

DOCUMENTO ELETRÔNICO

ADVERTÊNCIA

Este trabalho resulta de observações próprias do autor em relação à matéria, não refletindo necessariamente a opinião do Colégio Notarial do Brasil.

Foram adotados como espinha dorsal da exposição dois excelentes conjuntos de estudos sobre a matéria. Na área técnica, artigos publicados pelo Professor de Ciência de Computação da Universidade de Brasília, **Dr. Pedro Antonio Dourado de Rezende**. Na área jurídica, artigos de autoria do Professor de Direito Processual da Universidade de São Paulo, **Dr. Augusto Tavares Rosa Marcacini**.

A tais profissionais, nossos sinceros agradecimentos pelos valiosos subsídios.

Por outro lado, procuramos trazer a explicação de alguns conceitos que certamente para a maioria já serão conhecidos, mas que eventualmente poderia ser importante para aqueles que estão iniciando seu relacionamento com o documento eletrônico e a assinatura digital. A estes colegas, minhas desculpas antecipadas.

O DOCUMENTO

Documento é o registro de um fato (*documentum*, do verbo *docere*, ensinar, mostrar, indicar).

Documento é qualquer base de conhecimento, fixada materialmente e disposta de maneira que se possa utilizar para consulta, estudo, prova, etc. (Dicionário Aurélio da Língua Portuguesa).

A característica de um documento é a possibilidade de ser futuramente observado (o documento narra, para o futuro, um fato ou pensamento presente).

Como veremos, quase todas as definições de documento levam em consideração o fato de ser o documento uma coisa, material e tangível, escrita ou lançada em algum meio físico.

O Prof. Marcacini resgata em um de seus trabalhos algumas definições clássicas de documento.

Documento, em sentido amplo, é toda representação material destinada a reproduzir determinada manifestação do pensamento, como uma voz fixada duradouramente (Chiovenda).

O documento, como meio de prova, é toda coisa em que se expressa por meio de sinais, o pensamento (Pontes de Miranda).

Documento é a prova histórica real consistente na representação física de um fato. O elemento de convicção decorre, assim, na prova documental, da representação exterior e concreta do *factum probandum* em alguma coisa (José Frederico Marques).

Documento é a coisa representativa de um fato e destinada a fixá-lo de modo permanente e idôneo, reproduzindo-o em juízo (Moacyr Amaral Santos).

O DOCUMENTO ELETRÔNICO

Em palestra proferida em Viena, em junho último, no Seminário sobre Documento Eletrônico organizado pelo notariado austríaco, o Prof. Nicholas Negroponte estabeleceu um paralelo significativo entre o mundo a que estamos habituados,

povoado de átomos, e um novo mundo virtual a que nos devemos habituar, onde convivem **átomos** e **bits**. Olhado ao microscópio, o documento em papel é uma infinidade de átomos, formando uma coisa que, captada pelos nossos sentidos, nos transmite uma informação. Já o documento eletrônico é uma seqüência de bits que, captada pelos nossos sentidos com o uso de um computador e de um programa específico, também nos transmite uma informação.

Como se sabe, o computador processa as informações em forma numérica. Ou seja, texto, imagens, sons, são transformados em números para serem processados pelo computador. Assim, o documento eletrônico constitui-se em uma seqüência de números, o que permite considerá-lo como variável numa operação matemática que tem como resultado um outro número: **a assinatura digital**.

O documento eletrônico é uma seqüência de bits que, traduzida por meio de um determinado programa de computador, seja representativa de um fato (Augusto Marcacini).

O documento físico pode estar representado por um original e diversas cópias.

O documento eletrônico, ao contrário, caracteriza-se por ser dissociado do meio em que foi originalmente armazenado. Assim um texto (uma seqüência de bits) gerado em um disquete pode ser armazenado no disco rígido de um computador, ou em um CD, que o documento eletrônico continuará sendo o mesmo original.

A PROVA

Prova é tudo aquilo que atesta a veracidade ou a autenticidade de alguma coisa (Dicionário Aurélio da Língua Portuguesa).

Em Direito, a prova é a atividade realizada no processo com o fim de ministrar ao órgão judicial os elementos de convicção necessários ao julgamento (Idem).

O Código de Processo Civil Brasileiro admite que *todos os meios legais, bem como os moralmente legítimos ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa* (art. 332).

Com base nesse amplo preceito, alguns juristas sustentam não ser necessária a aprovação de uma lei específica para que o documento eletrônico seja admitido como meio de prova pelos tribunais brasileiros. No entanto, mesmo esses reconhecem a conveniência de existir uma lei sobre o assunto, que chame a atenção dos operadores do direito para um tema que é novo.

O DOCUMENTO ELETRÔNICO E A PROVA

Para servir como prova, o documento eletrônico deve ter asseguradas a **autenticidade** (autoria identificável), a **integridade** (impossibilidade de ser alterado de forma imperceptível) e a **irretratabilidade** (irrevogabilidade da transação eletrônica).

A criptografia assimétrica é hoje o único método seguro conhecido que permite assinar o documento eletrônico e assegurar sua integridade posterior.

A CRIPTOGRAFIA

Criptografar = encriptar = cifrar.

Decriptar = decifrar.

A técnica da criptografia permite tornar incompreensível o texto de uma mensagem, com observância de normas especiais consignadas numa cifra ou num código (cripto = oculto).

A criptografia pode ser **simétrica** ou **assimétrica**.

A **criptografia simétrica** ou convencional utiliza a mesma chave tanto para cifrar como para decifrar a mensagem. Conhecida a chave utilizada para cifrar a mensagem, esta poderá ser decifrada. Método clássico de criptografia simétrica é aquele que usado por Júlio César e que consistia em escrever as mensagens utilizando-se das três letras sucessivas e posteriores do alfabeto (A = D; B = E, etc.).

A **criptografia assimétrica** foi criada em 1976. A partir de 1994, passou a ser divulgada pela Internet como o programa *Pretty Good Privacy* (PGP), que pode ser obtido gratuitamente, para uso não comercial, na *home page* do PGP Internacional (www.dca.fee.unicamp.br/pgp). O uso comercial do PGP está hoje condicionado ao licenciamento por parte de sua atual proprietária, a Network Associates.

A criptografia assimétrica utiliza duas chaves: a chave pública (*public key*), que consta do banco de dados de quem a forneceu (*key repository*) e fica responsável por sua livre distribuição; e a chave privada (*private key*), a ser mantida em sigilo pelo usuário, sob sua responsabilidade e em seu exclusivo poder.

Os números de uma chave pública e de uma chave privada são relacionados entre si de tal forma que uma chave desfaz o que a outra faz. Assim, encriptando uma mensagem com a chave pública, somente com uma única chave privada poderemos decifrá-la. A recíproca é verdadeira: o que for encriptado com

uma chave privada somente poderá ser decifrado com uma única chave pública.

Não é possível conhecer a chave privada de uma pessoa a partir de sua assinatura digital ou do conhecimento da sua chave pública.

O programa denominado PGP exige que o usuário digite ainda uma senha escolhida por ele, além da chave privada, como proteção adicional.

Evidentemente, sendo a criptografia um método matemático de chegar a algum resultado numérico complexo, existem diferentes métodos e fórmulas usados para estabelecer o grau de segurança que a parte entende ser necessário. No entanto, sistemas com as características essenciais para gerar assinaturas, chamados algoritmos de criptografia assimétrica, são raríssimos. São constituídos de grandes conjuntos de pares de chaves criptográficas e as duas funções de cifragem. Se cada chave sempre inverter a operação de seu par, uma chave pública pode ser também usada para estabelecer comunicações sigilosas com seu titular. Dentre os algoritmos assimétricos conhecidos, apenas quatro são hoje satisfatoriamente seguros, todos eles descobertos no final da década de 70: o RSA, o ECC, o DSA e o Meta-ElGamal. A partir de 20 de setembro último, expirou o prazo de validade da patente do RSA nos Estados Unidos.

Em 1997, o Instituto Nacional de Padrões e Tecnologia (NIST) do governo americano abriu uma concorrência para que pesquisadores do mundo inteiro apresentassem propostas de criação de novos padrões de criptografia. Equipe liderada por Paulo Barreto, formado em Física pela Universidade de São Paulo (USP) e criptógrafo-chefe da Scopus, empresa de informática ligada ao Bradesco, composta dos pesquisadores belgas Joan Daemene e Vicent Rijmen, da Universidade de Leuven, mais o australiano Raif

Naffah, foi uma das que entraram no páreo inicial. Na segunda fase, em 1998, as equipes já estavam reduzidas a 15, de 12 países. Finalmente, em 2 de outubro deste ano, o Departamento de Comércio dos Estados Unidos anunciou o resultado favorável à equipe liderada por Paulo Barreto, que apresentou o algoritmo *Rijndael* (iniciais de Rijem e Daemene), a ser usado como padrão de criptografia pelo governo americano em todas as aplicações financeiras e contratuais que fizer pela Internet. O brasileiro ficou responsável pelo desenvolvimento, testes e otimização do novo código criptográfico AES (Advanced Encryption Standard) que irá substituir o DES (Data Encryption Standard), padrão usado nos últimos 25 anos e vigente até outubro último (Fonte: Elis Monteiro, in Caderno de Informática do Jornal do Brasil, outubro/00, pág. 4).

É preciso que se diga que, embora seja uma tecnologia altamente sofisticada, a criptografia pode resultar extremamente acessível a quem possua um computador 486, com programação de fonte aberta, como o programa Linux, no qual poderão ser instalados outros programas específicos livres, como o Open-SSL, ou o Gnu-PG, que permitem a geração de chaves, certificados e assinaturas digitais de diferentes formatos.

A ASSINATURA DIGITAL

O uso da criptografia assimétrica permitiu gerar assinaturas pessoais em documentos eletrônicos com a chave privada, sendo tal assinatura conferida com o uso da chave pública (mas, não é possível gerar uma assinatura com a chave pública).

A assinatura digital assim produzida fica vinculada ao documento eletrônico de que é parte, de tal forma que

- se houver a menor alteração no documento - a assinatura se torna inválida.

A **assinatura digital** é o resultado de uma complexa operação matemática tendo como variáveis o texto do documento eletrônico e a exclusiva chave privada do signatário. Assim, a assinatura de uma mesma pessoa será diferente para cada documento assinado, o que evita que uma mesma assinatura possa ser utilizada para outros documentos.

Como se disse, a criptografia de chave pública é hoje o único método seguro conhecido para impedir a alteração unilateral do documento eletrônico, permitindo conferir sua autenticidade.

A verificação da autenticidade da assinatura digital não é feita por inspeção visual, como estamos habituados a fazê-lo em relação à assinatura convencional aposta em papel.

O método de verificação da autenticidade e integridade do documento eletrônico consiste em aplicar ao documento o valor numérico da chave pública, para inverter o cálculo feito por ocasião da aposição da assinatura digital nesse mesmo documento. O resultado deverá produzir a seqüência binária exata contida no documento e representada pelo seu texto mais a chave privada de seu autor.

A chave pública não é um programa, mas uma seqüência aleatória de bits que permite a inversão das operações feitas pela aposição da chave privada ao documento eletrônico.

Na prática, o procedimento é o seguinte: João grava no seu computador o texto da mensagem (*plain text*) que deseja transmitir e aplica sua chave privada, cifrando a mensagem (*chipertext*); a mensagem é remetida a Pedro, que busca a chave pública de João e a aplica à mensagem recebida. Se o resultado acusado for positivo, significa que a mensagem provém de João

(imputação ou autoria), que a mensagem não sofreu qualquer adulteração (integridade) e que João não poderá sustentar que não enviou a mensagem (não repúdio).

A INTEGRIDADE DO DOCUMENTO ELETRÔNICO

Como se viu, o documento eletrônico consiste numa seqüência de bits e não está preso a qualquer meio físico. Logo, qualquer documento eletrônico é facilmente alterável, sem deixar vestígio físico, mesmo em relação à data e a hora de salvamento dos arquivos.

Programas conhecidos como **editores hexadecimais** podem alterar qualquer byte de qualquer arquivo eletrônico.

A assinatura digital do documento eletrônico por meio de chave assimétrica permite que o programa de computador acuse qualquer adulteração no teor original do documento, mesmo que seja a adição de um simples espaço entre duas palavras. Nesse sentido, o documento em papel é mais frágil que o documento eletrônico, pois necessita de um exame pericial para a constatação de eventual adulteração.

A AUTENTICIDADE DA CHAVE PÚBLICA

A criptografia assimétrica constitui-se hoje na única técnica conhecida como segura para viabilizar a contratação à distância, via internet. Como se viu, essa técnica exige que as partes conheçam a chave pública dos signatários do documento, para permitir a encriptação e a decryptação da mensagem.

O titular cria sua própria **chave pública**. A quantidade de números irá definir o tamanho da chave e a dificuldade para quebrar sua segurança. A partir de um certo número de caracteres, a segurança passa a ser absoluta, levando em conta a capacidade operacional dos computadores até agora em uso.

A autenticidade da chave pública significa ter a certeza de que ela provém de seu titular. Como fazer, então, para evitar que uma pessoa gere um par de chaves, atribuindo-lhe o nome de outrem (existente ou imaginário), criando uma chave pública não autêntica?

A prova da autenticidade da chave pública necessita ser feita mediante a apresentação de um **certificado de autenticidade** outorgado por um terceiro a quem seja atribuída fé pública para fazê-lo (*Certification Authorities - CA*).

Em todos os países que já possuem legislação a respeito, foi estabelecido que algumas pessoas assumam a função de **autoridade certificadora** da chave pública, mediante a adoção de critérios especiais de qualificação para permitir o trabalho de tais pessoas físicas ou jurídicas.

Algumas legislações inclinam-se por dar a esses certificadores um caráter oficial e público, exercido com independência por um terceiro (*Thrusted Third Party - TTP*) que possa gozar da confiança das partes que contratem eletronicamente e que tenham a necessidade de obter o par de chaves para aposição da assinatura digital. Esse papel seria exercido pelo notário (*cibernotary*).

Para certificar a chave pública, o agente autorizado identifica adequadamente o interessado, colhendo sua assinatura em documento próprio, no qual conste as características da chave pública apresentada (*key ID, fingerprints* e o tamanho da chave). Tais elementos são arquivados, em sua representação

gráfica, servindo para futura conferência, em caso de contestação da chave pública apresentada.

Key ID é um número identificador da chave pública, com 32 bits (cerca de 10 algarismos em base decimal).

Fingerprint (impressão digital) é uma espécie de resumo da chave pública, consistindo em um número de 128 bits (cerca de 40 algarismos em base decimal), escrito em base hexadecimal, formando um número que - pelo tamanho - é estatisticamente único.

É conveniente o registro do tamanho da chave porque, embora seja estatisticamente impossível que o uso normal do PGP gere duas chaves que tenham as mesmas *fingerprints*, é possível fazê-lo de modo proposital. Entretanto, neste caso, as chaves com as mesmas *fingerprints* não terão o mesmo número de bits.

A AUTENTICIDADE DA CHAVE PRIVADA

Também a **chave privada** é criada pelo próprio titular, como a chave pública. Esta chave é uma cadeia de bits aparentemente aleatórios (em geral 1.024 bits), usada para produzir a assinatura eletrônica, através de operação matemática de exponenciação modular, onde esses bits se misturam aos do documento. O resultado da mistura é um padrão binário único para cada documento, que será sua assinatura. Assim, poderíamos simplificar dizendo que a assinatura é o resultado da soma da chave privada com o próprio documento (**chave privada + documento = assinatura**).

A separação dos bits da chave e do documento, em uma assinatura, é praticamente impossível, não havendo hoje computador que possa realizar tal operação. No entanto, os bits

do documento podem ser recuperados com a aplicação da chave pública, que irá reverter a operação feita com a chave privada. Assim, poderíamos novamente simplificar dizendo que o documento é o resultado da soma da chave pública com o própria assinatura (**chave pública + assinatura = documento**).

Como se vê, a chave privada é o fator mais importante da equação. Por isso, o titular da chave privada deve tomar as cautelas necessárias para guardá-la, evitando que a mesma não seja utilizada por outra pessoa. Qualquer pessoa que conheça uma chave privada poderá fraudar uma assinatura eletrônica de forma perfeita, sem deixar vestígios.

Em geral, a chave privada encontra-se armazenada no disco rígido do computador de seu titular. Infelizmente, existem hoje em circulação na rede internet vários programas que podem ser infiltrados no computador por meio de mensagens recebidas pelo correio eletrônico. Esses programas embusteiros (*back doors*) chegam ao computador da vítima através de programas dissimuladores (*cavalo de tróia*), que podem desaparecer sem deixar vestígios, depois do ataque.

Por outro lado, o titular da chave privada pode ser coagido a fornecê-la a terceiro, da mesma forma que, no mundo do papel, alguém pode ser coagido a preencher um cheque ou assinar um documento. Esse terceiro utilizará a chave pública como se fosse seu próprio titular, sem qualquer possibilidade de desconfiança da parte contrária.

Assim, a utilização indevida da chave privada é o único risco para a segurança do sistema de chaves assimétricas. A eventual negligência em manter segura a chave privada é responsabilidade única de seu titular.

A criptografia não pode gerar confiança absoluta. Para proteger nossa chave privada, teremos que confiar

no programa que faz a intermediação entre o usuário e o computador, permitindo o acesso a ela.

A CERTIFICAÇÃO

Empresas comerciais denominadas **Autoridades Certificadoras** (CA), valendo-se de programas voltados para uso na rede internet (*browsers*), oferecem uma infra-estrutura global para o uso de chaves criptográficas assimétricas, denominada PKI (*Public Key Infrastructure*). No caso dos *browsers*, o processo obedece aos padrões adotados pelo protocolo de segurança neles implementado, denominado *SSL* (*Secure Sockets Layer*), já adaptado ao TCP/IP como TSL.

Ao pedir um certificado ao *browser*, o usuário gera um par de chaves assimétricas. A chave privada é armazenada no disco do computador do usuário. A chave pública será submetida à certificação pela Autoridade Certificadora escolhida, juntamente com os dados do titular, sendo devolvido ao *browser* um certificado expedido e assinado pela Autoridade Certificadora. O certificado assinado faz com que o *browser* implemente o protocolo de segurança SSL.

O certificado é um conjunto de números, letras e sinais gráficos, sem qualquer relação com a identificação pessoal do usuário.

Uma pessoa pode cadastrar diversas chaves públicas na Autoridade Certificadora. As Autoridades Certificadoras deveriam verificar a identidade civil do titular dos certificados que assina, mas na prática procuram eximir-se dessa responsabilidade, divulgando declarações a respeito dos direitos e obrigações recíprocos, nas páginas onde vendem tais serviços. É o caso, por exemplo, da Verisign, nos Estados Unidos,

e o da Certisign, no Brasil, que delegam essa responsabilidade aos serviços notariais e de registro.

A EVOLUÇÃO DA LEGISLAÇÃO

Uma breve passagem pela legislação hoje em vigor nos demais países nos dará o seguinte panorama.

ESTADOS UNIDOS

Como se sabe, nos Estados Unidos os estados membros podem legislar sobre matéria comercial. Assim, em 1995 foi editada a primeira lei regulamentando o uso da assinatura eletrônica, no Estado de Utah (USA). Detalhista, essa lei estabeleceu 37 definições e conceitos que se tornaram clássicos nas discussões posteriores sobre a matéria. É uma lei que iria iniciar o chamado **modelo prescritivo**, que regula o uso da assinatura digital e o funcionamento de PKIs.

Logo em seguida, ainda em 1995, a Califórnia editou uma legislação voltada para o uso opcional da assinatura digital em documentos apresentados aos órgãos públicos, com os mesmos efeitos de uma assinatura manual. Seria o chamado **modelo de critérios**, estabelecendo parâmetros de funcionalidade e confiabilidade para o reconhecimento legal de mecanismos eletrônicos autenticatórios.

Finalmente, legislações como a de Massachussets, adotaram o **modelo de outorga**, preferindo não abordar critérios ou mecanismos, mas delegar às partes envolvidas o poder de decidir qual mecanismo pode substituir eletronicamente a assinatura do próprio punho.

Hoje, 36 dos 50 Estados americanos possuem alguma legislação a respeito da assinatura digital.

Recentemente, duas leis federais foram aprovadas: o *Digital Millennium Commerce Act - DMCA* e o *e-Sign*, que se sobrepõem às leis estaduais até que estes uniformizem suas leis sobre autenticação eletrônica. Ambas seguem o modelo de outorga, deixando que as forças de mercado escolham a tecnologia mais adequada para a autenticação eletrônica. Além destas, encontra-se em tramitação nos Estados projetos de lei que procuram unificar as leis estaduais sobre o comércio eletrônico (UCITA), especialmente para a proteção dos produtores de programas de computador (*software*) em relação aos direitos dos consumidores, permitindo àqueles a adoção de um sistema de implosão remota de tais programas, quando houver suspeita de infração ao contrato, por parte do licenciado.

CANADÁ

Em junho de 1996, a Câmara de Notários de Quebec formou uma empresa sem finalidade lucrativa denominada *Notarius* para conceber, desenvolver e administrar projetos de implantação de novas tecnologias da informação para os serviços notariais de Quebec, contando com 3.200 profissionais.

Com esse objetivo, idealizou e executa um Plano de Integração Tecnológica da Profissão destinado ao intercâmbio de maneira segura dos documentos eletrônicos entre seus associados, com acesso mais rápido via rede *intranet* aos bancos de dados de interesse do notariado. Esse plano é bastante ambicioso, tendo sido adotado como padrão pela maioria dos países que professa o notariado do tipo latino.

O funcionamento é relativamente simples. O notário associado solicita à Câmara de Notários de Quebec uma assinatura numérica, que é emitida em colaboração com a *Notarius*. Essa assinatura numérica, baseada em uma infraestrutura de chaves públicas, permitirá certificar a identidade e a assinatura dos notários e de outras entidades ligadas à profissão notarial; assegurar a integridade das mensagens eletrônicas; preservar a confidencialidade das informações em suporte informático; e assegurar o não-repúdio das transações eletrônicas. É usada a tecnologia de assinatura numérica *Entrust*, através da qual o notário, mesmo sem conhecer o funcionamento técnico, pode clicar sobre determinados ícones para assinar, codificar ou verificar, por exemplo.

O projeto prevê a troca de informações com o Registro da Propriedade e o Arquivo Central de Testamentos, além do acesso a outros registros públicos e privados.

O funcionamento da assinatura numérica se dá a partir do processo de criptografia assimétrica. O *software* da *Entrust* atribui ao notário dois pares de chaves: um para **codificação**, que serve para assegurar a confidencialidade dos documentos transmitidos por via eletrônica; e outro para **assinatura**, que serve para assinar o documento e verificar sua integridade. Cada um desses pares de chaves está composto por uma *chave pública* depositada em um cadastro acessível a qualquer pessoa autorizada, e por uma *chave privada*, conhecida apenas por seu titular.

O notário associado paga uma taxa a *Notarius* pela admissão na rede, correspondente à licença de uso do *software Entrust* e aos gastos de suporte do sistema, inclusive transmissão dos dados.

Ao receber o código de autorização da entrada na rede, o notário é instruído sobre as normas de segurança que deve observar. O primeiro código de ativação é entregue pessoalmente ao notário, e o segundo é transmitido por meio diferente (correio eletrônico ou convencional), de tal forma que os códigos não sejam conhecidos por uma mesma pessoa, além do notário interessado. Durante a ativação, os dois códigos são utilizados pelo notário para gerar sua assinatura numérica, momento em que escolhe uma contrasenha *Entrust* como porta de acesso a sua assinatura numérica. Sendo a escolha dessa senha de acesso o momento mais delicado da operação, foram estabelecidas algumas regras para a criação da senha, que deverá conter no mínimo 8 caracteres, sendo no mínimo um especial, um maiúsculo e um minúsculo. Ao ativar o sistema, o notário deve ter cuidado especial, pois qualquer pessoa que utilize seu equipamento poderá usar a assinatura numérica do notário. Assim, é importante que o notário saia do sistema sempre que não for utilizá-lo, havendo dispositivo de proteção que fecha o programa automaticamente, após um tempo de inatividade. Em caso de esquecimento da senha pelo usuário ou suspeita de que a mesma é conhecida de pessoa não autorizada, feita a comunicação ao sistema *Entrust*, a senha antiga é imediatamente revogada, devendo ser criada uma nova senha pelo usuário.

MÉXICO

Participando junto com a França de um acordo de cooperação técnica com o Canadá, está desenvolvendo uma *Red de Certificación Notarial*, para agir como autoridade certificadora para seus associados, nos termos de lei aprovada em maio do corrente ano. A Associação Nacional dos Notários, de livre

inscrição, possui cerca de 2.000 participantes, dentre os 3.000 existentes no país. Destes, trabalham no Distrito Federal 240 notários, para uma população de 10 milhões de habitantes. Os notários entregarão aos usuários cartões magnéticos contendo a assinatura eletrônica dos mesmos, devidamente certificadas. O sistema de certificação notarial mexicano pode ser encontrado em www.acertia.com.

ARGENTINA

Não possuindo ainda lei federal que regulamente a matéria, mas tendo uma organização notarial muito bem estruturada, 2.446 dos 4.800 notários argentinos já estavam interligados entre si no início deste ano, em sistema denominado *Rede Eletrônica Notarial*, criado para o intercâmbio de informações técnicas entre seus participantes. A exemplo do Canadá, com o desenvolvimento do sistema e o advento de lei regulamentando o documento eletrônico, está prevista a interligação da rede notarial com a rede pública, para efeitos fiscais e de registro da propriedade. O Colégio Notarial trabalha no sentido de ser participante institucional na emissão do certificado da chave pública.

EUROPA

Os países pertencentes à União Européia possuem desde 13 de março de 1998 uma diretiva do Parlamento Europeu e do Conselho a respeito do documento eletrônico.

A maioria desses países já adaptou sua legislação interna a tal diretiva, sendo os mais recentes Portugal

(agosto de 1999), Espanha (dezembro de 1999) e França (fevereiro de 2000).

Enquanto a França optou por reconhecer apenas o valor como prova do documento eletrônico, modificando dispositivos de seu Código Civil, os demais países aprovaram extensa legislação regulando a matéria de forma exaustiva no âmbito das relações privadas e da administração pública.

Embora a atividade de certificação de assinaturas digitais não dependa de autorização administrativa prévia, de acordo com a diretiva do Parlamento Europeu e do Conselho, é certo que alguns dos Estados membros têm estabelecido um organismo de controle das condições de idoneidade e segurança das entidades certificadoras, como fez a Itália, por exemplo.

Nessas legislações, a figura do notário aparece como participante do sistema voluntário de credenciação, como qualquer particular, sujeitando-se obviamente ao controle do Estado, mencionado acima.

Na Holanda, a Real Associação dos Notários da Civil Law criou uma empresa denominada *DigiNotar*, que oferece aos profissionais associados a tecnologia, a infraestrutura e a segurança necessárias para que possam fazer certificações digitais em todo o país. O notário holandês verifica a identidade e a capacidade do solicitante, emitindo uma declaração digital a respeito do usuário.

Na Alemanha, a entidade nacional dos notários estimou em um milhão de dólares a necessidade de capital a ser investida pelo notariado daquele país para a montagem de uma rede federal de certificação, que será implantada proximamente.

ITÁLIA

Na Itália, a primeira norma reconhecendo a validade do documento eletrônico data de 15 de março de 1997, enquanto a legislação de 10 de novembro de 1997 e de 08 de fevereiro de 1999 regulamentou o uso da assinatura digital.

O sistema adotado pela Itália exige a utilização de chave pública assimétrica, com tecnologia escolhida entre o tipo *RSA (Rivest - Shamer - Adleman Algorithm)* e o tipo *DSA (Digital Signature Algorithm)*. A certificação das chaves públicas somente pode ser feita por sociedades constituídas por ações, devidamente inscritas no registro próprio que foi criado, denominado *Autorità per l'Informatica nella Pubblica Amministrazione*.

No que se refere à validade do documento eletrônico, a legislação italiana estabelece as seguintes regras: a) - o documento eletrônico não subscrito com uma firma digital tem a mesma eficácia limitada das reproduções mecânicas, ou seja, só fazem prova se a outra parte não o repudiar; b) - o documento eletrônico subscrito com uma firma digital tem a mesma eficácia probatória do instrumento particular, podendo ser contestado pelo incidente processual de falsidade; c) - a firma digital do documento eletrônico autenticada pelo notário torna a subscrição legalmente reconhecida, embora também possa ser contestada pelo incidente de falsidade, somente com base na preterição das cautelas determinadas pela lei para tal certificação.

ÁUSTRIA

Em recente *Simpósio Internacional sobre o Documento Eletrônico*, realizado em Viena, o Colégio Notarial da Áustria mostrou os resultados de parceria que fez com o Banco da Áustria e a Siemens, constituindo uma empresa denominada *Cyber Doc GmbH*, que está desenvolvendo aplicativos de transmissão de dados voltados em especial para a área da certificação eletrônica notarial. A característica especial de tal projeto é que, por envolver o Banco oficial da Áustria, repartições e empresas públicas estão participando da implantação do mesmo. Assim, agentes arrecadadores de nível local e nacional teriam seus bancos de dados atualizados em tempo real pelos notários, naquilo que a legislação do país dispuser.

Nesse Simpósio, o *Prof. Nicholas Negroponte*, fundador e diretor do *Media Laboratory - Massachusetts Institute de Technology (MIT)* e o *Prof. Viktor Mayer-Schönberger*, da *John F. Kennedy School of Government - Harvard University*, ambos de Cambridge (USA), fizeram interessante abordagem dos possíveis efeitos da transmissão de informações por via eletrônica nos atos jurídicos em geral, com destaque para a função notarial. A conclusão foi no sentido de que a contratação eletrônica à distância depende do fator *confiança* em muito maior escala do que a contratação pelos meios convencionais, razão pela qual - se os notários forem capazes de oferecer aos contratantes o fator *confiança* de que necessitam - o futuro da função estará absolutamente assegurado em relação ao mercado.

BRASIL

Desde 1996, diversos projetos de lei foram apresentados no Congresso tratando do comércio eletrônico, do documento eletrônico e da assinatura digital.

No Senado, tramita o Projeto de Lei nº 672/99, de autoria do Senador Lúcio Alcântara, dispondo sobre o comércio eletrônico, baseado em projeto padrão sugerido pela UNCITRAL (Comissão das Nações Unidas para o Direito Comercial Internacional sobre Comércio Eletrônico). O Relator Senador José Fogaça já apresentou seu parecer, estando a matéria pronta para ser votada na Comissão de Constituição, Justiça e Cidadania do Senado. É um projeto com 26 artigos, estabelecendo princípios dentro do modelo de outorga, deixando à regulamentação e ao interesse das partes o encaminhamento da melhor solução para o mercado.

Na Câmara dos Deputados, tramita o Projeto de Lei nº 1589/99, apresentado pelo Dep. Luciano Pizzatto, com base em sugestão encaminhada pela Ordem dos Advogados do Brasil - Seção de São Paulo, dispondo sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital. É um projeto excelente, sob o ponto de vista jurídico e técnico, dentro do modelo prescritivo, prevendo e regulando a participação notarial no sistema de autenticação da assinatura digital, junto com empresas comerciais autenticadoras. Foi formada uma Comissão Mista presidida pelo Dep. Arolde de Oliveira, para examinar o projeto, ao qual foram apensados os demais projetos que tramitavam na Câmara sobre esse assunto. O Relator Dep. Júlio Semeghini deve apresentar seu parecer sobre o projeto ainda este ano. Existe forte pressão dos diversos setores interessados, no sentido de que projeto seja votado o mais rapidamente possível. É impossível fazer uma avaliação neste momento do resultado do processo legislativo, face aos elevados interesses econômicos envolvidos.

As principais disposições desse projeto, no que interessa aos notários, estão a seguir assinaladas.

Documento original (art. 14)

Considera-se original o documento eletrônico assinado pelo autor, mediante sistema criptográfico de chave pública.

Assinatura digital - Requisitos (art. 15)

Ser única e exclusiva para o documento assinado; ser passível de verificação; ser gerada sob exclusivo controle do signatário; estar de tal modo ligada ao documento eletrônico que, em caso de posterior alteração deste, a assinatura seja invalidada; não tenha sido gerada posteriormente à expiração, revogação ou suspensão das chaves.

Cópia (art. 14)

Considera-se cópia o documento eletrônico resultante da digitalização do documento físico, bem como a materialização física de documento eletrônico original.

A cópia do documento eletrônico é equiparada ao original, desde que autenticada pelo tabelião.

A cópia não autenticada terá o mesmo valor probante do original, se a parte contra quem foi produzida não negar sua conformidade.

Autenticação de cópias (art. 33/34)

A cópia eletrônica de documento físico original será autenticada com a aposição da assinatura digital do tabelião.

A cópia física de documento eletrônico original será autenticada mediante declaração do tabelião de que: a cópia impressa confere com o original eletrônico; as assinaturas digitais foram conferidas com o uso das chaves públicas; foram utilizados os identificadores das chaves públicas para conferência das assinaturas e respectivas certificações que contiverem; o nome dos que apuseram assinatura digital no documento eletrônico; a data das assinaturas; a data e a assinatura do tabelião.

Data do documento (art. 19)

A data do documento eletrônico é presumida verdadeira entre as partes.

Autenticação da chave pública por particular (art. 17)

A autenticação da chave pública por particular é considerada uma mera declaração de que a chave pública pertence ao titular indicado, não gerando presunção de autenticidade perante terceiros.

Autenticação da chave pública por tabelião (art. 25/26)

A autenticação da chave pública por tabelião faz presumir sua autenticidade.

O tabelião certificará a autenticidade de chaves públicas entregues pessoalmente pelo seu titular, devidamente identificado.

O pedido de certificação será efetuado por escrito e assinado pelo requerente, que informará os dados suficientes para a identificação da chave pública, a ser arquivada no tabelionato.

O tabelião deverá entregar ao solicitante informações adequadas sobre o funcionamento das chaves pública e privada, sua validade e limitações, bem como sobre os procedimentos adequados para preservar a segurança das mesmas.

O tabelião é proibido de receber em depósito a chave privada, bem como solicitar informações pessoais do requerente, além das necessárias para desempenho de suas funções, devendo utilizá-las apenas para os propósitos da certificação.

O certificado de autenticidade das chaves públicas deverá conter, no mínimo, as seguintes informações: a identificação e assinatura digital do Tabelião; a data de emissão do certificado; a identificação da chave pública e do seu titular; elementos que permitam identificar o sistema criptográfico

utilizado; o nome do titular e poder de representação de quem solicitou a certificação, no caso do titular ser pessoa jurídica; o prazo de validade do certificado.

Revogação do certificado eletrônico (art. 27/28)

O tabelião deverá revogar um certificado eletrônico: a pedido do titular da chave de assinatura ou de seu representante; de ofício ou por determinação do Poder Judiciário, caso se verifique que o certificado foi expedido com base em informações falsas; se tiver encerrado suas atividades, sem que tenha sido sucedido por outro tabelião.

A revogação deve ser feita perante o tabelião que emitiu o certificado e indicar a data a partir da qual será aplicada, não se admitindo revogação retroativa.

Uso do documento eletrônico (art. 36)

O uso do documento eletrônico em atividade notarial ou de registro, não prevista expressamente pela lei, poderá ser objeto de autorização especial do Poder Judiciário.

O DOCUMENTO ELETRÔNICO NA ADMINISTRAÇÃO PÚBLICA

O Decreto nº 3.587, de 05.09.00, estabeleceu a regulamentação do Poder Executivo Federal para o uso do documento eletrônico e da assinatura digital no âmbito da administração pública federal.

Foi criado o ICP-Gov como Infra-Estrutura de Chaves Públicas do Poder Executivo Federal, com poderes para utilizar a criptografia assimétrica.

Compete à *Autoridade de Gerência de Políticas (AGP)* propor a criação de AC-Raiz, estabelecer normas para o funcionamento da AC, AR e demais políticas relativas à segurança criptográfica.

Compete à *Autoridade Certificadora Raiz (AC Raiz)* emitir os certificados das Autoridades Certificadoras (AC) públicas e privadas que forem credenciadas, gerenciando a Lista de Certificados Revogados (LCR).

Compete à *Autoridade Certificadora (AC)* emitir, revogar e renovar certificados, gerenciar as chaves criptográficas e administrar o banco de dados dos certificados, divulgando as respectivas informações.

Compete à *Autoridade de Registro (AR)* receber os pedidos de certificação dos usuários, confirmar a identidade destes e a validade do pedido e encaminhar os documentos à AC responsável.

O decreto estabelece o prazo de 120 dias para sua regulamentação e contém um glossário útil para conhecer o significado dos termos usados no sistema de certificação.

No âmbito do Ministério da Fazenda, encontrava-se já em vigor desde 27 de dezembro de 1999 a Instrução Normativa SRF nº 156, de 22.12.99, que instituiu o certificado eletrônico da Secretaria da Receita Federal, a ser usado por pessoas físicas e jurídicas no relacionamento com aquele órgão, por meio eletrônico.

De acordo com tal instrução, a SRF atuará como AC Raiz, credenciando AC privadas, que fornecerão aos contribuintes seus respectivos certificados.

A emissão do certificado para o contribuinte obedecerá ao seguinte procedimento:

- o contribuinte acessa a página da Receita Federal na Internet, transferindo para seu computador o certificado digital da SRF e instalando-o; a seguir, escolhe na mesma página uma AC credenciada e contrata a emissão do certificado, transferindo para seu computador o respectivo instrumento;

- o contribuinte comparece à AR, onde será identificado e assinará o contrato, que será autenticado e remetido à AC;
- a AC emite o certificado em favor do contribuinte e registra o contrato em cartório.

O NOTÁRIO E O DOCUMENTO ELETRÔNICO

Sabemos que, de acordo com o inciso III do art. 6º da Lei nº 8.935/94, o notário possui hoje uma reserva de mercado para **autenticar fatos**.

Como se viu, a legislação em exame no Congresso pode dar ao notário brasileiro um elenco maior de responsabilidades, gerando novos serviços de mais alta importância para a sociedade.

No entanto, deve ser considerado que o inverso também poderá ocorrer, ou seja, ser aprovada uma legislação que deixe o notário fora do processo de autenticação, o que - sob nossa ótica - é muito provável que aconteça, tendo em vista o grau de interesse econômico que a atividade desperta e o receio de que o notariado monopolize o mercado, se a sua autenticação der maior garantia do que aquela expedida por uma empresa comercial.

É importante, pois, que se monte uma estratégia bem definida para atender às duas situações, o que ainda não foi feito, até mesmo por falta de recursos do Colégio Notarial do Brasil, cuja Diretoria entendeu dever deixar a critério dos próprios associados a fixação dos interesses individuais para o setor.

Em primeiro lugar, deveríamos definir quais os serviços que os notários têm interesse de prestar, dentro da estrutura das transações eletrônicas que aqui foi desenhada.

Definida a área de atuação, seria importante estabelecer quais as tarefas específicas exercidas pelo tabelião de notas que poderão ser otimizadas com o documento eletrônico e a assinatura digital.

Obviamente, a primeira nova tarefa que se vislumbra é a de autenticação das chaves públicas. Esse espaço, no entanto, já vem sendo ocupado no Brasil por empresas comerciais que são formadas a partir de capitais estrangeiros, do porte de uma *Certisign*, braço da americana *Verisign*, de que faz parte a Microsoft. Sabendo-se que a proprietária do programa RSA também é associada à *Verisign*, como fazer para concorrer com tais empresas? Qual seria o custo do licenciamento desse mesmo programa para os notários? Haveria segurança em tal dependência técnica dos notários, de natureza crucial para a autenticação?

Por outro lado, abrindo mão do mercado representado pela autenticação das chaves públicas, ainda assim os notários deverão ficar com a parte melindrosa do sistema, que será a identificação dos titulares das chaves, trabalho que irão realizar a pedido das empresas comerciais autenticadoras das chaves públicas, no caso de exigência da outra parte, para agregar maior confiança ao sistema. Ou seja, a *Certisign* cobrará para assinar digitalmente o certificado, deixando a responsabilidade pela identificação da parte a ser feita pelo notário, que não será remunerado pelo risco correspondente ao elo mais frágil da cadeia.

Essa incerteza não deve, todavia, deixar o notariado de mãos amarradas. Ao contrário, pensamos que devemos nos preparar culturalmente para fornecer os serviços de que a sociedade irá necessitar brevemente. Essa preparação poderia passar, por exemplo, pela criação de uma pequena rede de correio eletrônico seguro entre os notários, na qual o Colégio Notarial seria a autoridade certificadora, passando a ser usada a

assinatura digital na documentação que habitualmente transmitimos entre nós. Formada essa pequena rede, os colegas poderiam aderir à medida que houvesse interesse e os recursos técnicos adequados.

A imprensa está ávida por notícias na área de novas tecnologias. A simples divulgação da existência da rede pela mídia daria ao notariado uma importante exposição no sentido de que a sociedade seja informada de que existem tabeliães aptos a exercer assessoramento para o desenvolvimento de transações cuja necessidade nem seja hoje objeto de nossas considerações.

A ampliação dessa rede notarial poderá levar a comunicações seguras entre os tabelionatos de notas e registros de imóveis, seja para o fornecimento pelo registrador de certidões negativas necessárias à lavratura de escrituras, seja para a remessa pelo tabelião de notas de escrituras para conferência prévia pelo registrador, abreviando-se sobremaneira o tempo de entrega do documento à parte; nas relações entre tabelionatos de protestos e instituições financeiras, para o apontamento de duplicatas e prestação de contas; nas relações entre tabelionatos de notas e órgãos arrecadadores do Poder Público, para a obtenção de certidões negativas.

Se, ao final do procedimento legislativo ora em andamento, for admitida pela lei a participação do notário na venda de certificados de chaves públicas, e aceita a conveniência na disputa por esse mercado, estaríamos prontos para competir com muito maior grau de eficiência e, sobretudo, com maior confiança da sociedade.

A expedição pelo notário de um certificado de autenticidade irá conferir a presunção de autenticidade à chave pública que o tabelião certificar, efeito que não terá o certificado expedido por empresa comercial.

Por outro lado, se o próprio notário participar do documento eletrônico com sua assinatura digital, estará corroborando sua validade.

Parece-nos intuitiva a vantagem de ser criada pelo Colégio Notarial uma rede de associados cibernotários, divulgando institucionalmente as chaves públicas desses profissionais e criando um promissor mercado para uma atividade que será realidade dentro de pouco tempo. O Colégio Notarial poderia, ainda, certificar as chaves públicas de seus associados, divulgando-as regularmente, de tal forma que fosse criada uma cultura popular de utilização do notário como autoridade certificadora da chave pública de empresas e pessoas físicas.

Note-se que essa atividade certamente poderá ser exercida por outras entidades ou corporações (bancos em relação a seus clientes, OAB em relação aos advogados, administração pública em relação a seus agentes, etc.). Assim, é bem provável que os precursores nessa atividade terão grande chance de entrar no imaginário popular como aqueles que estão mais capacitados a outorgar o certificado da chave pública.

No momento em que o documento eletrônico seja aceito como prova reconhecida legalmente, e a sociedade adquira a cultura de usá-lo regularmente, algumas outras atividades correlatas poderão ser inseridas no cotidiano da vida notarial, sendo o tabelião de notas chamado a atender a algumas necessidades, como por exemplo:

- um cliente necessita realizar um contrato à distância e não se julga apto a fazê-lo, ou por desconhecer as regras, ou por não dispor de equipamento adequado, ou, ainda, por simples receio de utilizar um procedimento novo;
- um cliente necessita eventualmente comprovar que um documento eletrônico foi transmitido em determinada data e o faz utilizando-

se do serviço do notário, que irá apor sua própria assinatura digital ao documento;

- a adoção de um registro especial para tais transmissões, no caso de não desejar usar sua própria firma digital no documento;

- a extração e autenticação da cópia em meio físico de um documento eletrônico;

- a simples autenticação da cópia em meio físico de um documento eletrônico, após sua conferência com o original, que é feita por meio de programas especiais existentes no mercado;

- a expedição via internet de qualquer dessas cópias a um terceiro, certificada por sua assinatura digital;

- a necessidade de guarda da chave privada, que pode ser assegurada através de escrito particular corroborado por escritura pública lavrada a pedido do interessado, na forma equivalente a um testamento cerrado, documento que poderá ou não ficar sob a guarda do tabelião, para entrega ao próprio interessado ou a quem ele indicar;

- a conveniência de que um contrato à distância, entre partes de países diferentes, tenha a participação notarial, envolvendo a necessidade de exame de sua regularidade com a lei aplicável nos respectivos países.

Embora seja acentuada a conveniência da existência de uma lei reguladora da matéria, nem por isso os notários devem ficar omissos às necessidades que hoje eventualmente possam já ser realidade. Assim, quem deseje fazer uso de uma assinatura digital pode dirigir-se a um tabelião e pedir que seja lavrada uma escritura na qual declare os dados de sua chave pública e sua responsabilidade pelos documentos eletrônicos gerados com a aplicação de sua chave privada.

É preciso, entretanto, que não seja esquecida a regra básica processual de que a autenticação notarial

estabelece apenas a presunção de veracidade da cópia em relação ao documento original. Equivale dizer que - se for alegada a falsidade - torna-se necessário o confronto com o original. Daí a importância de que o tabelião esteja preparado com o conhecimento técnico adequado para conhecer os limites dos novos meios que irá utilizar em sua atividade, resguardando-se para a eventualidade de ser chamado a juízo para comprovar a lisura de seu procedimento.

Como hoje no mundo do papel, o maior valor que o notário poderá agregar às transações realizadas por meio eletrônico é a **confiança**. Aliás, no mesmo simpósio sobre documento eletrônico realizado pelo notariado austríaco, de que já falamos anteriormente, o Prof. Negroponte destacava o fato de que a sobrevivência do notário no mundo virtual das transações eletrônicas irá depender do maior ou menor grau de confiabilidade que as partes considerarem estar sendo agregada a tais operações pela participação notarial.

Com a disseminação do uso da assinatura eletrônica, será exigida uma maior valorização da atividade notarial, especialmente no que se refere às funções de interpretação e adequação da vontade das partes e do controle da legalidade dos atos, como bem lembrou o notário italiano Raimondo Zagami, doutor em direito de informática pela Universidade de Bolonha, em entrevista concedida ao registrador paulista Sérgio Jacomino.

Na certificação do documento eletrônico, o notário deverá ter um papel diferente daquele que se espera das empresas comerciais de certificação. Como se sabe, a verificação de uma assinatura digital não fornece a verdadeira identidade do subscritor, mas a da pessoa que é responsável pela assinatura. Assim, a assinatura digital aposta por pessoa diversa do titular é idêntica àquela que o legítimo titular firmaria, o que pode não

dar ao negócio contratado a segurança jurídica verdadeira que dele se espera.

Entretanto, a autenticação e o reconhecimento da assinatura eletrônica pelo notário, mediante a aposição de sua própria assinatura digital no documento, pressupõe a certificação de que a firma eletrônica foi aposta em sua presença, tendo sido previamente verificada a identidade pessoal do signatário, a validade da chave utilizada e a legalidade do documento subscrito, ficando o notário responsável pela certeza de três elementos: a) - a real identidade do subscritor; b) - a conformidade do ato subscrito com a lei local, de suma relevância na contratação internacional à distância; c) - a conformidade do ato com a vontade da parte signatária. Evidentemente, como nos atos praticados em papel, a intervenção notarial somente será solicitada naquelas transações que justifiquem o cuidado a que nos referimos.

CERTIDÃO EXTRAÍDA VIA INTERNET

Devem ser ressaltados dois princípios básicos a respeito do documento eletrônico:

- a) - o documento eletrônico não assinado não permite, por si, que seja demonstrada sua autoria, não servindo como meio de prova;
- b) - somente a assinatura criptográfica permite que um documento eletrônico seja insuscetível de modificação;
- c) - uma página da rede internet pode ser alterada a qualquer momento, de forma que não fique vestígio material do que estava escrito anteriormente;
- d) - o registro em poder de uma parte, sem a inalterabilidade conferida pela assinatura criptográfica da outra parte, é amplamente suscetível de modificações.

A gravação feita num *CD Worm* (*write once read many* - escrever uma vez, ler muitas vezes) permite que se grave uma única vez, não podendo ser apagado.

CRIPTOGRAFIA POR SISTEMAS BIOMÉTRICOS

A Prefeitura de Oceanside, CA, trocou o código dos sites governamentais da cidade por dispositivo biométrico (impressão digital). A vantagem para os contribuintes locais é que a senha é pessoal, não podendo ser roubada ou compartilhada.

Estão sendo desenvolvidos outros sistemas biométricos, como o exame da íris e do tom de voz.

SEGURANÇA E PRIVACIDADE NA REDE

O Departamento de Justiça dos Estados Unidos está promovendo uma devassa no programa denominado **Carnivore**, utilizado pelo FBI para exercer vigilância sobre a *internet* e o trânsito de *e-mails*.

PROJETOS SOBRE COMÉRCIO E DOCUMENTO ELETRÔNICO

Dia 29.11.00, quarta-feira, será realizada sessão da Comissão Especial da Câmara dos Deputados para marcar a data da última audiência pública antes da apresentação do relatório sobre o Projeto nº 1589/99. Serão convidados Rui Rosado, Ministro do STJ, e José Rogério Cruz, Professor da Faculdade de Direito da USP, para tratar dos aspectos vinculados ao Código de Defesa do Consumidor.

SUMÁRIO

- Advertência
- O Documento
- O Documento Eletrônico
- A Prova
- O Documento Eletrônico e a Prova
- A Criptografia
- A Assinatura Digital
- A Integridade do Documento Eletrônico
- A Chave Pública
- A Chave Privada
- A Certificação
- A Evolução da Legislação no Mundo
 - Estados Unidos - Canadá - México - Argentina - Europa -
 - Itália - Áustria - Brasil
- A Administração Pública e o Documento Eletrônico
- O Notário e o Documento Eletrônico
- Atualidades