèvy, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999. 260 p.

Lòpes yepes, José. Reflexiones sobre el concepto de documento ante la revolución de la información: ¿un nuevo profesional del documento? *Scire,* v.3, n.1, p.11-29, ene./jun. 1997.

Marcacini, Augusto Tavares Rosa. O documento eletrônico como meio de prova. Augusto Marcacini, São Paulo, nov. 1999. Disponível em: http://augustomarcacini.cjb.net/index.php/DireitoInformatica/DocumentoEletronico. Acessado em: 06 fev. 2005.

Nascimento, Lúcia Maria Barbosa do. *A dimensão diplomática do documento jurídico digital*. Marília, 2002. 180 f. Dissertação (Mestrado em Ciência da Informação) – Faculdade de Filosofia e Ciências, Universidade Estadual Paulista. Marília, 2002.

NÚÑEZ contreras, Luis. Concepto de documento. In: *Archivistica: estúdios básicos*. Sevilla: Diputación Provincial, 1981. p. 25-44.

Paiva, Mário Antônio Lobato de; Cuervo, José. A firma digital e entidades de certificação. *Jus Navigandi,* Teresina, a. 6, n. 57, jul. 2002. Disponível em: http://www1.jus.com.br/doutrina/texto.asp?id=2945. Acessado em: 05 fev. 2005.

Reinaldo filho, Demócrito. A certificação de documentos eletrônicos. *Infojus*, Recife, mai. 2000. Disponível em: http://www.infojus.com.br/webnews/noticia.phd?id_noticia=541&. Acessado em: 05 fev. 2005.

Sola, José Eduardo Martins. *A proteção dos direitos autorais a partir da realidade Internet: a perspectiva brasileira*. Marília, 2002. 172 f. Dissertação (Mestrado em Ciência da Informação) - Faculdade de Filosofia e Ciências - Universidade Estadual Paulista, 2002.

Sposito, Rosa. O e-commerce desencantou. São Paulo: Abril. *Info Exame,* n. 226, jan. 2005. p. 54-59.

Uncitral. United Nations Commission on International Trade Law. *United Nations*, Vienna, jul. 2001. Disponível em: <**http://www.uncitral.org**>. Acesso em: 07 jan. 2002.

Notas

[1] O presente artigo surgiu no decorrer das discussões do NEPI – Núcleo de Estudos, Pesquisas, Integração e Práticas Interativas do UNIVEM – Centro Universitário Eurípides de Marília, mantido pela Fundação de Ensino "Eurípides Soares da Rocha".

[2] Delegado de Polícia, Mestre em Ciência da Informação pela UNESP de Marília, Professor de Processo Penal do UNIVEM, membro e pesqui-

sador do NEPI. E-mail: mariofur@flash.tv.br.

[3] Graduando em Direito no UNIVEM e membro do NEPI. E-mail: gbellinetti@ig.com.br.

[4] Levy (1999) salienta ser o Ciberespaço o resultado da interconexão mundial de redes de computadores, não caracterizado apenas pela infra-estrutura, mas também pelas informações e as relações humanas que o alimentam.

[5] O presente item foi extraído e adaptado de Furlaneto Neto (2003) que, inclusive, abordou critérios de confiabilidade do conteúdo da informação de uma página *web*.

[6] Heredia Herrera (1988, p. 36-37, tradução nossa) define Diplomática como a "ciência que estuda o documento, sua estrutura, suas cláusulas, para estabelecer as diferenças tipológicas e suas gênesis dentro das instituições escriturarias, com o fim de analisar sua autenticidade".

[7] A interdisciplinaridade entre a Ciência da Informação e o Direito, por meio da interface com a Diplomática, está consubstanciada no dogma constitucional do direito ao acesso à informação, se consolidando quando conceitos comuns são discutidos por ambas as áreas, como, por exemplo, o Direito do Autor de um documento ou de uma obra científica ou literária, estudados por pesquisadores como Fernández Molina (1999), na Espanha, e por Sola (2002), no Brasil, ou o caráter instrumental da Diplomática para o tratamento temático de documentos na área jurídica (GUIMARÃES, 1998), ou ainda, em pesquisas como a dimensão diplomática do documento jurídico digital (NASCIMENTO, 2002) e os elementos diplomáticos como subsídio à caracterização da autoria do delito de pornografia infantil na *Internet* (FURLANETO NETO, 2003).

[8] O nome da pessoa física ou jurídica que tenha a autoridade e capacidade de editar o documento ou em cujo nome ou cujo comando o documento foi editado.

[9] O nome da pessoa física ou jurídica que tenha autoridade e capacidade para articular o conteúdo do documento.

[10] O nome da pessoa física ou jurídica que aponta o endereço eletrônico em que o documento foi gerado e/ou transmitido.

[11] O nome da pessoa física ou jurídica para quem o documento é direcionado ou pretendido.

[12] A data e horário possível de compilação de um documento incluído pelo autor ou pelo sistema eletrônico no interesse do autor.

[13] A data e o horário possível que o documento é transmitido para o interessado.

[14] A data e horário em que o documento ingressa no espaço em que foi gerado.

[15] O arquivo vinculado é a relação que liga cada documento, desenvolvimento, para o anterior e subseqüente e todos aqueles que participam de alguma atividade. Ele é originário (ex., ele vem a existir quando um documento é feito ou transmitido e desprezado), necessário (ex., ele existe para todo documento) e determinado (ex., ele é caracterizado pela proposta do documento).

[16] O escritório (ou cartorário) formalmente competente para exteriorizar a ação relatada pelo documento ou pela matéria à qual o documento pertence.

[17] O escritório (ou cartorário) formalmente competente para a manutenção da autoridade do documento, que é o documento criado pelo criador para ser o oficial.

[18] Anotações são adições feitas em um documento após ele estar completo. Por essa razão, não são considerados elementos da forma documentária do documento.

[19] Modificações técnicas são quaisquer mudanças nos componentes digitais do documento como definido pelo *Preservation Task Force*. Desta maneira, modificações incluirão quaisquer alterações no estilo de quaisquer elementos do documento digitais além de mudanças nos métodos (softwares) aplicados para reproduzir o documento para o estoque de componentes digitais; Que é, quaisquer mudanças que podem elevar questões como o documento produzido é como teria sido antes da modificação técnica. A indicação de modificações pode referir a documentos adicionais externos para o documento que explicar mais detalhes da natureza dessas modificações.

[20] Vide, a título de exemplo, o PL 1589/1999, que dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, bem como a exposição de motivos do PL 2281/2003 que prevê a instituição de taxa de Credenciamento, Fiscalização e Manutenção de Credenciamento, bem como multas relativas às atividades de certificação digital.

[21] Vide Medida Provisória nº 2.200-2/2001 que instituiu a chamada Infra-Estrutura de Chaves Públicas Brasileira e a exposição de motivos

[22] O Comitê Gestor da ICP-Brasil foi regulamentado pelo Decreto nº 3.872, de 18 de julho de 2001.