A FIRMA DIGITAL E ENTIDADES DE CERTIFICAÇÃO

Mário Antônio Lobato de Paiva (*)
José Cuervo (*)

Sumário: Introdução; 1- Firma analógica (manuscrita); 1.1- Características da firma; 1.2- Elementos da firma; 1.3- Aspectos legais; 2- Firma digital (eletrônica); 2.1- Características da firma eletrônica; 2.2 Aspectos legais; 2.2.1- Nos Estados Unidos; 2.2.2 – Na Europa; 2.2.3 – No México; 2.2.4 – No Brasil; 2.2.5- A nivel internacional; 2.3- Legalidade dos documentos com firma digital; 3- Autoridade ou entidade de certificação de chaves; 3.1 Funções das autoridades de certificação; 3.2 Autoridades públicas de certificação; 3.3- Autoridades privadas de certificação; 4- Conclusões; 5; Bibliografia.

Introdução

A incorporação das novas tecnologias da informação em nossa sociedade fazem com que em diversas situações, os conceitos jurídicos tradicionais sejam pouco idôneos para interpretar as novas realidades. O avanço de sua implantação em todas as atividades tem provocado transformações de ampla magnitude que nos permite afirmar que a sociedade atual está imersa na era da revolução informática. Este avanço nos permite o acesso a todo tipo de informação, obtendo com ela um benefício correspondente.

A informação tem sido qualificada como um autêntico poder nas sociedades avançadas, demonstndo sua importância desde a antiguidade e que com o desenvolvimento da telemática seu valor tem expandido de tal forma que se dirige a um futuro pomissor para uns e incertos para outros.

O comércio, como disse DEL PESO NAVARRO, pioneiro em inovações jurídicas introduzidas no passado por meio de costume, uma vez mais toma a dianteira e inumeráveis transações econômicas vem sendo realizadas através dos meios eletrônicos, sem mais suporte legal que ao pacto entre as partes.

A contratação eletrônica em seu mais puro sentido, pouco a pouco vem sendo desenvolvida e cresce de forma espetacular. Uma vez mais temos caminhado diante deste direito, entendendo esse como direito positivo.

Na maioria das situações que envolvem questões jurídicas relacionadas com a informática quando tratamos de reconduzir estes novos feitos as figuras jurídicas jurídicas existentes nos deparamos com certas dificuldades. As velhas intituições jurídicas que, através dos séculos tem sido incorporadas as novas realidades sociais, quando tem de fazê-lo com respeito a estas novas tecnologias entram em conflito ou as admitem com reservas. Assim ocorre quando tratamos de adaptar o conceito de firma, tal como antigamente se concebia, ao novo campo das transações eletrônicas.

O objetivo pretendido com o presente ensaio é de adentrar-mos no tema “documento informático”, da firma e sua autenicação e sua importância, bem como os efeitos probatórios do documento em si, fazendo um breve repasse em sua aceitação nacional e internacional e as futuras autoridades de certificação das firmas digitais

1. Firma analógica

Segundo CARRASCOSA LÓPEZ , podemos indicar que em Roma, os documentos não eram firmados. Existia uma cerimônia chamada manufirmatio, pelo qual, logo após a leitura do documento por seu autor e o notarius, era estendido sobre uma mesa e se passava a mão pelo pergaminho em sinal de sua aceitação. Somente depois de cumprir essa cerimônia era estampado o nome do autor.

O sistema jurídico Visigótico existia a confirmação do documento pelas testemunhas que o tocavam (Chartam tangere), assinavam e subescreviam (firmatio, roboratio, stipulatio). Os documentos privados são, em ocasiões, confirmados por documentos reais. Desde a época euriciana as leis visigotas determinavam as formalidades documentais, regulando detalhadamente as assinaturas, signos e comprovação de escrituras. A “assinatura” respresentada pela indicação do nome do signante e a data, e o “signum”, um rasgo (traço dado com pena) que a substitue se não se souber ou não se puder escrever. Com a “assinatura” é dado pleno valor probatório ao documento e ao “signum” devia ser complementado com o juramento de dizer a verdade por parte de uma das testemunhas Se faltar a firma ou o sinal do autor do documento, está será inoperante e deve completar-se com o juramento das testemunhas sobre a veracidade do conteúdo.

Na idade média, a documentação régia vinha garantida em sua autenticidade pela implantação do selo real, selo que posteriormente passou as classes nobres e privilegiadas.

A firma era definida pela doutrina como o signo pessoal distintivo que, permite informar acerca da identidade do autor de um documento, e manifestar seu acordo sobre o conteúdo do ato.

A Real Academia da Língua Espanhola define a firma como: “nome e apelido ou título de uma pessoa que está por com rúbrica ao pé de um documento escrito a mão própria ou alheia, para dar-lhe autenticidade, para exepressar que se aprova seu conteúdo ou para obrigar-se ao que nele se disse”.

O Novo Dicionário da Língua Portuguese define firma como: “assinatura por extenso ou abreviada, manuscrita ou gravada”

No vocabulário de COUTORE se define como: “traçado gráfico, contendo habitulamente o nome, os apelidos e a rúbrica de uma pessoa, com a qual se

subscrevem os documentos para dar-lhes autoria e virtualidade e obrigar-se a que neles foi dito".

1.1. Características da firma

Das anteriores definições se depreendem as seguintes características:

a) Identificativa: serve para identificar quem é o autor do documento

b) Declarativa: significa a assunção do conteúdo do documento pelo autor da firma. Sobretudo quando se trata da conclusão de um contrato, a forma é o sinal principal que representa a vontade de obrigar-se.

3- Probatoria: permite identificar se o autor da firma é efetivamente o que celebrou a ato de firmar o documento.

1.2. Elementos da firma

Temos que distinguir entre:

a) Elementos formais: são aqueles materiais da firma que estão relacionados com os procedimentos utilizados para firmar e ao grafismo mesmo da firma.

- A firma como sinal pessoal

A firma é representada como uma espécie de sinal distintivo e pessoal, já que deve ser posta pelo punho e letra do firmante. Essa característca da firma manuscrita pode ser eliminada e substituída por outros meioscomo por exemplo, na firma eletrônica.

- O animus signandi

b) Elemento intencional ou intelectual da firma: consiste na vontade de assumir o conteúdo de um documento, que não deve ser confundido com a vontade de contratar.

c) Elementos funcionais

Tomando a noção de firma como o sinal ou conjunto de sinais, podemos distinguir um dupla função.

- Identificadora

A firma assegura a relação jurídica entre o ato firmado e a pessoa que o firmou.

A identidade da pessoa determina sua personalidade e os efeitos de atribuidos no campo dos direitos e obrigações.

A firma manuscrita expressa a identidade, aceitação e a autoria do firmante. Não é um método de autenticação totalmente confiável. No caso de ser reconhecido a firma, o documento poderia ter sido modificado quanto ao seu conteúdo – falsificado- e no caso de que não existir a firma autografada parece fica prejudicado outro meio de autenticação. Em caso de dúvida ou negativa deverá ser realizada competente perícia caligráfica para seu esclarecimento.

-Autenticação

O autor do ato expressa seu consentimento e faz sua própria mensagem.Destacando:

- Operação passiva que não requer o consentimento, nem mesmo do próprio sujeito identificado.

- Processo ativo pelo qual algúem se identifica conscientemente bem como quanto ao conteúdo subscrito atribuido ao mesmo.

1.3. Aspectos legais

A firma credita a autoria do documento subscrito normalmente ao final do mesmo e representa a formalização do consentimento e a aceitação do exposto, e portanto originina direitos e obrigações. A firma será válida sempre que não seja falsificada ou tenha sido obtido com engano, coação ou de qualquer outro procedimento ilícito.

2.Firma digital (eletrônica)

As firmas digitais baseadas na criptografia assimétrica podem ser enquadradas em um conceito mais geral de firma eletrônica, que não pressuõe necessariamente a utilização de tecnologias de cifrado assimétrico, pois que geralmente, vários autores referem indistintamente da firma eletrônica ou de firma digital.

Tem os mesmos encargos da firma manuscrita, porém expressa a identidade e a autoria, a autenticação, a integridade, a data, a hora e a recepção, através de métodos criptográficos assimétricos de chave pública (RSA, GAMAL, PGP, DAS, LUC, etc...), técnicas de selamento eletrônico e funções Hash, o que faz com que a firma esteja em função do documento que se subscreve (não é constante), porém que seja feita de forma absolutamente inimitável caso não possua a chave privada com a que esta encripitada, verdadeira atribuição a identidade e autoria.

Para Y. POULLET a firma eletrônica supõe uma série de características assinaladas ao final do documento. É elaborada segundo procedimentos criptográficos, e leva um resumo codificado de mensagem, é a identidade do emissor e receptor.

Para DEL PESO NAVARRO assevera que firma eletrônica é um sinal digital representado por uma cadeia de bits que se caracteriza por ser secreta, fácil de reproduzir e de reconhecer, difícil de falsificar e transformar em função da mensagem e em função do tempo, cuja a utilização obriga a aparição do que se denomina fedatário eletrônico ou telemático que será capaz de verificar a autenticidade dos documentos que circulam através das linhas de comunicação, ao ter não somente uma informação informática, mas também jurídica.

As firmas eletrônicas ou digitais consistem basicamente na aplicação de algoritmos de encriptação de dados, desta forma, só será reconhecido pelo destinatário, que poderá comprovar a identidade do rementente, a integridade do documento, autoria e autenticação, preservando o mesmo tempo a confidencialidade.

A seguridade do algoritmo está diretamente relacionada com seu tipo, tamanho, tempo de cifrado e a violação do segredo.

Os criptosistemas de chave pública, são mais idôneos como firma digital, além disso tecnicamente são muito resistentes, pois calcula-se que levaria muitos anos para que o computador mais potente pudesse romper a chave. Seu mecanismo de segurança se baseia sobretudo no absoluto segredo das chaves privadas, tanto na sua geração quando no armaenamento bem como na certificação da chave pública pela autoridade certificadora.

Entre os objetivos da firma eletrônica está de a conseguir a mundialização de um modelo universal de firma eletrônica.

2.1. Características da firma eletrônica

Das definiçõe anteriores podemos destacar as seguintes características:

- Deve permitir a identificação do signatário. Adentramos no conceito de “autoria eletrônica” como forma de determinar que uma pessoa é quem diz ser.

- Não pode ser gerada por pessoa diversa da do emissor do documento, infalsificável e inimitável.

- As informações geradas a partir da assinatura eletrônica devem ser suficientes para poder validá-la, porém insuficientes para falsificá-la

- A posivel intervenção o Notário eletrônico dará mario segurança ao sistema.

- A aposição de uma assinatura deve ser significativa e esteja relacionada de forma indissociavel ao documento a que se refere.

- Não deve existir dilação de tempo nem lugar entre a aceitação pelo signatário e a aposição da assinatura.

2.2.1. Nos Estados Unidos

No final da década de sessenta, o governo dos Estados Unidos publicou o Data Encryption Standard (DES) para comunicações de dados sensíveis porém não classificados. Em 16 de abril de 1993, o governo dos EE.UU anunciou uma nova iniciativa criptográfica com vistas a proporcionar a civis um alto nível e segurança nas comunicações: projeto Clipper. Esta iniciativa baseou-se em dois elementos fundamentais:

a) Um chip cifrador a prova de qualquer tipo de análise ou manipulação (o Clipper chip o EES (Escrowed Encryption Standard) e;

b) Um sistema para compartilhar as chaves secretas (KES -Key Escrow System) que, em determinadas circunstâncias, outorgaria o acesso a chave mestra de cada chip e permitindo conhecer as comunicações cifradas por ele.

Nos EE.UU é onde encontramos a mais avançada legislação sobre firma eletrônica, através do projeto de standartização do NIST (The National Institute of Science and Technology. O NIST foi introduzido no projeto Cpasone, o DSS (Digital Signature Standard) como uma espécie de standart da firma, apesar do governo americano não ter assumido como stanadat sua utilização. O NIST promove a afirma abandeira de equiparação da firma manuscrita a digital.

A lei de referência da firma digital, para os legisladores dos Estados Unidos da ABA (American Bar Association), Digital Signature Guidelines, de 1 de agosto de 1996.

O valor probatório da firma tem sido admitido em Utah, primeiro estado a dotar-se de uma lei de firma digital. A firma digital de Utah (Digital Signature Act Utah de 27 de fevereiro de 1995, modificado em 1996) se baseia em um “Criptosistema Assimétrico” definido como um algoritmo que proporciona um par de chaves seguro.

Seus objetivos são os de facilitar o comércio por meio de mensagens eletrônicas confiáveis, minimizar a incidências da falsificação de firmas digitais e a fraude no comércio eletrônico.

A firma digital é uma transformação de uma mensagem utilizando um criptosistema assimétrico, de tal forma que uma pessoa que tenha a mensagem cifrada e a chave pública de quem a firmou, pode determinar com precisão a

mensagem em claro e se foi cifrada usando a chave privada que corresponde a pública do firmante.

O Estado de Utah tem redação de um projeto de lei (The Act on Electronic Notarization) em 1997.

A California define a firma digital como a criação pelo computador de um identificador eletrônico que inclue todas as caracteríticas de uma firma válida, aceitável, como a única capaz de comprovar-se através de um só controle, entrelaçando-se com os dados de tal maneira que se houver modificação dos dados a firma autoatiamente é invalidada levando-se em consideração o modelo universal adotado pelas seguintes organizações:- The International Telecommunication Unión.- The American National Standards Institute.- The Internet Activities Board.- The National Institute of Science and Technology.- The International Standards Organization. Podemos fazer referência a: ABA, Resolution concerning the CyberNotary: an International computer-transaction specialist, de 2 de agosto de 1994. The Electronic Signature Act Florida , de maio de 1.996 que reconhece a equivalência probatória da firma digital com a firma manual. E nesta lei é usado o termo “international notary” em vez de “cybernotary” utilizado em outras leis nos EE.UU. The Electronic Commerce Act, de 30 de maio de 1997, que faz referência ao cybernotary.

The Massachusetts Electronic Records and Signatures Act, de 1996, que reconhece todo o mecanismo capaz de proporcionar as funções da firma manuscrita sem cingir-se a um tipo concreto de tecnología.

2.2.2.Na Europa

A Comissão Europeia tem pretendido harmonizar os regulamentos de criptografia de todos os Estado membros. Até o momento, só aluns países dispõem de leis sobre firma digital e ou cifrado.

Na Espanha

A legislação atual e a jurisprudência, são suficientemente amplas no esclarecimento do conceito e firma manuscrita a firma digital ou a qualquer outro tipo de firma. O certo é que por razões de segurança e para oferecer maior confiança aos usuários e juízes que julguem casos evolvendo a firma digital, há necessidade de uma reforma da lei cujo o objetivo é o de equiparar a firma manuscrita a qualquer outro meio de firma que cumpra as mesmas finalidades.

O artigo 3 da RD 2404/1985, de 18 de dezembro, ao regular os requisitos mínimos das faturas, não exige que sejam firmadas. Bem é verdade que o Código de Comércio não exige, pela regra geral, para uma eficácia do contrato ou da fatura, a firma nem nenhum outro signo de validade, apesar de muitos ordenamentos jurídicos requererem que os documentos estejam firmados de forma manuscrita – de punho e letra – como para da solenidade da transação de forma privada.

Cremos que não existe inconveniente algum em admitir a possibilidade de uma firma eletrônica.

A circular do Banco da Espanha 8/88 de 14 de junho criando o regulamento do Sistema Nacional de Conpensação eletrônica, se converteu-se em um marco na proteção e segurança necessária na identificação para o acesso a informática, ao indicar que a informação será cifrada, para que as entidades introduzam um dado de autenticação com a informação de cada comunicação, o que é reconhecido a este método o mesmo valor que o que um escrito firmado por pessoas com poder bastante para tal fim.

O artigo 45 da Lei 30/1992 do regime das Administrações públicas e do Procedimento Administrativo Comum incorporou o emprego e aplicação dos meios eletrônicos na atuação administrativa aos cidadãos Para sua regulamentação, o Real Decreto 263/199 de 16 de fevereiro, indica que deverão adaptar-se as medidas técnicas que garantam a identificação e a autenticidade da vontade declarada, porém não há nenhuma regulamentação legal para a “firma eletrônica”.

Na Alemanha

A lei de firma digital regula os certificados de chaves e a autoridade certificadora. Permite o pseudônimo, porém preve sua identificação real por ordem judicial. A firma eletrônica tem sido definiada como selo digital, com uma chave privada associada a chave pública certificada por um certificador.

A lei de 19 de setembro de 1996 é o primeiro projeto de lei de firma digital na Europa e entrou em vigor em 01 de novembro de 1996.

Na França

A França é um dos países que mais tem avançado em termos de legislação em matérias envolvendo a informática.A reforma do Código Civil da República da França mediante a Lei n 2000-230 de 13 de março de 2000, sobre adaptação do direito de prova as novas tecnologias da informação e relativa a firma eletrônica introduziu imprantes modificações no Capítulo VI, Da prova das obrigações e do pagamento, em seu artigos 1315 inciso 1 e artigo 1316 incisos 1 a 4.

O inciso mais importante a nosso ver foi o artigo 1316-1 que dispõe: L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. (O escrito em forma eletrônica será admitido como prova com igual força que o escrito em suporte de papel, salvo reserva de que pode ser devidamente identificada a pessoa de que emana e que seja gerado e conservado m condições que permitam garantir sua integridade.)

Como podemos observar da leitura do artigo, é atribuído força probatória ao documento eletrônico nas mesmas circunstâncias que o escrito em suporte de papel, desde que observe três condições fundamentais; a) identificação do autor do documento; b) o processo de geração do documento deve garantir sua integridade; c) o processo de conservação do documento deve garantir sua integridade.

Na Itália

A lei nº 59 de 15 de março de 1997, é a primeira norma do ordenamento jurídico italiano que reconhece o princípio da plena validez dos documentos informáticos baseando-se em solucões etrangeiras e supranacionais.

O regulamento aprovado pelo Conselho de Ministros de 31 de outubro de 1997 define a firma digital como o resultado do processo informático (validação) baseado em um sistema de chaves assimétricas ou duplas, uma pública e uma privada, que permite ao subescritor transmitir a chave privada e ao destinatário transmitir a chave pública, respectivamente, para verificar a procedência e a integralidade de um documento informático ou de um conjunto de documentos informáticos (artigo 1º alínea b). No regulamento da firma digital está baseado exclusivamente no emprego de sistemas de cifrado chamados assimétricos. Regulam a lei e o regulamento entre outras coisas: A validez do documentos informático; o documento informático sem firma digital; o documento informático com firma digital; os certificadores; os certificados, autenticação da firma digital; o “cybernotary”; os atos públicos notariais; a validação temporal; a caducidade, revogação e suspensão da chaves; a firma digital falsa; a duplicidade, cópia e extratos do documento e a transmissão do documento.

O Reino Unido

Há um vivo debate sobre a possibilidade de regulamentação dos terceiros de confiança – TC. Existe um projeto de lei sobre firma dgital e terceiros de Cofiança.

Nos Países Baixos

Se tem criado um organismo ministerial encarregado do estudo da firma digital. Na Dinamaca, Suiça e Bélgica está sendo elaborado um projeto de lei sobre firma digital. Na Suécia organizou-se uma audiência púlica sobre a firma digital em 1997.

Na Comunidade Europeia

O artigo 6 do Acordo EDI (Electronic Data Interchange) da Comissão das comunidades Europeias, que determina a necessidade de garantia de origem do documento eletrônico, não atenta para a regulamentação da firma eletrônica.

Não obstante PERALES VISCASILLAS acreditar que não exista inconveniente algum em admitir a possibilidade de uma firma eletrônica ser apoiada nas seguintes circunstâncias:

a) A Confiabilidade da firma eletrônica é superior a da firma manuscrita;

b). A equiparação no ambito comecial internacional da firma eletrônica e da firma manuscrita

c) No contexto das transações EDI é habitual a utilização da conhecida como “firma digital" que é baseada em algoritmos simétricos nos quais ambas as partes conhecem a mesma chave e os em “algoritmos assimétricos” nos quais, pelo contrário, cada contratante tem uma chave diferente. No mesmo sentido Isabel HERNANDO referindo-se aos contratos-tipo da EDI indica que se as mensagens EDI são transmitidas mediante procedimentos de autenticação como a firma digital, estas mensagens terão entre as partes contratantes o mesmo valor probatório que o acordado em documento escrito firmado.

A Comissão Europeia tem financiado numerosos projetos (INFOSEC, SPRI, etc.) cujo objetivo é a investigação dos aspectos técnicos, legais e econômicos da firma digital.

A Comissão Europeia publicou em outubro de 1997 uma Comunicação ao Conselho, ao Parlamento Europeu, ao Comitê Econômico e Social e ao Comitê das Regiões intitulado “Iniciativa Europeia de Comércio Eletrônico”, com um subtítulo de “Criar um Marco Europeu para a Firma Digital e o Cifrado”

O que pretende a Comissão Europeia é encontrar um reconhecimento legal comum na Europa sobre firma digital, com o objetivo de harmonizar as diferentes legislações, para que esta carta tenha natureza e eficácia legal perante os tribunais em matéria penal, civil e mercantil, para efeitos de prova, apercebimento e autenticidade.

Para conseguir essa coerência europeia deverá, sem dúvida, passar pelo estabelecimento de uma política europeia de controle suscitando o mínimo de conflitos com outras potências econômicas como o EE.UU, Canadá e Japão.

2.2.3. No México

A utilização de certificados emitidos na rede de certificação digital em convênio com a Associação nacional de Notariado Mexicano A. C. e Acertia. Com e que veiculam a uma pessoa determinada a um par de chaves e necessária para dar segurança e fidelidade ao uso de firmas eletrônicas em comunidades amplas e de grande escala. Assim se soluciona o problema da integridade, autenticidade e a recusa de sua origem.

O uso do par de chaves em princípio é único e tem base no sistema informático e apoio na geração do certificado se considera imanipulável e para os casos de algum defeito na geração de chaves, os credores das chaves serão responsáveis de algum defeito ocorrido.

O funcionamento do registro público de comércio nulifica a possibilidade de fraudes ou recusa das transações em curso.

Surge como fonte geradora de obrigações a relação do notário e o particular no processo de outorgamento de certificados digitais.

O papel do terceiro como testemunha eletrônico será capaz de desenvolver a forma de fazer negócios na internet. Outorgando a certeza e segurança jurídica necessária para que as partes possam celebrar contratos eletrônicos da mesma forma com que celebram os de forma escrita.

O contrato eletrônico cumpre com todos os elementos do contrato pelo que sua validade jurídica é plena.

O notário público no México é o mais indicado para agir como testemunha eletrônica já que é uma pessoa em que o Estado tem delegado sua faculdade de dar fé aos atos jurídicos.

No México com o conjunto de reformas legais aplicáveis ao comércio eletrônico, será possível a firma eletrônica e assim desta maneira proporcionar o suporte legal necessário para seu funcionamento, sem embargo de uma maior regulação em matéria de contratação eletrônica aonde se incluam temas como as obrigações das partes, a participação de terceiro como testemunha, o objeto do contrato, os meios de manifestação da vontade, a formação do contrato, a segurança e prova do contrato (firma eletrônica e certificados digitais), a forma de execução do contrato, a legalidade da fatura eletrônica, formas de dinheiro eletrônico, a forma de pagamento, e forma de resolução de conflitos.

2.2.4. No Brasil

No Brasil temos apenas e em tramitação o Projeto de Lei nº 3.173, de 1997 (PLS nº 22/97), aprovado no Senado, em 13.5.97, na forma de um Substitutivo, encaminhado recentemente para a Câmara do Deputados para revisão, nos termos do art. 65 da Constituição Federal que dispõe sobre os documentos públicos e privados produzidos e arquivados em meio eletrônico, sua conservação, garantia de autenticidade, oportunidade em que poderão ser eliminados e sua força probatória em juízo.

Na Justificação, o Senador Sebastião Rocha apregoa as vantagens da utilização do meio eletrônico, que se constitui em um avanço tecnológico sem precedentes na história da humanidade, sendo, o atual sistema de arquivamento de

documentos, ultrapassado, na medida em que se constitui num mero empilhamento de papéis repletos de microorganismos. Pela nova sistemática, a autenticidade dos documentos poderá ser certificada pelo órgão de origem, com a identificação dos servidores responsáveis pelo procedimento.

Porém muito ainda há para ser feito nessa seara daí a necessidade do estudo da legislação e doutrina estrangeira no sentido de aprimorar nossos conhecimentos e implantar em nosso país as benfeitorias desses estudos para a melhor convivência da sociedade digital.

2.2.5. A nivel internacional.

Nas Nações Unidas

A Comissão das Nações Unidas para o Direito Mercantil Internacional (CNUDMI-UNCITRAL) em seu 24º período de sessões celebrado de 1991 encarregou ao Grupo de Trabalho denominado “Pagos internacionais” o estudo dos problemas jurídicos relacionados ao intercâmbio eletrônico de dados (EDI: Electronic Data Interchange).

O Grupo de Trabalho dedicou seu 14º período de sessões, celebrado em Viena de 27 de janeiro à 7 de fevreiro de 1992, a este tema e elaborou um informe que foi levado a Comissão. Mencionado encontro determinou a definição de firma e outros meios de autenticação que deveriam ser inseridos em convenções internacionais.

Foi adotada por uma grande parte de países a definição ampla de “firma” contida na Convenção das Nações Unidas sobre Letra de Cambio Internacionais e Pagamentos Internacionais, que dispõe: “o termo firma designa a firma manuscrita, seu fac-símile ou uma autenticação equivalente efetuada por outros meios”. Pelo contrário, a Lei modelo sobre transferências internacionais de Crédito utiliza o conceito de “autenticação” ou de “autenticação comercialmente razoável”, prescindindo da noção de firma, afim de evitar dificuldades que esta pode ocasionar, tanto a concepção tradicional deste termo como sua concepção ampliada. Em seu 25º período de sessões celebrado em 1992, a Comissão examinou o informe do 1º Grupo de Trabalho e rencomendou a preparação de uma regulamentação jurídica do EDI ao Grupo de Trabalho, agora denominado Intercâmbio Eletrônico de Dados. O Grupo de Trabalho sobre Intercâmbio Eletrônico de Dados, celebrou seu 25º período de sessões em Nova York de 04 a 15 de janeiro de 1993 em que foi tratada a autenticação da mensagens EDI, com vistas a estabelecer um equivalente funcional com a ‘firma’.

O Plenário da Comissão das Nações Unidas para o Direito Mercantil Internacional (CNUDMI-UNCITRAL), em junho de 1996 em seu 29º período de sessões celebrado em Nova York, examinou e aprovou o projeto de Lei Modelo sobre aspectos jurídicos da EDI com base na Lei Modelo sobre comércio eletrônico (Resolução Geral da Assembléia 51/162 de 16 de dezembro de 1996). O arigo 7

da Lei modelo reconhece o conceito de firma. A Comissão recomendou ao Grupo de Trabalho, agora denominado “sobre comercio eletrônico” que se ocupe em examinar as questões jurídicas relativas as firmas digitais e as autoridades de certificação. A Comissão pediu a Secretaria que preparasse um estudo de antecedentes sobre questões relativas as firmas digitais. O estudo da Secretaria ficou reconhecido no documento A/CN.9/WG.IV/WP.71 de 31 de dezembro de 1996. O Grupo de Trabalho sobre Comércio Eletrônico celebrou seu 31 periodo de sessões em Nova York de 18 a 28 de fevereiro de 1997 e tratou de fixar as diretrizes sobre as firmas digitais publicadas pela American Bar Association. O Plenário da Comissão da Nações Unidas para o Direito Mercantil Internacional, que celebrou seu 30 período de sessões em Viena de 12 a 30 de maio de 1997, examinou o informe do grupo de Trabalho, suas conclusões e recomendou a preparação de um regime uniforme sobre as questões jurídicas da firma numérica e as entidades certificadoras.

O artigo 7 da Lei Modelo sobre Comércio Eletronico (LMCE) regula o equivalente funcional de firma, estabelecendo os requisitos de admissibilidade de uma firma produzida por meio eletrônico, que nos dando um conceito amplo de firma eletrônica e dipondo que “quando a lei requerer a firma de uma pessoa, esse requisito ficará satisfeito em relação a uma mensagem de dados quando: a) for utilizado um método para identificar e para indicar que essa pessoa aprova a informação que figura na mensagem de dados; e, b) se referido método é confiável e apropriado para os fins que se criou ou comunicou a mensagem de dados, a luz de todas as circunstâncias do caso, incluindo qualquer ato pertinente”.

O artigo 3 do projeto letra A do WP.71 indica que “uma firma digital aderida a uma mensagem de dados deve ser considerar autorizada se for possível a sua verfificação de acordo com os procedimentos estabelecidos por uma autoridade certificadora”

Na O.C.D.E.

A Recomendação da OCDE (Organização para a Cooperação e Desenvolvimento Econômico) sobre a utilização da criptografia (Guidelines for Cryptography Policy) foi apovada em 27 de março de 1997. Esta Recomendação não tem força vinculante e assinala uma série de regras que os governos deveriam levar em consideração na formulação da legislação sobre firma digital e terceiros de confiança, com o fim de impedir a adoção de diferentes regras nacionais que poderiam dificultar o comércio eletrônico e a sociedade da informação em geral.

Na Organização internacional de Normas ISSO

Na norma ISSO/IEC 7498-2 (Arquitetura de Seguridade de OSI) sobre a que descansam todos os desenvolvimentos normativos posteriores, regula os serviços de segurança sobre confidencialidade, integridade, autenticidade, controle de

acessos e não repúdio. Através de sua subcomissão 27, SC 27, trabalha em uma norma referente a firma digital.

2.3. Legalidade de documentos com firma digital

O principal problema diz respeito as legislações de muitos países que ainda impõem requisitos de escrita e firma manuscrita como condição de validade e como condição de provas dos contratos e atos jurídicos. Em conseqüência, partindo-se desse ponto de vista legal, e para que estes contratos tenham validade a jursiprudência deverá interpretar o termo firma em sentido latu sensu equiparando a firma digital a firma manuscrita.

Todavia não se tem provado a validez legal da firma digital e ninguém visa ante os Tribunais de Justiça, não existindo por isso garantias jurídicas plenas para seu uso. Não obstante, a firma digital, através do meios criptográficos seja considerada mais segura do que a firma manuscrita, já que não só comporta autenticidade do documento firmado, sua integridade e a certeza de que não foi alterado em nenhuma de suas partes.

Atualmente não existe problema legal para o uso da firma figital por um grupo de usuários, sempre que estes firmem “manualmente” um acordo prévio acerca do uso em suas transações comerciais, assim como o método de firma e os tamanhos (e valores) das chaves públicas a empregar.

3. Autoridade ou entidade de certificação das chaves

A crescente interconexão dos sistemas de informação, possibilitada pela geral aceitação dos sistemas abertos, e cada vez maiores prestações das atuais redes de telecomunicação, obtidas principalmente pela digitalização, estão potenciando formas de intercambio de informática impensáveis até poucos anos. Por sua vez, ele esta conduzindo a uma avalanche de novos serviços e aplicações telemáticas, com um enorme poder de penetração nas emergentes sociedades de informação. Assim o teletrabalho, a teleadministração, o comércio eletrônico, etc.. estão modificando revolucionariamente as relações econômicas, administrativas, laborais de tal forma que em poucos anos serão radicalmente distintas de como são agora.

Todas esses novas aplicações inseridas pela informática na sociedade não poderão ser desevolvidas em sua plenitude se não forem dotadas de serviços e mecanismos de segurança confiáveis. Dentro desse sistema de segurança que indicamos, para que qualquer usuário possa confiar em outro haveria a necessidade de serem estabelecidos certos protocolos, especificamente, as regras de comportamento a seguir. Existem diferentes tipos de protocolos onde há a intervenção de terceiros confiáveis (Trusted Third Party, TTP, na terminologia inglesa). São eles:

a) Os protocolos arbitrados- neles uma TPC ou Autoridade de Certificação participa das transações para assegurar que ambos os lados atuem segundo as pautas marcadas pelo protocolo.

b) Os protocolos notariais- neste caso a TPC, além de garantir a correta operação, também permite julgar se ambas as partes atuaram por direito segundo a evidencia apresentada através dos documentos firmados pelos participantes e incluídos dentro do protocolo notarial. E nestes casos, com a chancela do notário na transação, poderá este atestar sua validade, posteriormente, em caso de disputa.

c) Os protocolos autoverificáveis- nestes protocolos cada parte pode verificar se a outra esta agindo de má-fé, durante o transcurso da operação. A firma digital em si, é um elemento básico dos protocolos autoverificáveis, nesse caso não será preciso a intervenção de uma Autoridade de Certificação para determinar a validade de uma firma.

A Autoridade ou Enidade de Certificação deve reunir os requisitos que determinem a lei, além dos conhecimentos técnicos e experiência necessária, de forma que se ofereça confiança, confiabilidade e segurança. Deverá ser previsto o caso de desaparecimento do organismo certificador e criar algum registro geral de certificação tanto nacional como internacional, que por sua vez fize-se regularmente auditorias nas entidades encarregadas para justamente garantir seu funcionamento, emvirtude da carência de normas que regulem a autoridade ou entidade de certificação.

Para uma certificação de natureza pública, o Notário, no momento de subescrever os acordos de intercâmbio e validação de prova, pode gerar e entregar com absoluta confidencialidade a chave privada. O documento WP.71 de 31 de dezembro de 1996 da Secretaria das Nações Unidas indica em seu parágrafo 44 que as entidades certificadoras devem seguir alguns critérios como:

a) Independência de recursos e capacidade financeira para assumir a responsabilidade pelo risco de perdimento;

b) Experiência em tecnologias de chave pública e familiaridade com procedimentos de segurança apropriadas que garantam a longevidade desses mecanismos;

c) Aprovação da equipamento e os programas;

d) Manutenção de um registro de auditoria e realização de auditorias por uma entidade independente;

e) Existência de um plano para caso de emergência, bem como programas de recuperação em casos de desastres ou depósito de chaves;

f) Seleção e adminsitração de pessoal;

g) Disposições para proteger sua própria chave privada;

h) Segurança interna;

i) Disposições para suspender as operações, incluindo a notificação dos usuários;

j) Garantias e representações (outorgadas ou excluídas);

l) Limitação da responsabilidade;

m) Seguros;

n) Capacidade para a troca de dados com outras autoridades certificadoras;

o) Procedimentos de renovação (no caso de a chave criptográfica tenha sido perdida ou haja ficado exposta).

Podem ainda, as autoridades de Cetificação emitir diferentes tipos de certificados, como:

a) Os certificados de identidade que são os mais utilizados atualmente dentro dos criptosistemas de chave pública e ligam uma identidade pessoal (usuário) ou digital (equipe, softare, etc..) a uma chave pública;

b) Os certifiados de autorização são aqueles que certificam outro tipo de atributos do usário distintos a identidade.

c) Os certificados transnacionais são aqueles que atestam que algum feito ou formalidade aconteceu ou foi presenciada por um terceiro;

d) Os certificados de tempo são aqueles que atestam que um documento existia em um instante determinado de tempo.

O Setor de autoridades de certificação, até hoje, ncontra-se dominado por entidades privadas americanas, já que já existiam iniciativas póprias na União Europeia que ultrapassam as fornteiras de seus países de origem, ou seja, sem sair de outros Esatdos membros.

O termo TTP (Tercera Parte Confiable) a que antes nos referiamos nos indicam associações que ministram uma amplo margem de serviços, frequentemente associados com o acesso legal a chaves criptográficas. Ao que não se descarta que as TTP atue como autoridades de Certificação (AC), as funções de ambas tem sido considerado progressivamente diferentes destacando-se a expressão AC para as organizações que garantem a associação de uma chave pública a certa

entidade, o que por motivos obvios deveria excluir do conhecimento por parte de dita autoridade da chave privada, que é justamente o que supõe deveria conhecer uma TTP.

A Comissão Europeia distingue entre:

Autoridades de certificação (AC): o serviço essencial é “autenticar a propriedade e as características de uma chave pública, de maneira que resulte digna de confiança, e expedir certificados”. Terceiros de confiança (TC).

Oferecem diversos serviços, podendo gozar de acesso legítimo a chaves de cifrado. Uma TC poderia atuar como uma AC.

O que a Comissão pretende é que as legislações sobre firma digital e AC/TC dos distintos países membros é que:

Sejam baseadas em critérios comunitários delimitando suas tarefas – certificação ou administração de chaves – e serviços podendo estabelecer-se prescrições técnicas comuns para as transações por realizadas por intermédio da firma digital através de normas claras em matéria de responsabilidades (usuários frente a AC) erros, etc...

3.1. Funções das autoridades de certificação

As funções de uma autoridade de certificação devem ser, entre outras, as seguintes:

a) Geração e registro de chaves;

b) Identificação de petições de certificados;

c) Emissão de certificado;

d) Armazenamento na AC de sua chave privada;

e) Manter as chaves vigentes e revogá-las;

f) Serviço de diretório.

3.2. Autoridades de certificação

A estrutura e o quadro de funcionamento das autoridades de certificação (public key infrastructure) prevêem uma estrutura hierarquizada em dois níveis: O nível superior só será ocupado por autoridades públicas, que é a que certifica a autoridade subordinada, normalmente privada.

Na Espanha

O Projeto CERES, em que participam o MAP, o Conselho Superior de Informática, o Ministério da Economia e Fazenda e Correios e Telégrafos e contempla o papel da Fabrica Nacional da Moeda e Timbre como entidade encarregada de prestar serviços que garantam a segurança e validez da emissão e recepção de comunicações e documentos por meios eletrônicos, informativos e telemáticos.

Se pretende garantir a segurança e a validez na emissão e recepção de comunicações e documentos por meios eletrônicos, informáticos e telemáticos a as relações entre órgãos da Administração Geral do Estado e outras Administrações, e entre estes e os cidadãos, seguindo diretrizes de legislação prévia (Lei de Regime Jurídico das Administrações Públicas e do Procedimento Administrativo comum, de 1992, e Real Dereto 263/1996.

O objetivo desta autoridade de certificação, assim como as outras entidades comerciais de certificação será o reconhecimento de todos os efeitos legais do certificado digital, o que ainda não se contempla na legislação espanhola.

Os serviços oferecidos são:

Primários- Emissão de certificados, arquivo de certificados, geração de chaves, arquivo de chaves, registro de feitos auditáveis.

Interativos- Registro de usuários e entidades, renovação de certificados, publicação de políticas e modelos, publicação de certificados, publicação de listas de revogação e diretorio seguro de certificados.

De certificação de mensagens e transações – Certificação temporal, certificação de conteúdo, mecanismos de não-repúdio (confirmação de envio e confirmação de recepção)

Da confidencialidade – suporte de mecanismos de confidencialidade, agente de recuperação de chaves e recuperação de dados protegidos

Os notários através de seus colégios respectivos tem a função de adaptar seus modelos aos novo tempo virtuais tornando acessível esse serviço público notarial a quem dele necessite.

Na Itália

A autoridade nacional de certificação é a AIPA (Autorità per l´Informatica nella Pubblica Amministrazione).

3.3. Autoridades privadas de certificação

Na Espanha

Existem focos privados de atividade, vinculados com a confiabilidade. A mais importante é a denominada ACE (Agencia de Certificación Electrónica) que é formada pela CECA, SERMEPA, Sistemas 4B e Telefónica, que é uma Autoridade de Certificação corporativa do sistema financeiro espanhol, também existindo como terceiro de confiança.

En Bélgica

Existe o Terceiro certificador chamado Systèeme Isabel, que oferece serviços certificadores a sócios financeiros e comerciais. A Câmara de Comercio unida a empresa Belsign tem formado um Trusted Third Party na qual a Câmara de Comércio exerce as funções de Registro e Belsign fica com as funções notariais..

Nos Estados Unidos

Utah Digital Signature Trust, One So. Main, Salt Lake City, Utah

ARCANVS, S.A. Sanders Lane, Kaysville, Utah

Na Internet

Existem servidores na internet conhecidos como “servidores de chaves” que recopiam as chaves de milhares de usuários. Todos os servidores de chaves existentes no mundo compartem desta informação, pelo que basta publicar a chave em um de propriedade desse servidor para que em poucas horas esteja disponível para todos os usuários.

Conclusões

Este ensaio teve como um de seus objetivos o de demonstrar as importantes mudanças que tem experimentado a firma desde suas origens até nosso dias e como devemos tratar de adaptar estas transformações a realidade social e deixar a porta aberta para outros futuros avanços, bem como o surgimento de novas tecnologias que sem dúvida virão.

As novas tecnologias da informação e das comunicações, unidas a outras técnicas dão confiabilidade ao documento eletrônico e trazem consigo uma maior segurança mediante o desenvolvimento e extensão de remédios técnicos e procedimentos de controle baseados na criptografia. Esta maior segurança poderá ser alcançada com uma adequação normativa que nos conduza a uma autenticação eletrônica.

O maior entrave existente no que concerne as novas tecnologias da informação diz respeito a não formação e adequação das pessoas e meios a realidade social.

A criação dos notários públicos eletrônicos nos levará a uma avanço e maior segurança com relação a autenticação de documentos que circulem através das meios eletrônicos de comunicação assim como a criação de um fichário público de controle com maiores garantias dos que as atuais.

Uma única Entidade de Certificação de âmbito universal é inviável, portanto deverão existir uma ou várias redes de autoridades nacionais ou setoriais, interrelacionadas entre sí e que por sua vez devem servir os usuários de suas circunscrições.

A firma digital, com as garantias exigidas para a necessária segurança jurídica, abrirá um promissor caminho elastecendo e valorizando ainda mais a fé pública. Entre os objetivos da firma digital está o de conseguir a universalizacão de um modelo de firma eletrônica que possa ser utilizado por uma expressiva quantidade de países sendo elaborada por uma Diretiva Comunitária.

Por fim alertamos para que sejam tomadas como diretrizes para o desenvolvimento da firma digital as seguintes conclusões expostas na IX Jornada Notarial Iberoamericana realizada em Lima, Peru que são as seguintes:

a) Que o notário não pode permanecer alheios aos avanços tecnológicos que possam e devem ser aplicados em sua atividade, na medida que melhore a prestação da função e incremente seguridade jurídica.

b) Que o suporte informático em substituição ao suporte em papel possa ser utilizado na prestação da função notarial, sempre que os avanços na segurança de sua conservação, e da firma eletrônica, eliminam os atuais riscos, e que o conteúdo do documento, com a intervenção do notário, seja assumida pelas partes, mediante sua firma eletrônica e autorizado pelo notário com a sua.

c) As chaves públicas e privadas do notário não podem estar sujeitas a limites temporais de caducidade das chaves dos outorgantes Não devem impedir a obtenção de reproduções de documento.

d) Deve regular-se o documento público eletrônico, sua conservação (protocolo eletrônico) e o sistema de translado de seu conteúdo às partes ou pessoas com direito a conhecê-lo, sem que se possa acessá-lo através da rede sem a intervenção notarial.

e) Os sistemas de comunicação telemática devem servir para estreitar a colaboração entre os notários dos países tradição romano-germânica, a fim de incrementar a segurança jurídica no trafico internacional de documentos.

f) Os avanços informáticos devem servir para facilitar as relações entre os serviços notariais e registrais.

g) O documento público eletrônico, autorizado por notário, deve poder gozar dos mesmos efeitos legitimadores, executórios e probatórios dos documentos em papel".

Bibliografia

ALCOVER GARAU, Guillermo, "La firma electrónica como medio de prueba (Valoración jurídica de los criptosistemas de claves asimétricas)", Cuadernos de Derecho y Comercio nº 13, abril 1994, Consejo General de los Colegios Oficiales de Corredores de Comercio, Madrid. págs. 11 a 41.

ALVAREZ-CIENFUEGOS SUÁREZ, José María, "Las obligaciones concertadas por medios informáticos y la documentación electrónica de los actos jurídicos", Informática y Derecho nº 5, UNED, Centro Regional de Extremadura, Aranzadi, Mérida, 1994, págs. 1273 a 1298.

ALVAREZ-CIENFUEGOS SUÁREZ, José María, "Documento electrónico", Marco legal y deontológico de la Informática, Mérida 19 de septiembre de 1997.

ASÍS ROIG, Agustín de, "Documento electrónico en las Administración Pública", en "Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996, págs. 137 a 189.

BARRIUSO RUIZ, Carlos, "Interacción del Derecho y la Informática", Dykinson, Madrid, 1996.

BARRIUSO RUIZ, Carlos, " Contratación Electrónica", Marco legal y deontológico de la Informática, Mérida, 17 de septiembre de 1997.

BARRIUSO RUIZ, Carlos, "La contratación electrónica", Dykinson, Madrid, 1998.

CAMPS LLUFRIÚ, Mateo; JOYANES AGUILAR, Luis; SANTAELLA LÓPEZ, Manuel "Aspectos sociojurídicos de la contratación electrónica", XII Encuentro sobre Informática y Derecho, Instituto de Informática Jurídica Facultad de Derecho de la Universidad Pontificia Comillas (ICADE), Madrid, 12 de mayo de 1998.

CARRASCOSA LÓPEZ, Valentín; BAUZA REILLY, Marcelo; GONZÁLEZ AGUILAR, Audilio, "El derecho de la prueba y la informática. Problemática y perspectivas", Informática y Derecho nº 2, UNED, Centro Regional de Extremadura, Mérida, 1991.

CARRASCOSA LÓPEZ, Valentín; POZO ARRANZ, Asunción; RODRÍGUEZ DE CASTRO, Eduardo Pedro, "Valor probatorio del documento electrónico", Informática y Derecho nº 8, UNED, Centro Regional de Extremadura, Mérida, 1995, págs. 133 a 173.

CARRASCOSA LÓPEZ, Valentín; POZO ARRANZ, Asunción; RODRÍGUEZ DE CASTRO, Eduardo Pedro, “El consentimiento y sus vicios en los contratos perfeccionados a través de medios electrónicos”, Informática y Derecho nº 12, 13, 14 y 15, UNED, Centro Regional de Extremadura, Mérida, 1996, págs. 1021 a 1037.

CARRASCOSA LÓPEZ, Valentín, “El documento electrónico o informático”, Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, 1995, págs. 43 a 46.

CARRASCOSA LÓPEZ, Valentín, “El documento electrónico como medio de prueba”, en Dogmática penal, política criminal y criminología en evolución de Carlos María Romeo Casabona (ed.), Editorial Comares S.L., Centro de Estudios Criminológicos, Universidad de la Laguna, 1997, págs. 187 a 201.

CARRASCOSA LÓPEZ, Valentín; POZO ARRANZ, Asunción; RODRÍGUEZ DE CASTRO, Eduardo Pedro, “La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos”, Editorial Comares S.L, Granada, 1997.

CASTAÑO SUAREZ, Raquel, “El Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado”, X años de encuentros sobre informática y Derecho 1996-1997, Facultad de Derecho e Instituto de Informática jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, Pamplona, 1997, págs. 413 a 419.

CAVANILLAS MÚGICA, Santiago, “Introducción al tratamiento jurídico de la contratación por medios electrónicos (EDI)”, Actualidad Informática Aranzadi nº 10, enero de 1994.

CAVANILLAS MÚGICA, Santiago, “Régimen jurídico del intercambio electrónico de datos”, Encuentros sobre Informática y Derecho 1995-1996, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, Pamplona, 1996, págs. 103 a 106.

DAVARA RODRÍGUEZ, Miguel Ángel, “Las telecomunicaciones y las Tecnologías de la Información en la Empresa: Implicaciones Socio-Jurídicas”, Informática y Derecho nº 1, UNED, Centro Regional de Extremadura, Mérida, 1992, págs. 27 a 39.

DAVARA RODRÍGUEZ, Miguel Ángel, “El Intercambio Telemático de datos en las transacciones comerciales. Su validez jurídica”, Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, 1995, págs. 58 a 60. Actualidad Informática Aranzadi nº 14, enero de 1995.

DAVARA RODRÍGUEZ, Miguel Ángel, “De las Autopistas de la Información a la Sociedad Virtual”, Aranzadi, 1996.

DAVARA RODRÍGUEZ, Miguel Ángel, “Manual de Derecho Informático”, Aranzadi, Pamplona, 1997.

DAVARA RODRÍGUEZ, Miguel Ángel, “El documento electrónico, informática y telemático y la firma electrónica”, Actualidad Informática Aranzadi nº 24, Julio de 1997.

DAVARA RODRÍGUEZ, Miguel Ángel, “La sociedad de la información y el tratamiento de datos de carácter personal”, Encuentros sobre Informática y Derecho 1997-1998, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, 1998, págs. 19 a 32.

DÁVILA MURO, José; MORANT RAMÓN, José Luis ;SANCHO RODRÍGUEZ, Justo, “Control gubernamental en la protección de datos: proyecto Clipper”, X años de encuentros sobre Informática y Derecho 1996-1997, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, 1997, págs. 25 a 50.

DÁVILA MURO, José; MORANT RAMÓN, José Luis; SANCHO RODRÍGUEZ, Justo, “Autoridades de certificación y confianza digital”, Encuentros sobre Informática y Derecho 1997-1998, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, 1998, págs. 159 a 184.

DOMÍNGUEZ, Agustín, “Transferencia electrónica de fondos y de datos. Protección jurídica de los datos personales emitidos en una operación de pago electrónico”, Encuentros sobre Informática y Derecho 1992-1993, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, Pamplona, 1993, págs. 117 a 132.

GALLARDO ORTIZ, Miguel Ángel, “Criptología; Seguridad Informática y Derecho. Leyes del Ciberespacio”, Informática y Derecho nº 4, UNED, Centro Regional de Extremadura, Aranzadi, Mérida, 1994, págs. 473 a 480.

GALLARDO ORTIZ, Miguel Ángel, “Firmas electrónicas mediante criptología asimétrica”, Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, 1995, págs. 19 a 23.

GALLARDO ORTIZ, Miguel Ángel, “Informatoscopia y tecnología forense”, en “Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996, págs. 21 a 61.

GÓMEZ, José Manuel, “PGP 5”, y World, Año II, número 2, febrero 1998.

GONZÁLEZ AGUILAR, Audilio, “EDI (Echange Data Informatics): Desafío de una nueva práctica”, Informática y Derecho nº 4, UNED, Centro Regional de Extremadura, Aranzadi, Mérida, 1994, págs. 555 a 568.

HERNANDO, Isabel, “La transmisión electrónica de datos (EDI) en Europa (Perspectiva jurídica)”, Actualidad Informática Aranzadi nº 10, enero de 1994.

HEREDERO HIGUERAS, Manuel, “ Valor probatorio del documento electrónico”, Encuentros sobre Informática y Derecho 1990-1991, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia Comillas (ICADE), Aranzadi, 1991.

JULIÁ BARCELÓ, Rosa, “Firma digital y Trusted Third Parties: Iniciativas reguladoras a nivel internacional”, Encuentros sobre Informática y Derecho 1997-1998, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, 1998, págs. 217 a 226.

LARRIEU, J. “Les nouveaux moyens de preuve: pour ou contre l´identification des documents informatiques à des escrits sous seing privé”, Cahiers Lamy du Droit de l´Informatique, noviembre 1988, Pantin.

LÓPEZ ALONSO, Miguel Ángel, “El Servicio EDI y su contratación”, Informática y Derecho nº 12, 13, 14 y 15, UNED, Centro Regional de Extremadura, Mérida, 1996, págs. 1039 a 1053.

MADRID PARRA, Agustín, “EDI (Electronic Data Interchange): Estado de la cuestión en UNCITRAL”, Revista de Derecho Mercantil nº 207 enero-marzo 1993. Madrid, págs. 115 a 149.

MADRID PARRA, Agustín, “Firmas digitales y entidades de certificación a examen en la CNUDMI/UNCITRAL”, Actualidad Informática Aranzadi nº 24, julio de 1997.

MELTZER CAMINO, David, “Comunicado sobre la experiencia obtenida por el Departamento de Ingeniería y Arquitecturas telemáticas de la UPM en el desarrollo de un EDI seguro dentro del proyecto EDISE”, Encuentros sobre Informática y Derecho 1995-1996, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, Pamplona, 1996, págs. 147 a 152.

MORANT RAMÓN, José Luis y SANCHO RODRÍGUEZ, Justo, “Garantías de la firma electrónica de contratos y autenticación de las partes”, Encuentros sobre Informática y Derecho 1992-1993, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad de Comillas (ICADE), Aranzadi, Pamplona, 1993, págs. 107 a 115.

MORANT RAMÓN, José Luis; DÁVILA MURO, Jorge; SANCHO RODRÍGUEZ, Justo, “Registros públicos digitales: el tiempo y su veracidad”, XII Encuentro sobre Informática y Derecho, Instituto de Informática Jurídica Facultad de Derecho de la Universidad Pontificia de Comillas (ICADE), Madrid, 11 de mayo de 1998.

NO-LOUIS Y CABALLERO, Eduardo de, “Internet, germen de la sociedad de la información”, Encuentros sobre Informática y Derecho 1997-1998, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad de Comillas (ICADE), Aranzadi, 1998, págs. 227 a 242.

PAIVA, Mário Antônio Lobato de Paiva. A Mundialização do Direito Laboral. LEX-Jurisprudência do Supremo Tribunal Federal. Ano 23, julho de 2001, n 271. Editora Lex.S/A, São Paulo-SP, páginas 05.

_____. O e-mail como instrumento de divulgação sindical. Jornal Trabalhista Consulex, Ano XVIII, n 863, Brasília 14 de maio de 2001, página 06.

_____. A informatização da justa causa. Jornal Trabalhista Consulex, Ano XVIII, n 849, Brasília 05 de feveeiro de 2001, página 08.

_____. Aspectos Legais na Internet. “O Liberal”, página 02, caderno atualidades, 28 de setembro de 2000.

_____. Os crimes da informática. Jornal “O Liberal”, página 02, caderno atualidades, 12 de fevereiro de 2000.

_____. O impacto da informática nas relações laborais. Repertório da jurisprudência da IOB. N 6, 2O. quinzena de março de 2001.

_____. O Impacto da alta tecnologia e a informática nas relações de trabalho na América do Sul. Justiça do Trabalho: Revista de Jurisprudência Trabalhista, nº 209, mio de 2001, HS Editora, página 7.

_____. O Documento, a Firma e o Notário Eletrônico. Separata da Revista Trimestral de Jurisprudência dos Estados. Vol. 181-182 Abr/Jun 2001 pag 39

_____. O impacto da informática no direito do trabalho. Direito Eletrônico: A Internet e os Tribunais, editora edipro, 1º edição 2001, página 661.

PEÑA MUÑOZ, José de la, “Hacia un marco Europeo para la firma digital y el cifrado”, Revista SIC (Seguridad en Informática y Comunicaciones) nº 28, febrero 1998, págs. 28 a 32.

PERALES VISCASILLAS, Mª del Pilar, “La factura electrónica”, Actualidad Informática Aranzadi nº 24, Julio de 1997.

PÉREZ LUÑO, Antonio-Enrique, “Manual de informática y derecho”, Ariel Derecho, Barcelona, 1996.

PÉREZ LUÑO, Antonio-Enrique, “Ensayos de Informática Jurídica”, Biblioteca de Ética, Filosofía del Derecho y Política nº 46, México, 1996.

PESO NAVARRO, Emilio del, “Resolución de conflictos en el intercambio electrónico de documentos”, en Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996, págs. 191 a 245.

POZO ARRANZ, Mª Asunción y RODRÍGUEZ DE CASTRO, Eduardo Pedro, “Nueva Perspectiva de la contratación ante las modernas tecnologías”, Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, 1995, págs. 11 y 12.

RIBAGORDA GARNACHO, Arturo, “Las Autoridades de Certificación en los nuevos servicios y aplicaciones telemáticas”. Ponencia en las Jornadas sobre Seguridad en Entornos Informáticos. Instituto Universitario “General Gutiérrez Mellado”, Madrid 9-12 de marzo de 1998.

ROUANET MOSCARDÓ, Jaime, “Valor Probatorio Procesal del Documento Electrónico” , Informática y Derecho nº 1, UNED, Centro Regional de Extremadura, Mérida, 1992, págs. 163 a 175.

ZAGAMI, Raimondo, “La firma digitale tra soggetti privati nel regolamento concernente. Atti, documenti e contratti in forma elettronica”, Il Diritto dell´informazione e dell´informatica. Anno XIII nº 6 novembre-dicembre 1997, Editore A. Giuffré, Milano, págs. 903 a 926.

http://dev.abanet.org/scitech/ec/isc/dsgfree.html. The American Bar Association Section of Science and Technology.

http://www.Banesto.es. Ofrece los servicios de Tercero de Confianza a sus usuarios.

http://www.cohasset.com/elec_filing/pag10.html.

http://www.ilpf.org./digsig/intl.htm. Digital Signature Legislation.

http://www.ispo.cec.be/Ecommerce. “A European Initiative in Electronic Commerce”

http://www.itd.umich.edu/ITDigest/0797/news05.html. Digital Signature Laws.

http://www.kriptopolis.com. Criptografía, PGP y seguridad en Internet.

http://www.map.es/csi. Comité Técnico del Consejo Superior de Informática.

http://www.state.ut.us/web/commerce/digsig/dsmain.htm. Utah Digital Signature Program.

(*) Mário Antônio Lobato de Paiva é advogado em Belém; sócio do escritório Paiva & Borges Advogados Associados; Professor da Universidade Federal do Pará; Sócio-fundador do Instituto Brasileiro da Política e do Direito da Informática – IBDI; Membro do Conselho Editorial da Editora Oficina de Livros em Brasília; Autor e co-autor de oito livros jurídicos e uma centena de artigos publicados em revistas especializadas nacionais e estrangeiras; E-mail: malp@interconect.com.br
(*) José Cuervo é advogado; graduado social pela Escola Social de Salamanca; especializado em temas de Direito Informático. Mestre em administração de empresas com especialização em Direito Empresarial pela Fundação Geral da Universidade Politécnica de Madrid.