

NOTAS PROMISSÓRIAS ELETRÔNICAS: Uma análise do endosso eletrônico

Carlos Alberto Rohrmann*

INTRODUÇÃO

- I. UMA RETROSPECTIVA DO DIREITO COMERCIAL
 - A. As notas promissórias e suas origens
 1. O comércio como empreendimento internacional
 2. O uso de notas promissórias como títulos de crédito negociáveis ao longo da História
 - B. As notas promissórias segundo as leis americanas
 - C. A Lei Uniforme de Genebra para Notas Promissórias
 - D. O Direito Comercial e o mundo *online*
 1. O comércio eletrônico e sua regulamentação nos Estados Unidos
 2. Dinheiro digital: circulação de dinheiro no espaço virtual

- II. ANÁLISE DA LEGISLAÇÃO REFERENTE A NOTAS PROMISSÓRIAS QUE EMPREGAM ASSINATURAS DIGITAIS
 - A. Assinaturas digitais e circulação de notas promissórias eletrônicas
 1. Assinaturas digitais *versus* assinaturas escritas, de acordo com o *Statute of Frauds*
 2. Algoritmos de criptografia para assinaturas digitais e sua regulamentação
 - B. *Utah Digital Signature Act*: a primeira lei sobre notas promissórias eletrônicas
 1. Notas promissórias eletrônicas, segundo o *Utah Digital Signature Act*
 2. *Cibernotários* e disposições legais sobre a negociabilidade das notas promissórias eletrônicas
 - C. Propostas de legislação federal sobre *Statute of Frauds* para registros eletrônicos

* Professor da Faculdade de Direito Milton Campos. Bolsista da CAPES-Brasília Brasil durante o Doutorado em Direito na Universidade da Califórnia em Berkeley. Master of Laws (UCLA). Mestre em Direito Comercial (UFMG). Bacharel em Direito (FDMC). Bacharel em Ciência da Computação (UFMG). Membro professor da *Computer Law Association*. Advogado. Este trabalho é baseado no texto da tese de Mestrado defendida na UCLA. Meus sinceros agradecimentos aos seguintes professores da UCLA School of Law: Prof. Stuart Biegel (orientador deste trabalho), Prof. Joel Handler, Prof. Phillip R. Trimble, Prof. Jerry Kang, Prof. Eugene Volokh, Prof. Kenneth L. Karst e Prof. Frederick E. Smith. Meus agradecimentos especiais ao Prof. Dr. Arthur José Almeida Diniz por seu entusiasmo e sempre paciente auxílio em todos os momentos do estudo desta nova área do direito, ao Prof. Luiz Otávio Linhares Renault por seus valiosos ensinamentos e apoio constante à minha pesquisa nos Estados Unidos, ao Prof. Dr. Osmar Brina Corrêa-Lima por seu incentivo de longa data e por suas valiosas e pacientes lições virtuais de direito comercial e ao Prof. Dr. Wille Duarte Costa por sua leitura de uma versão anterior deste trabalho, ainda em inglês e por sua dedicação, pioneirismo e incentivo ao estudo do tema dos títulos de crédito eletrônicos. Finalmente, meus agradecimentos a João Bosco Miquelão por sua preciosa ajuda em todo o *hard job* de tradução deste trabalho. Este artigo está disponível em formato "pdf" no *web site* do Instituto Online para Direito e Informática, em <http://www.home.earthlink.net/~lcgems/NotasProm.pdf>, fev. 2000.

- 1.U.C.C., Artigo 2B: contratos de *software* e licenças de informação
 - 2.Congresso Americano: lei federal para regulamentação de assinaturas digitais
- D. Leis estrangeiras que tratam de promissórias eletrônicas e assinaturas digitais
- 1.*UNCITRAL* e OCED: Tentativa de formular uma legislação uniforme para as assinaturas digitais
 - 2.Europa, Japão e América do Sul
- E. Uma assinatura digital é capaz de identificar, legalmente, quem assina uma nota promissória eletrônica

III. UMA ANÁLISE DAS QUESTÕES DAS NOTAS PROMISSÓRIAS ELETRÔNICAS E ASSINATURAS DIGITAIS SOB O PONTO DE VISTA POLÍTICO

- A. O espaço virtual padece da falta de uma tecnologia de criptografia uniforme para regulamentação do comércio eletrônico
1. Razões segundo as quais a criptografia deve ter a preferência na tarefa de identificar pessoas no *ciberespaço*
 2. Criptografia, privacidade e exportação da criptografia forte
- B. Endosso – como uma nota promissória eletrônica pode circular no espaço virtual
- C. Os certificados estrangeiros devem ser reconhecidos mundialmente para possibilitar a circulação de notas promissórias eletrônicas
- D. O espaço virtual necessita de nova regulamentação para títulos de crédito: uma proposta de emendas à Lei Uniforme de Genebra para notas promissórias eletrônicas

IV. CONCLUSÃO

INTRODUÇÃO

O desenvolvimento da Internet¹ vem sendo responsável pelo surgimento de muitas questões.² Devido à criação de comunidades *online* na nova “era da informação”,

¹ Este artigo assume que a Internet é uma rede mundial de computadores (na verdade, a Internet é uma rede de redes de computadores que utilizam o TCP/IP como protocolo). A Internet cria o "mundo *online*". O espaço virtual (ou *ciberespaço*) é o ambiente da Internet (é o "mundo *online*"). A análise desenvolvida por este texto pode ser aplicada a outras redes de computadores. Maiores informações referentes à Internet e à sua história são encontradas em: CAMERON. *Internet Telephony: Should the Federal Communications Commission Regulate Internet Telephony under Its Regulatory Authority over Communications Law?* <http://www.lawcircle.com/iclo29ii.html>, visitada em março de 1998;

The Internet is essentially a computer network. [The] Internet, as it appears today, grew from the experimental network created by the military called ARPANET, run by the Pentagon's Advanced Research Projects Agency (ARPA).

Outras fontes de informação referentes à Internet estão disponíveis na própria rede. Um bom exemplo é *Internet Society*, onde a história da Internet pode ser achada com maiores detalhes. LEINER, Barry M., et al., *All About the Internet: A Brief History of the Internet*, <http://www.isoc.org/internet/history/brief.html>, visitada em 12 de janeiro de 1999;

The Internet today is a widespread information infrastructure, the initial prototype of what is often called the National (or Global or Galactic) Information Infrastructure. [T]he first recorded description of the social interactions that could be enabled through networking was a series of memos written by J.C.R. Licklider of MIT in August 1962 discussing his "Galactic Network" concept. He envisioned a globally interconnected set of through which everyone could quickly access data and programs from any site. In spirit, the concept was very much like the Internet of today.

² Uma vez que a Internet cresce todos os dias (e de uma forma descentralizada) é difícil determinar quantos computadores estão interligados à rede. É também muito difícil dizer quantas pessoas estão fazendo uso da Internet. Alguns autores chegam a defender a tese de que não é possível determinar o número de usuários da rede ao redor do mundo. NEGROPONTE, Nicholas, *Being Digital* (1995); <http://www.obs-us.com/obs/english/books/nn/bdcont.htm>, visitada em 11 de janeiro de 1999;

Nobody knows how many people use the Internet, because, first of all, it is a network of networks. As of October 1994, more than forty-five thousand networks were part of the Internet. There were more than 4 million host processors (growing at more than 20 percent per quarter), but that is not a helpful measure for estimating the number of users.

Por outro lado, há números relacionados com o crescimento da Internet, número de computadores, redes, *web sites*, dentre outros recursos relacionados à rede: ZAKON, Robert Hobbes, *Hobbes' Internet Timeline v4.0*, <http://www.isoc.org/guest/zakon/Internet/History/HIT.html>, visitada em 8 de janeiro de 1999;

WWW Growth: Date 12/98 - Sites 3,689,227

Hosts: Date 07/98 - Hosts 36,739,000

temas como liberdade de expressão,³ direitos humanos,⁴ e até o direito à privacidade⁵ no espaço virtual⁶ começaram a ser debatidos. Um dos mais importantes tópicos relaciona-se à segurança⁷ da rede, principalmente no que se refere às relações e transações comerciais. O comércio, uma das mais antigas atividades da humanidade, surge agora na

Number of Internet users: This is controversial, and relatively inaccurate, an issue which the author does not want to get flamed or spammed for. His guess would be between 1 (himself) and 6 billion (but again, one never knows if you are a dog on the Net).

³ O tópico da liberdade de expressão na Internet é um tema da maior relevância, todavia não será objeto do presente artigo. Maiores referências: The Harvard Law Review Association, *The Message in the Medium: First Amendment on the Information Superhighway*, 107 Harv. L. Rev. 1062 (1994). O Prof. Eugene Volokh fez uma análise sobre a Internet como um mercado livre de idéias: VOLOKH, Eugene. *Cheap Speech and What It Will Do*, 104 Yale L.J. 1805 (1995).

⁴ COCHRANE. *The Law of Nations in Cyberspace: Fashioning a Cause of Action for the Suppression of Human Rights Reports on the Internet*, 4 Mich. Tel. Tech. L. Rev. 6 (1998);
All human rights regimes recognize a right to freedom of information or expression, although the scope of that rights varies considerably.

⁵ Conforme ROTHFEDER, Jeffrey. *Privacy for Sale: How Computerization Has Made Everyone's Private Life an Open Secret*, Simon and Schuster (1992).

⁶ O glossário de termos de telecomunicações compilado pelo Federal Standard 1037, encontrado em <http://www.its.bldrdoc.gov/fs-1037/> (visitada em 8 de janeiro de 1999) não define o termo "cyberspace."

Por outro lado, o "The Free On-Line Dictionary of Computing", <http://wombat.doc.ic.ac.uk/foldoc/index.html> (visitada em 8 de janeiro de 1999), assim define "cyberspace":

Notional "information-space" loaded with visual cues and navigable with brain-computer interfaces called "cyberspace-decks"; a characteristic prop of cyberpunk SF. At the time of this writing (mid-1991), serious efforts to construct virtual reality interfaces modeled explicitly on Gibsonian cyberspace are already under way, using more conventional devices such as glove sensors and binocular TV headsets. Few hackers are prepared to deny outright the possibility of a cyberspace someday evolving out of the network [...].

O "Internet Literacy Consultants" tem um glossário disponível pela Internet em <http://www.matisse.net/files/glossary.html>, visitada em 8 de janeiro de 1999, que define o termo "cyberspace" referindo ao termo cunhado pelo autor William Gibson:

Cyberspace: Term originated by author William Gibson in his novel *Neuromancer* the word Cyberspace is currently used to describe the whole range of information resources available through computer networks.

Os autores discordam quanto à definição do termo "cyberspace".

Este artigo assume que "cyberspace" é a mídia criada pelas redes de computadores (tais como a Internet e as redes locais de computadores), é o mundo *online*.

⁷ A segurança na Internet é um assunto importante devido ao risco de fraude no ambiente *online*. Este artigo propõe a utilização da criptografia forte como uma solução no sentido de minimizar a incidência de fraude no comércio eletrônico. Uma análise específica referente à segurança da Internet está além do escopo deste texto. Para maiores referências, uma boa fonte é: DIAMOND, Edwin e BATES, Stephen. *Law and Order Comes to Cyberspace*, MIT Technology Review, outubro de 1995.

rede. O comércio eletrônico tem um papel importante na Internet⁸. Há quem diga que esse novo tipo de comércio⁹ provocará o surgimento de um novo Direito Comercial. A discussão sobre os sistemas de pagamento na Internet e como cumprir as leis são questões que desafiam o Direito Comercial.

Ao se falar sobre sistemas de pagamento, devem ser consideradas duas questões principais. A primeira relaciona-se à transferência do próprio dinheiro (por exemplo, a tentativa de se criar o “dinheiro eletrônico”)¹⁰ e a segunda, que será muito discutida neste trabalho, refere-se às operações em que as partes ainda não dispõem de dinheiro. Em outras palavras, uma situação em que não existe dinheiro, mas crédito em curso de transferência. A diferença crucial consiste no fato de que, na transferência de dinheiro, existe total garantia para as partes, visto que a operação inteira é feita de uma só vez; sobre a transferência de crédito, ao contrário, sempre paira uma certa dúvida, porque o crédito se transformará em dinheiro somente após algum tempo e se ocorrer o respectivo pagamento.

⁸ GLADSTONE, Julia Alpert. *Designing Legislation to Facilitate Electronic Commerce on the Internet*, 45-FEB R.I. B.J. 13 (1997);

As of January 1995, it [Internet] has grown to a Network linking 4.85 million computers and over 36.e million users in 85 countries. In 1996, commerce on the Internet is a reality even though it was formally excluded until 1992. Two hundred million people are expected to be "on line" by 1999. It is estimated that by the year 2000 Internet business transactions will generate from \$2 to 5 billion per year.

⁹ NIMMER, Raymond T. e KRAUTHOUSE, Patricia. *Electronic Commerce: New Paradigms in Information Law*, 31 Idaho L. Rev. 937 (1995);

The next century in commercial law and practice will be dominated by electronic commerce and information products. That dominance already exists in several fields; it will expand as information systems continue to pass from being unique or new technology to being commonplace and expected parts of the business world. The future of business lies in the effective handling of information assets. The future of business law lies in developing structures to support this form of commercial practice.

¹⁰ Estas soluções serão discutidas no tópico I.D.2.

Há muito tempo, o crédito vem sendo representado na prática comercial por títulos de crédito¹¹, podendo a nota promissória ser considerada como um exemplo interessante desse tipo de título¹². Uma característica importante desse documento é a de poder circular.¹³ Através de um título de crédito, na ausência de dinheiro em espécie, o valor intrínseco do documento associado ao valor de uma transação comercial pode circular, mesmo quando o que se tem é apenas uma promessa de dinheiro futuro. Logo, tal instrumento, poderoso, deve ser usado nas transações de crédito no *ciberespaço*, porque o comércio eletrônico também carece de um maneira segura e confiável de fazer a transferência do crédito¹⁴.

Versatilidade e criatividade não têm faltado ao comércio, hoje, envolvendo o mundo inteiro. As práticas comerciais, aceitas universalmente, deram origem à “Lex Mercatoria.”¹⁵ Até agora, levando-se em conta o que se fez para regular o comércio

¹¹ Todo título de crédito é criado por lei, alguns exemplos: cheques, letras de câmbio e as notas promissórias.

¹² Outro título de crédito poderia ter sido escolhido para a análise no ambiente da Internet. A escolha da nota promissória deve-se ao fato de ser um título mais simples do que a letra de câmbio e de uso bastante difundido.

¹³ A relação de crédito contida na nota promissória é extraída da relação fundamental que deu origem ao crédito. Há certa independência entre o crédito e a relação jurídica que deu origem ao mesmo (máxime quando há endosso do título e o mesmo circula).

¹⁴ PERRITT Jr., Henry H. *Legal and Technological Infrastructures for Electronic Payment Systems*, 22 Rutgers Computer & Tech. L.J. 1 (1996);

Commercialization of the Internet offers merchants and consumers access to the Internet's worldwide market. Great commercialization depends, however, on the establishment of a reliable and efficient method of payment. Economic transactions on the Internet will have to be at least as transparent, convenient, and secure for consumers and merchants as ordering merchandise by telephone with the use of a credit card.

¹⁵ JESSE Jr., Franklin C. *Breach and Adaptation of International Contracts: An Introduction to Lex Mercatoria*, 22 Denv. J. Int'l L. & Pol'y 209 (1993);

[I]ntroduces the concept of Lex Mercatoria, the notion that business practices can evolve independently of national legal systems to eventually comprise a system of rules that are autonomous in their existence and in their enforcement, from the legal systems of the contracting parties. [T]hat elements of such a law merchant can be found in the development of uniform international laws (e.g., the Vienna Convention on International Sales), standard

eletrônico, pode-se compará-lo à “Lex Mercatoria” - seria uma “Lex Cybercatoria”¹⁶, em que os “cyber-traders” aceitam as regras do comércio eletrônico.¹⁷ Logicamente, disciplinar o comércio eletrônico não é uma tarefa fácil quando não existem instrumentos legais formalmente definidos. Intuitivamente, percebe-se que a formalização de crédito numa nota promissória eletrônica, que pode ser executada por tribunais do mundo inteiro, atende os interesses dos participantes do comércio eletrônico.

No estudo da nota promissória eletrônica, torna-se imperativo observar os padrões estabelecidos e adotados por alguns países do mundo para a nota promissória comum. Deve ser analisada a legislação norte-americana e o modo com que trata a venda de mercadorias, assim como o “Statute of Frauds”.¹⁸ Este artigo demonstra ser possível aplicar o “Statute of Frauds” às notas promissórias através da legislação sobre assinaturas digitais. Por outro lado, muitos países europeus e sul-americanos¹⁹ preferiram

from international contracts or clauses (e.g. INCOTERMS of the International Chamber of Commerce), special standard trade practices within industries.

Outras referências: BERGER, Klaus Peter. *The Lex Mercatoria Doctrine and the Unidroit Principles of International Commercial Contracts*, 28 Law & Pol’y Int’l Bus. 943 (1997) e HIGHER, Keith. *The Enigma of Lex Mercatoria*, 63 Tul. L. Rev. 613 (1989).

¹⁶ “Lex Cybercatoria” refere à “Lex Mercatoria” do comércio eletrônico. Conforme PERRITT Jr., Henry (1996);

Under the proposed United Nations Commission on International Trade Law (UNCITRAL) model statute on EDI, the basic rule would be that the agreement of the parties governs the transaction.

¹⁷ Esta situação ocorre em países que ainda não têm regulamentação específica do comércio eletrônico. O Brasil é um bom exemplo. Embora em 1999 ainda não exista uma lei regulamentando as assinaturas digitais, alguns comerciantes eletrônicos brasileiros utilizam a assinatura digital para validar documentos eletrônicos. Há empresas brasileiras como a “Certisign” que oferecem serviços de “Certification Authority” para validação de documentos eletrônicos. Trata-se de um costume do comércio eletrônico no Brasil, maiores referências estão na Internet em <http://www.certisign.com.br/info/CertiSignCAPolicy.html>, visitada em março de 1998.

¹⁸ Uniform Commercial Code - Article 2, Sales, Formal Requirements; Statute of Frauds, discutido no item II.A.1 deste artigo.

¹⁹ Há estatísticas da Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet - ABRANET, disponíveis em <http://www.abranet.org>, visitada em 13 de janeiro de 1999, que demonstram o crescimento da Internet no Brasil ao longo dos últimos anos da década

adotar a Lei Uniforme de Genebra para Notas Promissórias (L.U.G.) para regular as notas promissórias. Este trabalho demonstrará que a solução proposta aqui não afeta, negativamente, os parâmetros da L.U.G.

Muito se tem dito sobre o *cyberspaço*²⁰ e o seu novo direito. Agora, na condição de ambiente global, o *cyberespaço* clama por uma legislação capaz de prover uma regulação efetiva sobre o maior número possível de jurisdições.²¹ *Links* no *cyberespaço* permitem ao usuário mudar de um país para o outro com um simples clique de *mouse*. As novas regras do *ciberespaço* deveriam ser elaboradas do modo mais uniforme possível. A

de noventa (estes números referem-se apenas ao acesso à Internet através de provedores de acesso):

Número de usuários: 1998 - 2.200.000
1997 - 1.100.000
1996 - 600.000
1995 - 250.000

²⁰ O Prof. Lessig, da universidade de Harvard considera que o espaço virtual é um lugar dotado de relativa liberdade: LESSIG, Lawrence. *The zones of cyberspace*, 48 Stan. L. Rev. 1403 (1996);

Cyberspace is a place. People live there. They experience all the sorts of things that they experience in real space, there. [A]s it is just now, cyberspace is such a place of relative freedom. The technologies of control are relatively crude. Not that there is no control. Cyberspace is not anarchy. But that control is exercised through the ordinary tools of human regulation--through social norms, and social stigma; through peer pressure, and reward. How this happens is an amazing question--how people who need never meet can establish and enforce a rich set of social norms is a question that will push theories of social norm development far.

²¹ Um artigo clássico que aborda as mudanças do Direito em face do surgimento da Internet é de autoria do professor Post, da Temple University of Law. Trata-se de uma referência obrigatória: JOHNSON, David R. e POST, David G. *Law and Borders--The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367 (1996); http://www.cli.org/X0025_LBFIN.html, visitado em 22 de outubro de 1998. Os autores defendem a idéia que a Internet fará surgir um ramo do direito autônomo;

Experience suggests that the community of online users and service providers is up to the task of developing a self-governance system. For example, the current domain name system evolved from decisions made by engineers and the practices of Internet service providers. Now that trademark owners are threatening the company that administers the registration system, the same engineers who established the original domain name standards are again deliberating whether to alter the domain name system to take these new policy issues into account.

legislação sobre as notas promissórias eletrônicas é um exemplo de lei uniforme que emerge do *cyberespaço* para o espaço real.²²

Este trabalho examina o emprego de assinaturas digitais com a finalidade de desenvolver o uso de notas promissórias eletrônicas. As assinaturas digitais podem tornar realidade o emprego de notas promissórias eletrônicas, propiciando ao comércio eletrônico um título de crédito seguro e de circulação mundial. A Parte I analisa os aspectos legais da nota promissória, desde sua origem, na Idade Média, até os dias de hoje, mostrando suas perspectivas diante da regulação do comércio eletrônico. A Parte II faz um exame das assinaturas digitais como solução técnica e legal capaz de identificar, legalmente, o emitente de uma nota promissória eletrônica, propiciando a sua circulação.²³ A Parte III explora as conseqüências do desenvolvimento do comércio eletrônico e o uso de assinaturas digitais, estabelecendo os parâmetros que devem ser observados na criação de uma legislação uniforme para a regulamentação da notas promissórias eletrônicas e do endosso eletrônico.²⁴

Este trabalho conclui que esse novo instrumento legal, implementado com assinaturas digitais, corresponde às necessidades do comércio eletrônico global para a circulação de crédito. Outra conclusão é a de que o espaço virtual, por ser um ambiente

²² Os títulos de crédito são regulados, no Brasil, pela Lei Uniforme de Genebra e nos Estados Unidos pelo UCC. A solução proposta por este artigo para a nota promissória eletrônica pode ser aplicada aos dois sistemas.

²³ A análise deste texto visa a unificação e a padronização da regulamentação das notas promissórias eletrônicas.

²⁴ A busca de uma lei uniforme é uma boa solução para o comércio eletrônico. O ciberespaço é um ambiente internacional e as transações comerciais podem atingir clientes em inúmeros países do mundo. O ideal seria que os documentos eletrônicos, uma vez validados por um país, pudessem ser aceitos nos demais, do contrário, inúmeras barreiras protecionistas surgirão para o comércio eletrônico.

diferente, necessita de novos regulamentos para suas relações, principalmente no que tange ao comércio eletrônico.²⁵

I. UMA RETROSPECTIVA DO DIREITO COMERCIAL

A. As notas promissórias e suas origens

1. O comércio como empreendimento internacional

O comércio²⁶, desde suas origens, tem sido um empreendimento internacional muito difundido. Seus participantes estão sempre em busca de novos mercados para seus produtos. Não existe preconceito em relação ao freguês. Como aumentar as vendas é uma tarefa importante para qualquer negócio, procurar mais clientes significa, sempre, o caminho para o sucesso. O vendedor não se preocupa com a etnia do cliente, religião, ou sua nacionalidade. O comércio tem como meta o lucro. Somente mercados, cada vez maiores, podem proporcionar mais lucros a seus participantes.

²⁵ A doutrina é majoritária no sentido de que os paradigmas do *ciberespaço* são diferentes daqueles do mundo *offline*. Neste momento no qual o *ciberespaço* é usado para atividades comerciais, a questão referente a quais parâmetros jurídicos são (ou devem ser) aplicáveis para a efetiva regulamentação da Internet é de grande importância, referências:

ALLEN, Tom e WIDDISON, Robin. *Can Computers Make Contracts?*, 9 Harv. J.L. & Tech. 25 (1996);

Technological innovation, however, continues apace. Already, we have arrived at the threshold of an era where trading will take place within the global electronic marketplace that is the Internet.

KATSH, Ethan. *Law in a Digital World*, <http://elj.warwick.ac.uk/elj/jilt/BookRev/1terrett/default.htm>, visitada em 10 de dezembro de 1998.

²⁶ Do Latim "cum merx", "com mercadorias".

Não se torna uma tarefa difícil demonstrar que o comércio sempre procurou buscar novos mercados. O mercado pode variar de tamanho – de uma simples vizinhança ao mundo inteiro. Exemplos dessa busca de novos mercados podem ser encontrados na História. Já no princípio da Idade Média, realizavam-se feiras na Europa. Vendedores de diferentes lugares procuravam vender seus produtos a novos clientes. Cidades como Florença e Veneza²⁷ desenvolveram-se muito graças às feiras de comércio. O comércio com o Extremo Oriente obrigou a Europa à realização dos grandes empreendimentos de navegação durante o Século XV. Buscaram-se novos mercados. O comércio das colônias mantinha-se sob o controle das metrópoles européias²⁸, fortalecendo seu poder. Houve conflitos entre as metrópoles européias e suas colônias, que buscavam liberdade de comércio. Os Estados Unidos são exemplo de como as colônias buscaram essa liberdade.²⁹

De volta dessa viagem ao passado, deparamo-nos com a Internet – outra fonte de mercados. Com um pequeno investimento, pode-se colocar um *web site* na Internet. Novamente, a questão aponta para a liberdade de comércio que possibilitará o desenvolvimento de novos mercados, novos clientes. Se de um lado o comércio

²⁷ Estas são exemplos das cidades-estado, de grande importância para o comércio durante o final da Idade Média.

²⁸ ROTUNDA, Ronald D. e NOWAK, John E. *Treatise on Constitutional Law: Substance and Procedure*, 1 Treatise on Const. L. s 4.3 (1992);

There had been no significant commercial problems in the colonies prior to the Declaration of Independence, for Britain had controlled the trade between the colonies themselves as well as that with foreign nations. The acts of the colonial governments were subject to review of the Privy Council, and the British Board of trade supervised the general commercial transactions through the colonies.

²⁹ Id.;

After the signing of the Declaration of Independence there was no central control over commercial transactions in the new states. The individual states were fearful of having their trade subjected to discriminatory restrictions either by states with conflicting commercial interests or a national government that might be controlled by such interests.

eletrônico clama por regulamentação, do outro, ele próprio pede liberdade, rejeitando a interferência³⁰ maciça do governo.³¹

2. Uso de notas promissórias como títulos de crédito negociáveis ao longo da História

Desde suas origens, na Idade Média, as notas promissórias têm-se constituído numa fonte importante de riqueza para a humanidade, uma vez que permite a circulação de crédito através da negociabilidade. Os mercadores usavam tais documentos não só para tornar mais seguro o transporte de valores de uma cidade para outra, em vez de transportar dinheiro vivo, mas, também porque esses títulos eram negociáveis. A negociabilidade é a característica das notas promissórias que tem permitido sua conversibilidade de uma maneira segura e confiável. A negociabilidade é a base dos princípios de que se revestem as notas promissórias, princípios esses idênticos aos dos papéis-moedas e cheques.³² Negociável pode ser entendido como transferível. Transferível, não só o documento, mas também todos os direitos que ele representa.

³⁰ O comércio eletrônico necessita de um mínimo de regulamentação referente aos títulos de crédito, métodos de pagamento e proteção ao consumidor.

³¹ Cuida-se do documento do governo americano: The White House, *A framework for global electronic commerce*, July 1, 1997, discutido no item I.D.1.

³² ROGER, James Steven. *The Myth of Negotiability*, 31 BCLR 265 (1990); "Negotiable" is an ambiguous word. In common speech, "negotiable" is frequently used simply to mean transferable. On the other hand, in the negative form it often carries the connotation that what appears to be a payment instrument is not intended to be genuine, as in the legend "non- negotiable" that one finds on play money, bogus checks used in advertising gimmicks, duplicate copies of money orders, and the like. As that usage indicates, the term has a great deal to do with the use of written instruments as payment devices. Most twentieth century lawyers would probably assert that in legal usage the term has a specific technical meaning: to say that an instrument is negotiable means that it is of appropriate type and form to be governed by the holder in due course rules so that a bona fide

B. As notas promissórias segundo as lei americanas

O U.C.C., artigo 3º, estabelece os pontos mais importantes relativos às notas promissórias e aos títulos de crédito nos Estados Unidos. Todos os estados norte-americanos adotaram o U.C.C., artigo 3º, com pequenas modificações.³³ Ele regulamenta a negociação, a transferência e o endosso³⁴ de títulos de crédito. As

purchaser for value takes the instrument free from all claims to it and free from most defenses of the parties obligated on it. Thus, unlike any other form of property, if a negotiable instrument is stolen and passed to a purchaser who qualifies as a holder in due course, the purchaser takes free of the claim of the true owner. Moreover, if a note or other negotiable instrument gets into the hands of one who qualifies as a holder in due course, it can be enforced against the maker despite most defenses that the maker would have had against the original payee.

³³ Conforme o "Legal Information Institute", *Negotiable Instrument Law Materials*, <http://www.law.cornell.edu/topics/negotiable.html>, visitado em 16 de dezembro de 1998;

Negotiable instruments are mainly governed by state statutory law. Every state has adopted Article 3 of the Uniform Commercial Code (U.C.C.), with some modifications, as the law governing negotiable instruments. The U.C.C. defines a negotiable instrument as an unconditioned writing that promises or orders the payment of a fixed amount of money. Drafts and notes are the two categories of instruments. A draft is an instruments that orders a payment to be made. An example is a check. A note is an instrument that promises that a payment will be made. Certificates of deposit (CD's) are notes. Drafts and notes are commonly used in business transactions to finance the movement of goods and to secure and distribute loans. To be considered negotiable an instrument must meet the requirements stated in Article 3. Negotiable instruments do not include money, payment orders governed by article 4A (fund transfers) or to securities governed by Article 8 (investment securities).

³⁴ Conforme a definição do U.C.C., Article 3, § 3-204, http://www.law.cornell.edu/ucc/3/3-204.html#Indorsement_3-204, visitado em 16 de dezembro de 1998;

§ 3-204. INDORSEMENT.

(a) "Indorsement" means a signature, other than that of a signer as maker, drawer, or acceptor, that alone or accompanied by other words is made on an instrument for the purpose of (i) negotiating the instrument, (ii) restricting payment of the instrument, or (iii) incurring indorser's liability on the instrument, but regardless of the intent of the signer, a signature and its accompanying words is an indorsement unless the accompanying words, terms of the instrument, place of the signature, or other circumstances unambiguously indicate that the signature was made for a purpose other than indorsement. For the purpose of determining whether a signature is made on an instrument, a paper affixed to the instrument is a part of the instrument.

(b) "Indorser" means a person who makes an indorsement.

exigências e definições referentes aos títulos de crédito estão estabelecidas no U.C.C.,
parágrafo 3- 104:

§ 3-104. NEGOTIABLE INSTRUMENT

(a) Except as provided in subsections (c) and (d), "negotiable instrument" means an unconditional promise or order to pay a fixed amount of money, with or without interest or other charges described in the promise or order, if it:

(1) is payable to bearer or to order at the time it is issued or first comes into possession of a holder;

(2) is payable on demand or at a definite time; and

(3) does not state any other undertaking or instruction by the person promising or ordering payment to do any act in addition to the payment of money, but the promise or order may contain (i) an undertaking or power to give, maintain, or protect collateral to secure payment, (ii) an authorization or power to the holder to confess judgment or realize on or dispose of collateral, or (iii) a waiver of the benefit of any law intended for the advantage or protection of an obligor.

(c) For the purpose of determining whether the transferee of an instrument is a holder, an indorsement that transfers a security interest in the instrument is effective as an unqualified indorsement of the instrument.

(d) If an instrument is payable to a holder under a name that is not the name of the holder, indorsement may be made by the holder in the name stated in the instrument or in the holder's name or both, but signature in both names may be required by a person paying or taking the instrument for value or collection.

(b) "Instrument" means a negotiable instrument.³⁵

C. A Lei Uniforme de Genebra para Notas Promissórias

A Lei Uniforme de Genebra para Notas Promissórias (L.U.G.) é o resultado de conferências internacionais³⁶ realizadas no princípio do Século XX na Europa, e foi um tratado³⁷ que experimentou estabelecer regras uniformes para as notas promissórias.³⁸ A respectiva convenção foi assinada em 7 de junho de 1930³⁹, tornando-se a base da legislação adotada na Europa e América do Sul⁴⁰, conseqüentemente, também no Brasil,⁴¹ para as notas promissórias.⁴²

³⁵ Disponível em <http://www.law.cornell.edu:80/ucc/3/3-104.html>, visitada em 26 de janeiro de 1999.

³⁶ Antes da conferência de Genebra, em junho de 1930, houve outras conferências em Haia, na Holanda, realizadas em 1910 e 1912.

³⁷ A doutrina é majoritária no sentido de que os tratados internacionais são a fonte mais importante do Direito Internacional público. CARTER, Barry E. e TRIMBLE, Phillip R. *International Law*, Little, Brown and Company (1995), p. 109;

Whether an instrument is a treaty or not carries a number of significant consequences. Under International Law a treaty creates international legal obligations, with corresponding duties of compliance and remedies, including rights of retaliation, in the event of a breach.

Outra comprovação é o estatuto da Corte Internacional de Justiça, artigo 38(1):

1. The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:

a. international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;

³⁸ A Lei Uniforme em questão trata não só das notas promissórias, mas também de outros títulos de crédito, como cheques e letras de câmbio.

³⁹ Os países que assinaram a convenção em 1930 foram: Alemanha, Áustria, Bélgica, Brasil, Colômbia, Dinamarca, Cidade de Dantzig, Equador, Espanha, Finlândia, França, Grécia, Hungria, Itália, Japão, Luxemburgo, Noruega, Holanda, Peru, Polônia, Portugal, Suécia, Suíça, Tchecoslováquia, Turquia e Iugoslávia.

⁴⁰ Conforme FRAN MARTINS, *Títulos de Crédito*, 11 ed., Rio de Janeiro, Forense, 1995.

⁴¹ Uma importante referência dos aspectos atuais dos títulos de crédito é DUARTE COSTA, Wille. *Atributos, Princípios Gerais e Teorias dos Títulos de Crédito: O Direito que Precisa Ser Repensado*, 4 Rev. Fac. Dir. Milton Campos, 145 (1997).

⁴² O sistema jurídico da América Latina é muito próximo do sistema da Europa continental, daí tantos países latino-americanos serem signatários da LUG.

A L.U.G. preceitua que as notas promissórias devem ser escritas⁴³ e conter a assinatura⁴⁴ do devedor. Esses dois requisitos demonstram uma característica importante das notas promissórias segundo a L.U.G.: elas devem ser emitidas num formato escrito. Ainda de acordo com a L.U.G., a nota promissória deve ser um “papel”.⁴⁵ Durante anos, aceitou-se a idéia de que a promessa deve ser apresentada em formato escrito num papel. De acordo com a L.U.G., se uma pessoa desejar executar uma nota promissória, ela deverá apresentar um “papel” ao tribunal; caso contrário, não haverá como dar início à execução judicial.⁴⁶

D. O Direito Comercial e o mundo *online*

Ao longo dos anos, foi difícil para o comércio determinar os parâmetros legais que deveriam ser aplicados às novas atividades. Agora, com o crescimento do comércio eletrônico, novos tipos de contratos estão surgindo. A partir do momento em que a importância do comércio eletrônico passou a ser reconhecida, muitos governos tentaram estudar legislações para regular esse comércio, de conformidade com um novo direito e com base em novos princípios. A doutrina, majoritariamente, afirma que a Internet trouxe mudanças consideráveis ao comércio e ao direito comercial.⁴⁷

⁴³ L.U.G., Anexo I, Título II, artigo 75, combinado com o artigo 2 do Título I, Anexo I.

⁴⁴ L.U.G., Anexo I, Título II, artigo 75, item 7.

⁴⁵ A noção do "papel" é muito importante para os parâmetros da L.U.G. O título é um documento, uma cártula.

⁴⁶ L.U.G., Anexo I, Título I, artigo 43, combinado com o artigo 77 do Título II, Anexo I.

⁴⁷ Conforme GLADSTONE, Julia Alpert. *Designing Legislation to Facilitate Electronic Commerce on the Internet*, 45-FEB R.I. B.J. 13 (1997);

As we approach the turn of the century, commercial law is struggling to keep pace with the changed expectations that have been necessitated by the emergence of electronic

1. Comércio eletrônico e sua regulamentação nos Estados Unidos

Os Estados Unidos têm assumindo uma posição muito enérgica em relação à regulação do comércio eletrônico.⁴⁸ Depois de reconhecer o potencial desse mercado, a Casa Branca⁴⁹ começou a trabalhar na sua regulamentação. O vice-presidente, Al Gore, vem dedicando parte de seu tempo ao *ciberespaço* e assuntos afins.⁵⁰ Um documento importante relativo à regulamentação do comércio eletrônico nos Estados Unidos, intitulado "A framework for global electronic commerce" (Fundamentos para o comércio eletrônico global)⁵¹ veio a público no dia 1º de julho de 1997.

Esse documento resume a posição dos Estados Unidos relativamente à regulação do comércio eletrônico, destacando-se, entre os pontos mais importantes, aquele em que o governo reconhece o surgimento de um mercado global, o fato de ser reconhecida a

commerce. Our industrial society is giving way to a society which places a high value on one's information and information resources.

⁴⁸ Vários estados norte-americanos já têm leis regulando a assinatura digital. Uma posição mais atual destas leis é encontrada em http://www.mbc.com/ds_sum.html, visitada em 15 de janeiro de 1999. Há também projetos de lei sobre a matéria tramitando no Congresso Americano, conforme II.C deste artigo.

⁴⁹ Uma referência genérica é encontrada em *Information Infrastructure Task Force*, <http://www.iitf.nist.gov/about.html>, visitada em 19 de janeiro de 1999;

The White House formed the Information Infrastructure Task Force (IITF) to articulate and implement the Administration's vision for the National Information Infrastructure (NII). The task force consists of high-level representatives of the Federal agencies that play a major role in the development and application of information and telecommunications technologies. Working together with the private sector, the participating agencies will develop comprehensive technology, telecommunications, and information policies and promote applications that best meet the needs of both the agencies and the country. By helping build consensus on difficult policy issues, the IITF will enable agencies to make and implement policy more quickly and effectively.

⁵⁰ Dentre os artigos do vice-presidente americano: GORE, Albert. *Bringing information to the world: the global information infrastructure*, 9 Harv. J.L. & Tech. 1 (1996).

⁵¹ The White House, *A framework for global electronic commerce*, July 1, 1997.

importância da iniciativa⁵² privada⁵³, e a elaboração de uma legislação específica efetiva por parte dos demais países⁵⁴.

A regulamentação das assinaturas digitais representa um passo importante na legislação norte-americana para a regulamentação do comércio eletrônico. Como será demonstrado a seguir, após esta breve retrospectiva, as assinaturas digitais poderão ser usadas para a emissão e o endosso das notas promissórias eletrônicas. Afinal de contas, o que se chama de nota promissória eletrônica não passa de uma gravação eletrônica composta de *bits*.⁵⁵ Através da assinatura digital, a gravação eletrônica, que representa

⁵² Cf. GIGANTE, Alexander. *Blackhole in Cyberspace: The Legal Void in the Internet*, 15 JMARJCIL 413 (1997);

As long as the development of new telecommunications products was subject to the whim of the regulatory process, however, the evolution of this industry was subject to uncertainty. Now communications business entrepreneurs can be sure that the marketplace and not the government will decide their fate. In summary, the FCC's abstention from the network regulation, the NSF/DARPA's withdrawal from Internet governance, and the government's invitation to private industry to assume responsibility for the Internet's future, mean that the existing Internet groups will no longer have any foundation of federal authority for their activities.

⁵³ Cf. *The National Information Infrastructure: Agenda For Action Executive Summary*, <http://metalab.unc.edu/nii/NII-Agenda-for-Action.html>, visitada em 19 de janeiro de 1999;

The private sector will lead the deployment of the NII. In recent years, U.S. companies have invested more than \$50 billion annually in telecommunications infrastructure -- and that figure does not account for the vast investments made by firms in related industries, such as computers.

⁵⁴ Por outro lado, o governo federal norte-americano tem se retirado da administração da Internet, conforme GIGANTE, nota 52;

[T]his new concern about establishing a legal cover for the Internet's organization derives from the federal government's plan to withdraw from active participation in the Internet's administration. [M]oreover, the FCC, the one federal agency with apparent statutory authority to provide such an umbrella, see e.g., 47 U.S.C. ss 151, 152, has repeatedly refused to enter the field.

⁵⁵ Neste caso, o registro eletrônico é apenas um conjunto de bits que representa o que a nota promissória de papel seria. Nota-se a idéia de que a economia está deixando de ser "atoms oriented" para ser "bit oriented." Maiores estudos acerca desta teoria foram desenvolvidos por NEGROPONTE, Nicholas. *Being Digital*, (1995); <http://www.obs-us.com/obs/english/books/nn/bdcont.htm>, visitada em 11 de janeiro de 1999;

The information superhighway is about the global movement of weightless bits at the speed of light.

uma nota promissória do mundo real, conformar-se-ia com as restrições delineadas pelo “ Statute of Frauds”.⁵⁶

2. Dinheiro digital: uma experiência de circulação de dinheiro no espaço virtual

O principal objetivo deste trabalho é o estudo das notas promissórias de modo a tornar possível a transferência legal de crédito através da Rede. Entretanto, não se pode negar outra finalidade ao presente trabalho: o estudo da transferência de dinheiro através da Internet, isto é, a criação de dinheiro digital⁵⁷, ou, como querem outros, moeda digital.⁵⁸

Uma solução seria a transmissão de *tokens* (cupons pré-pagos)⁵⁹, que teriam o mesmo valor do dinheiro. Esses cupons circulariam na Rede como dinheiro real. Uma

⁵⁶ A idéia básica é a seguinte: a nota promissória eletrônica teria o mesmo valor jurídico de um documento escrito em papel.

⁵⁷ O termo dinheiro digital ("digital money") é muito amplo, outras referências são encontradas em CLARKE, Roger. *The Monster from the Crypt: Impacts and Effects of Digital Money*, <http://www.anu.edu.au/people/Roger.Clarke/EC/Monster.html>, visitada em 3 de novembro de 1997.

⁵⁸ Há empresas nos Estados Unidos que já oferecem o dinheiro digital. Alguns exemplos: *Digicash*, <http://www.digicash.com>, visitada em 2 de janeiro de 1999 e *CyberCash*, <http://www.cybercash.com>, também visitada em 2 de janeiro de 1999.

⁵⁹ Para maiores detalhes, o professor Froomkin da Universidade de Miami é uma referência obrigatória: FROOMKIN, Michael. *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*; 15 J.L. & Com. 395 (1996);

Cryptologists have worked out methods for creating and transmitting tokens of value the digital equivalent of cash and checks over a network like the Internet. This "digital cash", also known as "electronic cash", "E\$," or "e-cash," will allow buying and selling goods or services over the Internet. Any digital cash system vastly expands the commercial possibilities of the Internet, particularly if the system has low transaction costs.

vez comprados, poderiam ser gastos sem revelar a identidade de seu possuidor.⁶⁰ Entretanto, tais cupons continuariam sendo cupons, e não dólares americanos. Do contrário, o banco que os emitisse estaria emitindo dinheiro, o que seria inconstitucional.⁶¹

Como esses cupons não poderiam ser considerados como moeda de curso legal, porquanto não seriam emitidos pelo Governo Federal Norte-Americano,⁶² restaria considerá-los como crédito. Mesmo não carecendo de certificação,⁶³ os cupons ainda continuariam não sendo moeda real. O *ciberespaço* é diferente e necessita de novas regras para a circulação de dinheiro. Se o *ciberdinheiro* é necessário, novas leis federais deverão ser criadas para regular como o governo fará a emissão do dinheiro virtual.

O dinheiro eletrônico não está tendo boa receptividade por parte do mercado. Em 1998, uma companhia que trabalhava com dinheiro eletrônico pediu concordata.⁶⁴

⁶⁰ Mais uma vez, o assunto aqui é a privacidade na Internet. Há organizações *online* tratando do estudo da privacidade das pessoas na Internet, dentre elas temos o *Center for Democracy and Technology*, <http://www.cdt.org>, visitado em 7 de dezembro de 1998.

⁶¹ U.S. Constitution, article I, s 10, cl. 1: somente o governo federal norte-americano pode emitir dinheiro.

⁶² Esta hipótese está além do escopo deste trabalho.

⁶³ Conforme PERRIT Jr., Henry H. *Legal and Technological Infrastructures for Electronic Payment Systems*, 22 Rutgers Computer & Tech. L.J. 1 (1996);

Another way to facilitate commerce on the Internet is to use digital cash ("cybercash"). Cybercash offers several features that make it an attractive alternative to credit card payments over the Internet. For example, cybercash is convenient, easy-to-use, and may not require third-party authorization before it can be used for a purchase. Cybercash can also be implemented so as to permit anonymous use, thereby avoiding the transactional records that conflict with the personal privacy preferences of many credit card users.

⁶⁴ WAYNER, Peter. *Electronic Cash for the Net Fails to Catch On*, The New York Times, November 28, 1998;

The most recent signal came as Digicash, a closely watched electronic payment company based in Palo Alto, California, filed for bankruptcy protection. The company was known for a collection of tools that made it possible for people to spend small amounts of money over the Internet using what is known as digital wallet, software that handles transactions in a manner similar to cash.

II. ANÁLISE DA LEGISLAÇÃO REFERENTE A NOTAS PROMISSÓRIAS QUE EMPREGAM ASSINATURAS DIGITAIS

Este capítulo analisa os aspectos jurídicos que envolvem o emprego de assinaturas digitais em notas promissórias, as fundamentações apresentadas pelos tribunais na análise do *Statute of Frauds* e os fundamentos da atual regulamentação. Primeiramente, será feita uma explanação global da idéia. Como se trata de uma questão técnica muito recente, não foram encontrados casos⁶⁵ que envolvem a matéria.⁶⁶ As leis que tratam de assinaturas digitais, assim como outras fontes legais serão analisadas.⁶⁷ Obedecendo a uma ordem lógica, a primeira lei a surgir nos Estados Unidos sobre o assunto (“Lei sobre Assinatura Digital do Estado de Utah”) será apresentada, assim como algumas propostas legislativas sobre notas promissórias eletrônicas. Ao final, será feita uma breve explanação sobre as leis de diversos países que dispõem sobre o uso internacional de notas promissórias.

Segundo a lógica estabelecida acima, pode-se concluir que as notas promissórias eletrônicas, como os contratos “não-escritos”, são um problema mundial. É fácil concluir que as assinaturas digitais significam a solução para transformar as notas promissórias

⁶⁵ Foram encontrados casos específicos tratando de patentes de assinaturas digitais, todavia ainda não foram encontrados casos referentes a notas promissórias eletrônicas que utilizam assinaturas digitais.

⁶⁶ As pesquisas foram feitas até o mês de novembro de 1998.

⁶⁷ A análise desenvolvida por este trabalho é limitada à utilização da assinatura digital para a implementação segura das notas promissórias eletrônicas. Existem inúmeras outras aplicações das assinaturas digitais que estão além do escopo deste artigo. Um bom exemplo é o uso das assinaturas digitais em documentos oficiais. Recentemente, um comunicado entre o governo americano e o governo da República da Irlanda foi digitalmente assinado, conforme artigo publicado em: *The Irish Times*, *Ahern to seal historic accord with Clinton*, September 1, 1998, <http://www.irish-times.com/irish-times/paper/1998/0901/fin4.html>, visitado em 8 de setembro de 1998;

eletrônicas em documentos confiáveis e reconhecidos pelo maior número possível de jurisdições. Uma convenção internacional sobre esse assunto seria uma providência bem-vinda pelo comércio eletrônico. No último capítulo, apresenta-se um modelo de proposta para um tratado.

A. Assinaturas digitais e circulação de notas promissórias eletrônicas

Antes de iniciar a discussão dos aspectos legais das assinaturas digitais, tornam-se necessárias algumas considerações sobre suas finalidades e sobre alguns aspectos técnicos. Em outras palavras, para que seria necessária uma assinatura digital e que papel ela desempenharia ao substituir uma assinatura escrita? Será feito um breve comentário sobre a tecnologia que se encontra por trás de uma assinatura digital e a discussão de algumas decisões de tribunais (item 2).

1. Assinaturas digitais *versus* assinaturas escritas, de acordo com o *Statute of Frauds*

Da mesma maneira que as transações comerciais do “mundo real”, algumas transações comerciais eletrônicas lidam com vendas de mercadorias⁶⁸ e devem observar

In a ceremony which will make digital history this Friday, the Taoiseach, Mr Ahern, and President Clinton will seal a joint communique on Internet-based electronic commerce, using electronic signatures rather than the traditional press.

⁶⁸ U.C.C., Article 2, § 2-105. Definitions: Transferability; "Goods"; "Future" Goods; "Lot"; "Commercial Unit", http://www.law.cornell.edu/ucc/2/2-105.html#Goods_2-105, visitado em 23 de dezembro de 1998;

(1) "Goods" means all things (including specially manufactured goods) which are movable at the time of identification to the contract for sale other than the money in which the price is to

as disposições estabelecidas no *Statute of Frauds*. Como as notas promissórias eletrônicas podem ser emitidas nessa situação, envolvendo a venda de mercadorias, um estudo jurídico das notas promissórias eletrônicas deveria considerar essa hipótese a fim de, pragmaticamente, atender a realidade do comércio eletrônico nos Estados Unidos.

Definida no artigo 2 do U.C.C.⁶⁹, a exigência de o contrato ter que ser apresentado no formato escrito não foi criada apenas como uma mera formalidade para tornar a vida dos contratantes mais difícil. Ao contrário, a idéia é propiciar segurança às partes envolvidas na transação comercial. Uma vez escrito e assinado o contrato, a gravação poderá ser usada, posteriormente, como prova de intenção dos contratantes. Trata-se de um detalhe muito útil no caso de uma ação judicial.⁷⁰

be paid, investment securities (Article 8) and things in action. "Goods" also includes the unborn young of animals and growing crops and other identified things attached to realty as described in the section on goods to be severed from realty (Section 2-107).

⁶⁹ U.C.C., Article 2 - Sales - § 2-201. Formal Requirements; Statute of Frauds, <http://www.law.cornell.edu/ucc/2/2-201.html>, visitado em 23 de dezembro de 1998;

(1) Except as otherwise provided in this section a contract for the sale of goods for the price of \$500 or more is not enforceable by way of action or defense unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought or by his authorized agent or broker. A writing is not insufficient because it omits or incorrectly states a term agreed upon but the contract is not enforceable under this paragraph beyond the quantity of goods shown in such writing.

⁷⁰ SZAFRAN, Marc E. *A Neo-Institutional Paradigm for Contracts Formed in Cyberspace: Judgment Day for The Statute of Frauds*, 14 Cardozo Arts & Ent. L. J. 491 (1996);

The writing requirement was a means of guarding against fraud perpetrated through perjured testimony, as well as a safeguard for the gullible and the unwary. Under these circumstances, the Statute frequently proved to be a justifiable, effective weapon against perjury and fraud. It facilitated the goal of preventing fraudulent claims from being enforced and protected individuals against questionable or non-existent oral agreements. The means of attaining this objective have historically been achieved by the requirement of evidence that could physically document the formation of a contract between two parties. Because a primary goal of the Statute of Frauds was to promote the use of "writings" when a contract was created, such "writings" could subsequently serve as a record of specific terms agreed upon. This record was used as evidence of a party's objectives and intentions, in addition to serving as a deterrent to fraudulent claims based on alleged oral agreements.

Antes de discutir a questão específica das assinaturas digitais, seria interessante examinar três casos decididos por tribunais norte-americanos, aos quais, tratando-se de documentos escritos, não-assinados, foi aplicado o *Statute of Frauds*.

No primeiro caso, *Spevack, Cameron & Boyd v. National Community Bank of New Jersey*,⁷¹ o tribunal decidiu que a assinatura usada num endosso pode assumir várias formas, mesmo ao se referir a uma única conta mantida pelo correntista no mesmo banco. Um aspecto importante dessa decisão reside no fato de que ela reconhece as inovações trazidas pelo computador e como o *Statute of Frauds* deve ser re-interpretado a fim de se tornar compatível com essa nova era da informação.⁷²

Outra decisão é a do caso *WPP Group USA, Inc. v. The Interpublic Group of Companies, INC.*,⁷³ sobre o qual o tribunal decidiu que um *fax* enviado com a legenda do remetente atendia os requisitos do *Statute of Frauds*.⁷⁴

A terceira decisão refere-se ao caso *Parma Tile Mosaic & Marble Co., Inc. v. Estate of Fred Short, etc., et al.*,⁷⁵ no qual, uma vez mais, em Nova Iorque,

⁷¹ Conforme 291 N.J.Super. 577, 677 A.2d 1168 (1996).

⁷² Conforme 291 N.J.Super. 577, 677 A.2d 1168 (1996);

We also affirm because we are persuaded that the endorsement in the form used by the payee was proper and complete. The "signature" used in an endorsement may take many forms. It need not be a signed name. "A signature is made by the use of any name upon an instrument, or by any word or mark used in lieu of a written signature." N.J.S.A. 12A:3-401(2). In this computer age the use of numbers as a means of identification has become pervasive. Indeed, numbers are more readily recognized and handled than signatures.

⁷³ Conforme 644 N.Y.S.2d 205 (1996).

⁷⁴ Conforme 644 N.Y.S.2d 205 (1996);

The fax was unsigned but on the letterhead of the sender, defendant Interpublic Group of Companies, Inc. In denying defendant's motion for summary judgment, the IAS court found that there was a question of fact as to whether the nonsolicitation agreement was superseded by the purchase agreement, an issue defendant does not pursue on this appeal, and that the fax, although unsigned, was nevertheless adequate for Statute of Frauds purposes because the fax bore the legend of the sender.

⁷⁵ Conforme 155 Misc.2d 950, 590 N.Y.S.2d 1019 (1992);

consideravam-se atendidos os requisitos do *Statute of Frauds* com a transmissão de um *fax*.

Esses casos demonstram que os tribunais americanos já interpretaram o termo “assinatura” de um modo mais amplo, além do antigo conceito de assinatura manuscrita. Há outros casos em que o conceito de “assinatura” também foi interpretado de maneira mais ampla.⁷⁶ Tudo isso mostra uma evolução na interpretação do *Statute of Frauds*, mas não ilustram, suficientemente, quanto os documentos eletrônicos ampliaram o conceito de “documento escrito assinado”. Chega-se ao ponto principal: o comércio eletrônico necessita de uma maneira confiável de assinar documentos. Procurar-se-á demonstrar que a assinatura digital apresenta-se como uma solução interessante, desde que atenda o *Statute of Frauds*, ofereça segurança às partes e utilize uma criptografia forte, conforme detalhado no próximo item deste artigo.

É importante deixar claro que uma assinatura digital não é a imagem digitalizada de uma assinatura escrita à mão.⁷⁷ Embora as assinaturas digitais desempenhem o mesmo papel das assinaturas escritas à mão, elas também são capazes de proteger a integridade do documento eletrônico através de recursos criptográficos. A assinatura digital em um documento eletrônico (uma mensagem de correio eletrônico, por exemplo) depende do texto do documento. Esse texto será usado como dado a ser processado pelo

Upon reconsideration of denial of those motions, the Supreme Court, Queens County, Le Vine, J., held that facsimile transmission constituted enforceable guarantee of subcontractor's debt.

⁷⁶ Conforme 247III.App. 3d 166, 617 N.E.2d 246, 187 III. Dec.38 (1993);

Term "signed" embodies not only act of subscribing document, but also anything which can reasonably be understood to symbolize or manifest signer's intent to adopt writing as his or her own and be bound by it; that may be accomplished in multitude of ways, only one of which is handwritten subscription.

⁷⁷ Conforme SMEDINGHOFF, Thomas J. *Online law: the SPA's legal guide to doing business on the Internet*. The Software Publishers Association, 1997.

algoritmo de criptografia em sua tarefa de gerar a assinatura digital. Uma vez que a menor alteração no texto que foi usado como entrada de dados para a criptografia invalida a assinatura digital, o processo protege o documento assinado digitalmente até contra as alterações mais insignificantes.⁷⁸

O conceito de assinatura digital⁷⁹ pode ser extraído da legislação⁸⁰ ou da doutrina.⁸¹ Assinatura digital é um selo afixado a um documento eletrônico. Esse selo é gerado pela chave privada de quem assina, de modo a comprovar quem é o assinante. A assinatura digital também preserva a integridade dos dados. O sistema também utiliza uma chave pública associada, outorgada por um *Certification Authority*. Essa entidade, além disso, emite um certificado que declara quem assina digitalmente o documento eletrônico.⁸²

⁷⁸ Conforme FROOMKIN, Michael. *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 Or. L. Rev. 49 (1996);

Because the signature uses the original text as an input to the encryption algorithm, if the message is altered in even the slightest way, the signature will not decrypt properly, showing that the message was altered in transit or that the signature was forged by copying it from a different message.

⁷⁹ O termo jurídico "assinatura digital" tem sido objeto de mais de uma interpretação, todavia, consideramos assinatura digital aquela que faz uso de processo de criptografia assimétrica (o que não deve ser confundido com a assinatura eletrônica, esta, apenas um código, um "pin number"). Neste sentido, WEISS, Peter N. *Security Requirements and Evidentiary Issues in the Interchange of Electronic Documents: Steps Towards Developing a Security Policy*, 12 J. Marshall J. Computer & Info. L. 425 (1993);

[T]he term "digital signature" is misleading in many ways.

⁸⁰ *Utah Digital Signature Act*.

⁸¹ WINN, Jane Kaufman. *Couriers Luggage: Negotiable Instruments and Digital Signatures*; 49 S. C. L. Rev. 739 (1998);

For the purposes of this article, a digital signature will be defined as (a) transformation of a message using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine (1) whether the transformation was created using the private key that corresponds to the signer's public key, and (2) whether the initial message has been altered since the transformation was made.

⁸² Conforme FROOMKIN, Michael, nota 79, *supra*.

A Certification Authority (CA) is a body, either public or private, that seeks to fill the need for trusted third party services in electronic commerce by issuing digital certificates that attest to some fact about the subject of the certificate.

O método⁸³ usado para gerar uma assinatura digital é relativamente simples.⁸⁴ Quem assina, criptografa a mensagem do correio eletrônico com sua chave privada⁸⁵ No ato, gera-se um selo criptografado que se embute na mensagem.⁸⁶ Esta, em seguida, é enviada ao destinatário. O destinatário decodificará a mensagem com a chave pública do remetente. Se o processo de decodificação ocorrer, perfeitamente, poder-se-á afirmar, com certeza, que a assinatura, realmente, é de autoria do possuidor da chave privada. Para conferir mais credibilidade ao sistema, o mesmo conta com a certificação de um terceiro - - "The Certification Authority" ("C.A.").

Em outras palavras, se o destinatário tem em mão a mensagem e o respectivo certificado do "C.A.", certificado esse que afirma que o remetente é, realmente, quem ele afirma ser, não existirá dificuldade em reconhecer, legalmente, a validade do documento eletrônico.

⁸³ Este método é a criptografia assimétrica. Maiores referências estão disponíveis no *site* da RSA, empresa americana que detém patentes de assinatura digital: <http://www.rsa.com>, visitada em 23 de novembro de 1998.

⁸⁴ Mais de um sistema computacional pode ser utilizado para implementar a criptografia. Alguns sistemas podem usar o padrão RSA (veja nota 92) que faz uso da criptografia assimétrica e funções computacionais do tipo *hash* para gerar resultados mais rapidamente. Basicamente a função *hash* trabalha com a fatoração de inteiros grandes em números primos. ELDRIDGE, Lonnie. *Internet Commerce and the Meltdown of Certification Authorities: Is the Washington State Solution a Good Model?*, 45 UCLA L. Rev. 1805 (1998);

The most commonly used method of public-key encryption is called "RSA." RSA has been incorporated into a variety of technological applications, including Internet browsers, secure phones, and drop-in computer cards. The fundamental security of the underlying algorithm is unknown, but has been subject of continual study by cryptologists, mathematicians, and amateurs since its release, and no one has publicly announced a quick way to break it.

⁸⁵ Este método requer a infra-estrutura de chaves públicas: *Public Key Infrastructure - PKI*.

⁸⁶ O termo mensagem é utilizado em sentido amplo para englobar arquivos de dados eletrônicos (podendo ser um e-mail, um arquivo do padrão Word, dentre outros).

Algumas formalidades, como as disposições do *Statute of Frauds*,⁸⁷ deveriam ser tidas como satisfeitas, desde que esses documentos eletrônicos estivessem certificados por um “C.A.” reconhecido legalmente. As assinaturas digitais usam um método confiável para “reconhecer uma assinatura”, o qual será demonstrado no próximo capítulo com o estudo de algoritmos de codificação. A lei confere ao “C.A.” a prerrogativa de emitir um certificado de autenticidade. O remetente tem a garantia de que o que escreveu não será alterado, uma vez que o processo de codificação usa todo o texto da nota promissória. Se qualquer dado for alterado, a chave pública não funcionará, corretamente, ao autenticar a assinatura digital. Em outras palavras, a alteração de um simples caractere no documento eletrônico impedirá seu reconhecimento legal.⁸⁸

2. Algoritmos de criptografia para assinaturas digitais e sua regulamentação

⁸⁷ Há autores que discordam desta posição. Trata-se de autores que entendem que o *Statute of Frauds* é uma barreira à utilização dos documentos eletrônicos. Para outras posições, FIELD, Richard L. *Digital Signatures: Verifying Internet Business Transactions*, 471 PLI/Pat 721 (1997); There have been two types of legal barriers to the widespread use of electronic signatures. First, many traditional laws and regulations, written prior to the electronic information age, impose paper-based requirements relating the form of documents and communications. The Statute of Frauds, for example, first enacted in England in 1967 and incorporated into a number of areas of US law, requires that certain documents, to be enforceable, must be in writing.

⁸⁸ Neste caso as assinaturas digitais são ainda mais seguras do que as assinaturas tradicionais uma vez que aquelas protegem a integridade do texto.

Como a criptografia forte⁸⁹ é a solução técnica mais importante que se dispõe para a implementação das assinaturas digitais⁹⁰, torna-se necessária uma análise desse assunto dentro do contexto legal norte-americano.

Atualmente, o algoritmo de criptografia para assinaturas digitais mais importante é o RSA⁹¹, aprovado pelo Departamento de Comércio dos Estados Unidos e usado por repartições do governo sem um prévio exame formal rotineiro.⁹²

RSA é o nome de uma empresa possuidora da patente de um programa de criptografia – sistema de chave pública – que pode ser usado na implementação de assinaturas digitais. Os tribunais reconheceram a legitimidade do dispositivo num caso

⁸⁹ Conforme definição da própria RSA, <http://www.rsa.com/rsalabs/faq/html/1-2.html>, visitada em 4 de fevereiro de 1999;

Encryption is the transformation of data into a form that is as close to impossible as possible to read with out the appropriate knowledge (a key). Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data. Decryption is the reverse of encryption; it is the transformation of encrypted data back into an intelligible form.

⁹⁰ RSA, *idem*;

To sign a message, Alice does a computation involving both her private key and the message itself. The output is called a digital signature and is attached to the message. To verify the signature, Bob does a computation involving the message, the purported signature, and Alice's public key. If the result is correct according to a simple, prescribed mathematical relation, the signature is verified to be genuine; otherwise, the signature is fraudulent, or the message may have been altered.

⁹¹ A "RSA" é uma empresa fundada em 1982 pelos inventores do "RSA Public Key Cryptosystem".

⁹² Referências em: RSA, U.S. *Department of Commerce Approves RSA Digital Signature Standard*, <<http://www.rsa.com/pressbox/html/990203.html>>, visitada em 4 de fevereiro de 1999; SAN MATEO, Calif., February 3, 1999. RSA Data Security, Inc., a wholly owned subsidiary of Security Dynamics Technologies, Inc. (NASDAQ: SDTI), today announced that the U.S. Department of Commerce has adopted RSA's digital signature technology and has approved the modification of the Federal Digital Signature standard (FIPS 186-1) to support the American National Standards Institute (ANSI) X9.31 standard for RSA digital signatures. As a result, government agencies will now be able to use RSA-enabled digital signature applications without having to go through a time-consuming standards waiver process. The approval also lends support for the growing use of RSA security technology across other industry sectors, including financial services, where the ANSI X9.31 standard is used to secure transactions and messages between banks and banking customers.

envolvendo a RSA⁹³ julgado pela justiça federal americana.⁹⁴ Deve-se ressaltar um aspecto importante da decisão: o tribunal considerou o programa patenteado pela RSA como uma solução técnica capaz de implementar as assinaturas digitais.⁹⁵

Uma análise desse caso demonstra que, embora indiretamente, os tribunais⁹⁶ tendem a aceitar a assinatura digital desenvolvida através da chave pública da RSA como uma solução para o reconhecimento legal de documentos eletrônicos.

B. *Utah Digital Signature Act*: a primeira lei sobre notas promissórias eletrônicas

Em 1995, Utah foi o primeiro estado norte-americano a votar uma lei destinada a regular as assinaturas digitais. Muitos outros estados seguiram sua iniciativa.⁹⁷ Por muitas razões, torna-se relevante uma análise do “Utah Digital Signature Act”.

⁹³ Acerca da "RSA Data Security, Inc.", suas origens e estrutura básica, <http://www.rsa.com>, visitada em 4 de fevereiro de 1999.

⁹⁴ No caso 1997 WL 542711 (N.D.Cal.) (1997), as cortes norte-americanas reconheceram a validade da patente da RSA.

The patent discloses a way of transforming plaintext message signals into ciphertext signals and then decoding the ciphertext into plaintext. The patent makes use of the principle that finding prime numbers is computationally easy, but that factoring the product of two such numbers can be computationally infeasible. Using modular arithmetic, the patent exploits the difficulty of factoring prime numbers to generate keys to be used in encoding and decoding devices.

⁹⁵ *Idem*;

The patent also provides a means for using the keys to create digital signatures for purposes of verification.

⁹⁶ Outros casos relativos à patente da RSA para assinaturas digitais: 939 F.Supp. 39 (1996); 1996 WL 88836 (N.D.Cal.) and 1994 WL 669858 (N.D.Cal.).

⁹⁷ Utah Code §§ 46-3-101 to 46-3-504, enacted by L. 1995, ch. 61, encontrado na Internet, visitada em 19 de dezembro de 1998, <http://host1.jmls.edu/cyber/statutes/udsa.html>.

Primeiramente, essa lei vem sendo usada como base para a legislação de outros estados. Em segundo lugar, o estado de Utah já deu autorização para que “Certification Authorities”⁹⁸ realizem seu trabalho. Essas empresas, licenciadas como “Certification Authorities”, estão realizando seu trabalho diário da Internet. Em terceiro lugar, O “Utah Digital Signature Act” contém dispositivos que, especificamente, permitem a circulação de títulos eletrônicos negociáveis, como é o caso das notas promissórias eletrônicas. Assim, nota-se que nos Estados Unidos as notas promissórias eletrônicas podem ser reguladas através de leis estaduais.⁹⁹

1. As notas promissórias eletrônicas segundo o Utah Digital Signature Act

Um dispositivo do “The Utah Digital Signature Act” , especificamente, permite a implementação das notas promissórias eletrônicas ao considerar os efeitos das assinaturas digitais:

46-3-402 - Effect of digital signature.

⁹⁸ State of Utah, *Utah Certification Authority License*, <<http://www.governor.state.ut.us/GOVERNOR/dst-lic.htm>>, visitada em 11 de fevereiro de 1999; Utah Department of Commerce, Division of Corporations and Commercial Code hereby licenses Digital Signature Trust Co. as a licensed certification authority pursuant to the Utah Digital Signature Act, Utah Code Annotated title 46, chapter 3 (1996). This license takes effect beginning 1997 Nov 13 00:00:00 GMT.

⁹⁹ Nos Estados Unidos, a competência para legislar sobre comércio interestadual é do estado, conforme a interpretação da "Commerce Clause" da Constituição dos Estados Unidos da América.

(1) A digitally signed document is as valid as if it had been written on paper.¹⁰⁰

Em outras palavras, reconhece-se a validade de uma nota promissória eletrônica produzida de conformidade com o “The Utah Digital Signature Act”. Existe, ainda, outro dispositivo na citada lei que trata, especificamente, dos títulos de crédito negociáveis, assinados digitalmente, pagáveis ao portador:

46-3-403 Digital signatures making instruments payable to bearer.

Notwithstanding any other provisions of this chapter, a digital signature which would make a negotiable instrument payable to bearer is void, unless the digital signature effectuates either a funds transfer within the meaning of Section 70A-4a-104, or a transaction between banks or other financial institutions.¹⁰¹

O disposto acima torna-se interessante ao admitir a existência de títulos de crédito eletrônicos negociáveis. Somente faz restrição aos títulos pagáveis ao portador. Trata-se de uma boa medida restritiva, uma vez que procura evitar fraudes e insegurança entre as partes que negociam no *ciberespaço*. Essa restrição também consta da “Proposta de Modelo de Legislação” apresentada no item III.D deste trabalho.

Abaixo, um exemplo de nota promissória eletrônica “emitida” de conformidade com o “The Utah Digital Signature Act” (observa-se que a assinatura digital do emitente

¹⁰⁰ Utah Digital Signature Act, part 4, "Effect of Digital Signature", <http://host1.jmls.edu/cyber/statutes/udsa-4.html>, visitada em 8 de fevereiro de 1999.

¹⁰¹ Utah Digital Signature Act, idem.

corresponde ao conjunto de números, letras e símbolos disposto no primeiro parágrafo do documento eletrônico):¹⁰²

<Signed by carlo@malon.com As = Maker Signature =
"234NJ2L;K34YkJH2cV5K04[2U15fT9VU5TOP99CAM1RKIG48VP234Ucx24
9U24UC24UpQb5PMVo29U4">

Promissory Note

I promise to pay to the order of the International Fund Bank one thousand, six hundred dollars and ten cents (\$1,600.10) on or before September 19, 1999, with interest at the rate of ten per cent (10%) per annum. If I default, the holder of this note may accelerate it.

Salt Lake City, January 19, 1999.

S/ Abraham Charles, Maker

*</Signed>*¹⁰³

2. Cibernotários e disposições legais sobre a negociabilidade das notas promissórias eletrônicas

¹⁰² Qualquer pessoa pode ler o texto de uma nota promissória eletrônica. No caso de o emitente necessitar de maior privacidade, ele poderá fazer uso de novo processo de criptografia, conforme GRANT, Gail L. *Understanding Digital Signatures*, CommerceNet Press, 1998;

Digital Signatures do not provide privacy, but that can be easily accomplished with the extra encryption step.

¹⁰³ Exemplos de notas promissórias eletrônicas estão disponíveis no "Utah Digital Signature Act Tutorial".

Já foi dito que as assinaturas digitais necessitam de certificados de autenticidade. “Certification Authorities” são as entidades responsáveis pela emissão desses certificados, as quais são vistas como *cibernotários*.¹⁰⁴ O trabalho dos *cibernotários* é essencial para a circulação das notas promissórias eletrônicas, uma vez que são eles que, em primeira mão, irão certificar a autenticidade do emitente, se a nota promissória foi corretamente transferida de um portador para outro,¹⁰⁵ e, finalmente, se o citado título foi pago. O “The Utah Digital Signature Act” define, distintamente, certificado e “certification authority”¹⁰⁶

C. Propostas de legislação federal sobre *Statute of Frauds* para registros eletrônicos

A partir da metade da década de 90, uma verdadeira onda de legislação sobre assinaturas digitais e assinaturas eletrônicas¹⁰⁷ vem surgindo nos Estados Unidos.

¹⁰⁴ CLOSEN, Michael L. e RICHARDS, R. Jason. *Cyberbusiness Needs Supernotaries*, The National Law Journal, página A19, publicado no dia 25 de agosto de 1997 (segunda-feira), <http://www.ljextra.com/internet/0825cybernotary.html>;

Cybernotaries, or "certification authorities," are about to be unleashed upon the United States marketplace to verify and authenticate digital signatures and electronic documents. They will necessarily possess significant economic power, and that is unsettling prospect, given the historic underqualification of notaries in this country.

¹⁰⁵ Quando uma nota promissória for transferida por endosso, a assinatura digital do endossante deve ser certificada pelo "Certification Authority."

¹⁰⁶ Utah Digital Signature Act, section 46-3-103, <http://host1.jmls.edu/cyber/statutes/udsa-1.html>, visitada em 9 de fevereiro de 1999;

(4) "Certificate" means: (a) a computer-based record identifying a subscriber and containing the subscriber's public key; or (b) if the certificate is issued by a licensed certification authority, a computer-based record identifying a subscriber containing the subscriber's public key, and additional data about the subscriber as specified in Section 46-3-104.

(5) "Certification authority" means a person who issues one or more certificates.

¹⁰⁷ Referência encontrada em: The Bureau of National Affairs, Inc. - BNA. *States Move Forward on Enactment of Electronic Signature Laws, Rules*. The United States Law Week, March 16, 1999. Vol. 67, No. 34, Pg. 2536;

Diversos estados pretendem adotar, ou já adotaram, algum tipo de legislação¹⁰⁸ semelhante à do estado de Utah, como a Califórnia¹⁰⁹ e Nova Iorque. Aquela considerada pela Califórnia (“California Law”) baseia-se no “Uniform Electronic Transactions Act - UETA”, redigido pela “The National Conference of Commissioners on Uniform State Laws - NCCUSL”¹¹⁰. A “The New York Law”¹¹¹ acompanha a idéia de que deve-se conferir ao documento assinado digitalmente a mesma capacidade legal atribuída ao

The transaction of business on the Internet can raise a host of legal issues, including what exactly qualifies as a legally binding signature, an issue that has largely been left to be resolved on a state-by-state basis. A number of states have made significant progress on enacting laws and regulations designed to give legal recognition to electronic signatures. Recently, such laws have been introduced in California and New York, and the Washington state Senate is considering a bill that would further elaborate on the state's existing electronic signature authentication act. In Alabama, the revenue department has proposed a taxpayer electronic signature rule.

¹⁰⁸ Outras iniciativas estaduais: http://www.mbc.com/ds_sum.html, visitada em 3 de março de 1999.

¹⁰⁹ Conforme: The Bureau of National Affairs, Inc. - BNA. Idem. *California Bill Based on Model Law*;

A bill was introduced Feb. 25 in the California state legislature that would give contracts made in electronic form the same weight as those on paper, as envisioned in the National Conference of Commissioners on Uniform State Laws' draft Uniform Electronic Transactions Act (67 U.S.L.W. 2103). California S.B. 820 (Sher and Bowen) is sponsored by Bion M. Gregory, the state legislative counsel, and a member of NCCUSL's UETA drafting committee. The two-sentence bill states: A commercial contract may not be denied legal effect solely because an electronic record was used in its formation. In a transaction, a person may establish reasonable requirements regarding the type of records acceptable to it. The intent of the bill is to clarify the use of electronic forms of communication in contracts. Gregory said if parties enter into a contract electronically, they would be subject to the same laws as contracts made on paper documents. The bill would apply to commercial contracts, but not to consumer transactions. Gregory told BNA that the bill expresses the general principles of UETA and is likely to be amended as the uniform law is finalized later this year.

¹¹⁰ Conforme: The United States Law Week Legal News. *Notable News Developments in the Law Legal News*. August 25, 1998 (67 U.S.L.W. 2103);

Another NCCUSL project, the Uniform Electronic Transactions Act, which deals with general electronic contracting and commerce issues, also received a largely favorable reception when read at the meeting. Both Article 2B and the UETA projects should be ready for consideration by the states in 2000.

¹¹¹ Conforme: The Bureau of National Affairs, Inc. - BNA. Idem. *New York's Legal Recognition*; Legislation has been introduced in the New York State Senate that would provide electronic signatures with the same force and effect as written signatures when certain conditions are met. The Electronic Signatures Act (S. 2155), which is currently before the Senate Judiciary

documento apresentado em papel. Como podem ser aplicados às legislações dos outros estados os princípios do “Utah Digital Signature Act”, esta parte focaliza a questão de modo a buscar uma uniformização em nível federal.

1. U.C.C., Artigo 2B: contratos de *software* e licenças de informação

Há outras áreas nas quais as assinaturas digitais podem ser usadas como ferramenta da lei. Apesar de não se tratar do principal objetivo deste trabalho, não se pode deixar de mencionar as iniciativas já tomadas para demonstrar que o *ciberespaço* vem exigindo algumas mudanças para regulamentação dos contratos eletrônicos.

A revisão do U.C.C. tem como finalidade a adequação das mudanças introduzidas nas práticas comerciais, trazidas pela Ciência da Computação nos últimos vinte anos. O Artigo 8^o¹¹² é um bom exemplo disto. O mesmo já foi revisto duas vezes (1978 e 1994), de modo a poder compatibilizá-lo com o uso das novas tecnologias adotadas por quem trabalha no ramo de seguros nos Estados Unidos.¹¹³ Não se pode deixar de mencionar

Committee, also would grant the New York Department of State authority to issue, suspend, and revoke certificates to verify electronic signatures.

¹¹² U.C.C., Article 8 - Investment Securities, <http://www.law.cornell.edu/ucc/8/overview.html#3-204>, visitado em 3 de março de 1999.

¹¹³ ROGERS, James Steven. *Policy Perspectives on Revised UCC Article 8*, 43 UCLA L. Rev. 1431, 1541 (1996);

The main thing that Revised Article 8 does is adapt to the modern indirect holding system, and state in simple and clear terms, rules that provide security of title to purchasers of investment securities who hold through intermediaries in much the same fashion that negotiability concepts provided security of title for the paper-based securities markets of a previous era or that real estate recording acts provide for the real estate markets.

uma alteração no seu “Statute of Frauds”, que se aproxima daquilo que se estuda neste trabalho.¹¹⁴

A revisão que ora se faz do Artigo 2B do U.C.C.¹¹⁵ pretende abordar os contratos de *software*¹¹⁶ e licenças de informação, tornando os acordos *online* compatíveis com o “Statute of Frauds”.¹¹⁷ Trata-se de uma questão do *ciberspaço* mais relacionada às transações de informação do que ao assunto “transferência de crédito”. De qualquer

¹¹⁴ U.C.C., Article 8, § 8-319. Statute of Frauds. <http://www.law.cornell.edu/ucc/8/8-319.html>, visitada em 5 de março de 1999;

§ 8-319. Statute of Frauds.

A contract for the sale of securities is not enforceable by way of action or defense unless:

(a) there is some writing signed by the party against whom enforcement is sought or by his authorized agent or broker, sufficient to indicate that a contract has been made for sale of a stated quantity of described securities at a defined or stated price;

(b) delivery of a certificated security or transfer instruction has been accepted, or transfer of an uncertificated security has been registered and the transferee has failed to send written objection to the issuer within 10 days after receipt of the initial transaction statement confirming the registration, or payment has been made, but the contract is enforceable under this provision only to the extent of the delivery, registration, or payment;

(c) within a reasonable time a writing in confirmation of the sale or purchase and sufficient against the sender under paragraph (a) has been received by the party against whom enforcement is sought and he has failed to send written objection to its contents within 10 days after its receipt; or

(d) the party against whom enforcement is sought admits in his pleading, testimony, or otherwise in court that a contract was made for the sale of a stated quantity of described securities at a defined or stated price.

¹¹⁵ The United States Law Week Legal News. *Notable News Developments in the Law Legal News*. August 25, 1998 (67 U.S.L.W. 2103);

UCC Article 2B is a joint project of the NCCUSL and the American Law Institute. The newly minted article seeks to update commercial law to address licensing issues related to software agreements and electronic commerce.

¹¹⁶ Trata-se da regulamentação dos contratos de “clickwrap” para licenças de programas de computador através da Internet.

¹¹⁷ Conforme nota 47, *supra*;

The revised U.C.C. Article 2 proposes a repeal of the Statute of Frauds and uses medium neutral terms like “record” instead of “writing.” England eliminated its Statute of Frauds from its Sale of Goods Act in 1954. Given the general decline in the enforcement of a writing requirement in traditional commercial law, it would be inappropriate to expect a writing in the electronic field which functions more efficiently without it.

maneira, é interessante observar que uma das minutas¹¹⁸ do U.C.C. (Artigo 2B), define “Autenticar” como:

*(3) "Authenticate" means to sign, or otherwise to execute or adopt a symbol or sound, or encrypt or similarly process a record in whole or part, with intent of the authenticating person[...]*¹¹⁹

Além das alterações propostas no “U.C.C.”, não se pode deixar de acrescentar que a “American Bar Association” também editou seu “Digital Signature Guidelines¹²⁰, uma demonstração de que os juristas e advogados dos Estados Unidos aprovam a tendência direcionada ao desenvolvimento da assinatura digital e de toda infra-estrutura de criptografia assimétrica.

¹¹⁸ Conforme uma das últimas alterações do "Article 2B": U.C.C., Article 2B, revision, draft of August 1, 1998, <http://www.law.uh.edu/ucc2b/080198/080198.html>, visitada em 7 de março de 1999.

¹¹⁹ U.C.C., Article 2B, SECTION 2B-102.

¹²⁰ Conforme a publicação da "American Bar Association" (ABA), *Digital Signature Guidelines*, <http://www.abanet.org/scitech/ec/isc/home.html>, visitada em 7 de março de 1999. A ABA apóia o uso do modelo PKI para assinaturas digitais como uma forma de tornar o comércio eletrônico mais seguro;

The "Guidelines" also describe a system for ensuring the identity of the holder of a private key, for making digital signatures as usable in commerce and in legal proceedings as a written signature on paper, and for ascribing appropriate responsibility to those engaged in electronic commerce should one of the parties involved deny liability under the transaction. Essential to the process is the concept of a Trusted Third-Party. Such parties will investigate to assure themselves, and the public, of the link between the public key and the holder of the private key, authenticate dates and times of transactions, and electronically publish reports of private keys that are no longer reliable. All of this -- the transaction, the signatures, the authentication, the dating, and so on -- is electronic and requires no paper and no warehouses full of documents, and can be accomplished with the speed that is now essential to world-wide commerce.

2. Congresso Americano: lei federal para a regulamentação de assinaturas digitais

A legislação federal das assinaturas digitais é uma solução ideal para eventuais conflitos entre leis estaduais. Por suposição, uma nota promissória emitida em Utah é negociada e transferida para a Califórnia. No caso de uma ação judicial, uma questão a ser discutida será a do conflito de leis, como no tocante às formalidades referentes à certificação.¹²¹ O conflito de leis nos Estados Unidos¹²² poderia ser minimizado com uma legislação federal que regulamentasse as assinaturas digitais e o licenciamento de “C.As”. A questão da emissão de certificados eletrônicos e sua aplicação no comércio eletrônico deveria ser uma prioridade no cenário das legislações estaduais.¹²³

Há muitos projetos de leis no Congresso dos Estados Unidos destinados a regular as assinaturas digitais¹²⁴ e o arquivamento de documentos eletrônicos, o que demonstra o

¹²¹ Uma proposta de solução dos conflitos de legislação no *ciberespaço* está além do escopo deste texto.

¹²² A referência em discussão neste texto é exclusivamente voltada para o conflito de leis estaduais norte-americanas.

¹²³ Discussões a respeito do tratamento constitucional de leis estaduais comerciais norte-americanas estão disponíveis em CHEMERINSKY, Erwin. *Constitutional Law Principles and Policies*, New York, Aspen Publishers, Inc., 1997, p. 284;

Traditionally, the Supreme Court has identified two major situations where preemption occurs. One is where federal law expressly preempts state or local law. The other situation is where preemption is implied by a clear Congressional intent to preempt state or local law. [A]lthough these categories, or minor variations, are frequently used, they are not distinct. [P]reemption is often a function of both perceived Congressional intent and the language used in the statute or regulation.

¹²⁴ O Congresso norte-americano disponibiliza pela Internet uma lista de projetos de lei em tramitação: <http://thomas.loc.gov>, visitado em 3 de março de 1999; *Computer Security Enhancement Act of 1997* (H.R. 1903), <http://thomas.loc.gov/cgi-bin/query/D?c105:1:./temp/~c105ggoTur:>, visitado em 3 de março de 1999: "It establishes a federal panel to develop digital signature and its required infrastructure";

desejo do governo de regular a Internet¹²⁵ sob uma legislação federal. Este artigo não pretende abordar essa questão, uma vez que alguns projetos poderiam ser alterados e, às vezes, nem mesmo ser aprovados. Torna-se importante deixar claro que existem outras tentativas para regular as assinaturas digitais e a circulação de documentos eletrônicos.

Electronic Financial Services Efficiency Act of 1997 (H.R. 2937), <http://thomas.loc.gov/cgi-bin/query>, visitado em 3 de março de 1999: "It provides for the recognition of digital authentication as an alternative to existing paper-based methods";

Electronic Commerce Enhancement Act of 1997 (H.R. 2991), <http://thomas.loc.gov/cgi-bin/query>, visitado em 3 de março de 1999: "Its purpose is to enhance electronic commerce by requiring agencies to use digital signatures, which are compatible with standards for such technology used in commerce and industry, to enable persons to submit Federal forms electronically, and for other purposes;"

Digital Signature and Electronic Authentication Law (SEAL) of 1998, introduced in the Senate (S 1594), <http://thomas.loc.gov/cgi-bin/query/D?c105:1:/temp/~c105VAn1ri:e913>; visitado em 3 de março de 1999: "It deals with the use of electronic certification by financial institutions";

Paperwork Elimination Act of 1999 (H.R. 439), <http://thomas.loc.gov/cgi-bin/query/D?c106:1:/temp/~c106MrFH0D::>; visitado em 3 de março de 1999: "Even though this bill covers the issue of electronic signatures, it is limited to the electronic filing of forms with federal agencies".

¹²⁵ O Congresso norte-americano tem legislado acerca da pornografia na Internet. Este tipo de legislação pode afetar de forma negativa o comércio eletrônico por impor certas restrições de acesso. Dentre estas leis temos o "Child Online Protection Act - COPA";

The US Congress has passed laws oriented to the regulation of the Internet. The target has been the large amount of pornography available in cyberspace. On the other hand, e-commerce may be affected by those regulations. The most recent example is the "Child Online Protection Act - COPA" (47 U.S.C. 231). It provides that "Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than \$50,000, imprisoned not more than 6 months, or both." It is a statute targeting the e-commerce of pornographic material. It is worthy of note that a lawsuit has been filed challenging the constitutionality of the COPA, under the First Amendment. The US District Court for the Eastern District of Pennsylvania has granted a preliminary injunction for the plaintiffs. One issue in this act that is related to the idea of digital signature and certification, is that the COPA provides as an "affirmative defense" the requirement of an "adult personal identification number" by the defendant. It is easy to conclude that "adult personal identification number" is a very broad term (and one that has been used as one of plaintiffs' arguments in the lawsuit). Another solution to avoid children's access to pornographic material available in cyberspace could be the requirement of a digital signature with an electronic certification of the age. Of course an argument that this requirement is another burden on e-commerce could be made. Nevertheless, it seems much closer to the system that exists in the real world, where merchants ask for customers' identification before selling them liquor.

Por outro lado, o Legislativo percorrerá um caminho incerto. No Congresso Norte-Americano, há muitos projetos sobre questões não-comerciais que dizem respeito a assinaturas digitais e documentos eletrônicos, mas nenhum desses projetos se destina a regular o uso nacional das assinaturas digitais para o comércio eletrônico, de modo a proporcionar uma estrutura única no país para as assinaturas digitais.¹²⁶

D. Leis estrangeiras que tratam de promissórias eletrônicas e assinaturas digitais.

Este capítulo se destina à análise das iniciativas de alguns países para adotar leis referentes a assinaturas digitais e certos tratados sobre legislação uniforme. A análise das legislações estrangeiras¹²⁷ e de outras iniciativas legais vindas de organizações globais torna-se importante para a compreensão global de um Direito Comercial para o *ciberespaço*.

1. UNCITRAL e OCED: Tentativa de formular uma legislação uniforme para as assinaturas digitais

¹²⁶ Congresso Norte-Americano; *Government Paperwork Elimination Act* (S. 2107), <http://thomas.loc.gov/cgi-bin/query/D?c105:1:./temp/~c1054ZqTJv::>, visitado em 3 de março de 1999; "It covers electronic signatures and the electronic filing of forms with federal agencies"; *Internal Revenue Service Restructuring and Reform Act of 1997* (H.R. 2676), <http://thomas.loc.gov/cgi-bin/query/D?c105:1:./temp/~c105hqn8ca::>, visitado em 3 de março de 1999; "This act is limited to electronic filing of income tax returns".

¹²⁷ BOSS, Amelia H. *Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform*, 72 Tul. L. Ver. 1931 (1998).

A *UNCITRAL (The United Nations Commission on International Trade Law)* idealizou um modelo de legislação para o comércio eletrônico. O projeto incorpora a idéia de uma gravação eletrônica em substituição do papel-documento. Uma breve análise de seus artigos sétimo¹²⁸ e oitavo¹²⁹ demonstra que os mesmos podem combinar-se de modo a alcançar a validação da nota promissória eletrônica. Essa Legislação Uniforme poderia ser facilmente aceita pelos países-membros desde que essa regulação não interferisse com os requisitos internos de cada membro para a validação das assinaturas digitais. Acrescenta-se que uma regulação uniforme seria uma solução muito bem-vinda para o comércio eletrônico.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE)¹³⁰ é um organismo internacional que cumpre um novo papel muito importante no âmbito do

¹²⁸ UNCITRAL, *Model Law on Electronic Commerce*, <http://www.un.or.at/uncitral/en-index.htm>, visitada em 11 de fevereiro de 1999;

Article 7. Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

- (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
- (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

¹²⁹ UNCITRAL, *idem*;

Article 8. Original

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

- (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and
- (b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

¹³⁰ Maiores informações referentes à OCDE estão disponíveis na página da organização na Internet: <http://www.oecd.org>, visitada em 12 de fevereiro de 1999;

The Organisation for Economic Co-operation and Development has been called a think tank, monitoring agency, rich man's club, an unacademic university. It has elements of all, but none of these characterisations captures the essence of the OECD. The OECD groups 29 member

Direito Internacional. Seu propósito não é o estabelecimento de “leis” propriamente ditas, mas a proposição de “soft law”.¹³¹ “Soft law” são leis informais. Entretanto, como muitos países¹³² são membros de organizações como a OCDE, esses países, geralmente, cumprem as leis dessas entidades. A exemplo da UNCITRAL, a OCDE baixou normas para a criptografia de assinaturas digitais.¹³³ A OCDE defende o uso da criptografia e assinaturas digitais contra fraudes no comércio eletrônico.

countries in an organisation that, most importantly, provides governments a setting in which to discuss, develop and perfect economic and social policy. They compare experiences, seek answers to common problems and work to co-ordinate domestic and international policies that increasingly in today's globalised world must form a web of even practice across nations. Their exchanges may lead to agreements to act in a formal way - for example, by establishing legally-binding codes for free flow of capital and services, agreements to crack down on bribery or to end subsidies for shipbuilding. But more often, their discussion makes for better informed work within their own governments on the spectrum of public policy and clarifies the impact of national policies on the international community. And it offers a chance to reflect and exchange perspectives with other countries similar to their own.

¹³¹ A doutrina diverge quanto o papel da "soft law." Alguns autores encaram "soft law" como uma nova e importante tendência dentro do Direito Internacional. Outros pensam que "soft law" é apenas uma boa idéia que os diversos Estados respeitam se quiser. Conforme CARTER, Barry E. e TRIMBLE, Phillip R. *International Law*, Little, Brown and Company, 3. Ed. (1999);

Now international law is increasingly being made by international organizations and important international norms are being created by private actors as well. These norms are not legally binding as a matter of formal law; they do not fit the traditional process for law-making which is largely limited to treaties and customary law. [I]nternational organizations [have a] role in the development of "soft law."

¹³² OCDE, *Membership*, <http://www.oecd.org/about/general/member-countries.htm>, visitada em 12 de fevereiro de 1999;

The OECD brings together 29 countries sharing the principles of the market economy, pluralist democracy and respect for human rights. The original 20 members of the OECD are located in Western countries of Europe and North America. Next came Japan, Australia, New-Zealand and Finland. More recently, Mexico, the Czech Republic, Hungary, Poland and Korea have joined.

¹³³ OCDE, *Cryptography policy: The Guidelines and The Issues*, <http://www.oecd.org/dsti/sti/it/secur/prod/GD97-204.htm>, visitada em 12 de fevereiro de 1999;

An important application for public key cryptography is “digital signature”, which can be used to verify the integrity of data or the authenticity of the sender of data. In this case, the private key is used to “sign” a message, while the corresponding public key is used to verify a “signed” message. Public key cryptography offers the benefits of confidential transmissions and digital signature in an open network environment in which parties do not know one another in advance. This development allows for broader applications of cryptographic methods, and this -- together with increases in computer power and decreases in computer prices -- has moved cryptography into the private sector domain.

É importante enfatizar que mais de um organismo jurídico aceitou a idéia de que as assinaturas digitais são a solução para a migração de muitos documentos em papel (e suas funções legais) para o *ciberespaço*. Além disso, a OCDE defende a importância de se implementar o comércio eletrônico¹³⁴ de acordo com uma política confiável a fim de derrubar algumas barreiras, tais como os riscos de falsificação que os usuários ainda enfrentam. Certamente, tal fato demonstra que há uma tendência no sentido de que o Direito Comercial Eletrônico seja implementado no *ciberespaço*, internacionalmente, de uma maneira uniforme, por exemplo, através de tratados.

2. Europa, Japão e América do Sul

A maioria dos países europeus e sul-americanos adota o sistema do Direito Civil.¹³⁵ Alguns desses países vêm trabalhando em leis destinadas a oferecer base legal às gravações eletrônicas que substituem os documentos em papel. Enquanto que, nos Estados Unidos, a maior barreira à nota promissória eletrônica é representada pelo “Statute of Frauds”, na maioria dos países que adotam o Direito Civil essa barreira é a L.U.G.¹³⁶ Todavia, o primeiro passo¹³⁷ para a implementação da promissória eletrônica nos países que adotam o Direito Civil é uma efetiva legislação das assinaturas digitais. Este trabalho procura demonstrar que o uso de assinaturas digitais não é uma solução doméstica restrita a um ponto de vista paroquial dentro dos Estados Unidos, mas, sim

¹³⁴ OCDE, *Dismantling the Barriers to Global Electronic Commerce*, <http://www.oecd.org/dsti/sti/it/ec/prod/DISMANTL.HTM>, visitada em 28 de fevereiro de 1999.

¹³⁵ A mais importante exceção é a Grã Bretanha.

¹³⁶ A barreira da L.U.G. é solucionada no item III.D.

¹³⁷ O próximo passo seria uma emenda à L.U.G.

uma solução que poderá ser empregada no mundo inteiro para as leis do comércio eletrônico e para os títulos de crédito eletrônicos.

A Comunidade Européia vem trabalhando na regulamentação das assinaturas digitais e criptografia. Apesar de o Parlamento Europeu não haver traçado diretrizes específicas sobre essa questão,¹³⁸ muitos países desse continente já implementaram suas leis para regular as assinaturas digitais. O exemplo mais marcante é o da Alemanha,¹³⁹ que já tem a sua lei sobre assinaturas digitais. Fora da Comunidade Européia, mas ainda dentro do escopo da L.U.G., a Rússia se destaca como um país que já possui uma legislação¹⁴⁰ sobre PKI que reconhece a validade legal das assinaturas digitais. Aquele país também já dispõe de uma legislação sobre o uso de documentos eletrônicos emitidos por sua Comissão Federal de Mercados Mobiliários.¹⁴¹

¹³⁸ Conforme: European Commission. *Common Framework for Electronic Signatures*, <http://www.ispo.cec.be/eif/policy/com98297.html>, visitada em 4 de março de 1999;

[To] ensure the proper functioning of the Internal Market in the field of electronic signatures by creating a harmonised and appropriate legal framework for the use of electronic signatures within the European Community and establishing a set of criteria which form the basis for legal recognition of electronic signatures.

¹³⁹ A lei alemã pode ser encontrada na Internet: German Digital Signature Law, <http://www.iid.de/rahmen/iukdgbt.html>, visitada em 4 de março de 1999.

¹⁴⁰ Conforme o RF Federal Act No. 24-FZ, adotado em 25 de janeiro de 1995 pelo Duma. Conforme Westlaw, 1995 WL 139853 (Rus.Legis.);

The legal force of a document stored, processed and transmitted by means of automated information and telecommunications systems may be confirmed by an electronic digital signature. The legal force of the electronic digital signature shall be recognized where the automated information system contains technical-programme means making it possible to identify the signature in the regime established for the use thereof.

¹⁴¹ Russia, Federal Securities Market Commission Decree No. 9, encontrado no Westlaw, 1997 WL 241126 (Rus.Legis.);

[R]ules of performance of operations in acceptance for safe custody or withdrawal from safe custody of securities, and also operations in the transfer, conveyance and restriction of rights with respect to securities accepted for safe custody; official instructions for employees and heads of sections of depositaries, and also for persons attesting documents with digital electronic signature.

A América Latina não dispõe de leis para as assinaturas digitais, as quais vêm sendo usadas em alguns países como uma “prática do *ciberespaço*”. A Argentina tomou uma iniciativa.¹⁴²

Há, também, projetos de leis similares na Colômbia¹⁴³ e no Congresso Brasileiro.¹⁴⁴

O Japão, outro país que também adota o sistema Lei Uniforme de Genebra para Notas Promissórias, adotou o *Certificate Authority Guidelines*.¹⁴⁵ Trata-se de um

¹⁴² República Argentina, *Decreto presidencial No. 427/98*, <http://www.sfp.gov.ar/decree427.html>, visitada em 5 de março de 1999. Disponível também em: <http://www.mbc.com/legis/argentina.html>, visitado em 5 de março de 1999;

On April 16, 1998, the President of Argentina signed Decree No. 427/98, creating a Public Key Infrastructure and providing for the use of digital signatures in the National Public Administration. The Decree provides that the use of digital signatures is authorized for a two-year period and shall have the same effect as a written signature for implementation of internal activities of the National Public Sector, including both centralized and decentralized administrative bodies, state-owned companies, government partnerships, public limited companies in which the government is a majority shareholder, state-owned banks and financial institutions, "and any other body in which the government or its decentralized institutions have a controlling interest." A "digital signature" is defined as "the result of the transformation of a digital document through the use of an asymmetric cryptosystem and a hash result, in such a way that a person that has the initial digital document and the public key of the signer can positively determine whether: (1) The transformation took place through the use of a private key that corresponds with the public key of the signer; (2) the digital document has been otherwise modified since the transformation took place.

¹⁴³ A Colômbia tem um projeto baseado no Model Law da UNCITRAL discutido no item II.D.1. Colômbia, *Draft Proposal of Law on Electronic Commerce, Digital Signatures and Certification Authorities*, http://www.qmw.ac.uk/~tl6345/colombia_sp.htm, visitado em 5 de março de 1999.

¹⁴⁴ No Brasil temos os projetos: 22/96 (senado) e 2644/96 (Câmara dos Deputados), dentre outros encontrados em <http://www.home.earthlink.net/~lcgems/Projetos.htm>.

¹⁴⁵ Conforme: Summary of Certification Authority Guidelines V 1.0, http://www.ecom.or.jp/ecom_e/, visitada em 5 de março de 1999;

Work process: Certification Authority (CA) WG focuses on operating policy for the CAs that issue digital certificates to verify that the entities involved in electronic transactions in open network environments such as the Internet are truly working to prevent parties on either end of a transaction from impersonating others.

importante projeto para o comércio eletrônico de autoria do *Electronic Commerce Promotion Council of Japan*.¹⁴⁶

E. Uma assinatura digital é capaz de identificar, legalmente, quem assina uma nota promissória eletrônica

O papel mais importante e relevante desempenhado por uma assinatura digital junto a uma nota promissória é a sua capacidade de identificar, legalmente, quem assina¹⁴⁷ o documento eletrônico. Algumas particularidades tornam o *ciberespaço* diferente do mundo real, considerando-o um lugar para a circulação de notas promissórias. Essas particularidades são: apesar de fazer negócios no *ciberespaço*, ninguém, fisicamente, encontra-se presente no computador do outro;¹⁴⁸ algumas interações podem ser realizadas entre dois computadores sem a intervenção direta dos respectivos usuários;¹⁴⁹ qualquer um que possuir um *web site* na Internet pode estar em

¹⁴⁶ Conforme a *web page* do "Electronic Commerce Promotion Council of Japan", http://www.ecom.or.jp/ecom_e/, visitada em 5 de março de 1999.

¹⁴⁷ Obviamente, quem assina pode ser tanto o emitente, quanto um endossante, ou avalista do título de crédito.

¹⁴⁸ A Internet permite a "projeção" uma pessoa de seu computador para outro. Maiores pesquisas acerca da teoria da "projeção": MITCHELL, William J. *City of Bits: Space, Place, and the Infobahn*, MIT Press, 1995, < http://mitpress.mit.edu/e-books/City_of_Bits/contents.html>, visitada em 31 de janeiro de 1999;

Without leaving my office at MIT, I teach a class in Singapore. Like the cruelly immobilized physicist and the venturesome musician, I extend the limited affordances of my fleshy sensors and effectors through some ingenious electronic jiggery-pokery; a window opens on my computer screen and a distant video camera temporarily becomes my eyes and ears.

¹⁴⁹ O que aconteceria se um computador emitisse uma nota promissória sem a presença humana? Alguns autores já começam a trabalhar este tema: ALLEN, Tom e WIDDISON, Robin nota 25, supra;

Despite slow and halting progress in artificial intelligence ("AI") research, [c]omputer systems are now emerging that can operate not just automatically but autonomously. Autonomous machines can learn through experience, [m]odify the instructions in their own programs, and even devise new instructions. [T]hey then can make decisions based on these self-modified or

todos os lugares ao mesmo tempo;¹⁵⁰ fazer alterações em um documento eletrônico torna-se uma tarefa relativamente simples.¹⁵¹ Todos os quatro tipos de problemas assim enumerados estão, de algum modo, relacionados às notas promissórias eletrônicas e podem ser resumidos numa questão maior: prover identidade de uma maneira segura. É o que se depreende de uma análise do assunto.

Prover uma certificação¹⁵² de quem assina é fator crucial para prova da intenção de quem emite um documento eletrônico. Desde os tempos a que se referem os casos aqui estudados anteriormente, o legislativo vem demonstrando uma certa preferência para o uso das assinaturas digitais em títulos de crédito eletrônicos.

self-created instructions. [I]f autonomous computers are able to learn and modify their own behavior in this way, a reasonable implication must be that they are capable of manifesting (or, at least, appearing to manifest) human cognitive processes that are associated with the exercise of free will.

¹⁵⁰ Esta situação leva a um problema jurídico: uma vez que a pessoa pode estar, ainda que virtualmente, em qualquer lugar, a quais leis ela estará sujeita? Em Estados Federativos está questão ainda é mais complexa. Especificamente no caso dos Estados Unidos, alguns autores já debatem o tema: HERNANDEZ, Dennis H.e MAY, David. *Personal Jurisdiction and the Net: Does Your Website Subject You to the Laws of Every State in the Union?*, Los Angeles Daily Journal, July 15, 1996, < <http://www.gseis.ucla.edu/iclp/dhdm.html>>, visitada em 24 de dezembro de 1999;

For a fee as little as \$50 a month, businesses can have their own website and, potentially, reach a market of more than 25 million Internet users. However, publishing globally may expose a business to risks in other jurisdictions and countries that it did not expect or anticipate. Does the mere use of the Internet, by maintaining a Website, constitute a presence or contact sufficient to confer jurisdiction?

¹⁵¹ FROMKIN, Michael nota 79, supra;

Internet Commerce: Fraud's Playground? Judging by the low amount of civil fraud (as opposed to crime) to date, the Internet's reputation as fraud's playground is undeserved. Yet, this may be the rare case in which expectations accurately predict a possible future. While there may be a great deal of Internet advertising and information exchange, there are still relatively few transactions for value over the Internet. As the amount of Internet commerce grows, the opportunities for fraud may grow unless security and authentication measures also grow.

¹⁵² Cabe resaltar que a certificação deve ser entendida como uma autenticação devidamente emitida por um terceiro, de acordo com as formalidades legais.

III. UMA ANÁLISE DAS QUESTÕES DAS NOTAS PROMISSÓRIAS ELETRÔNICAS E ASSINATURAS DIGITAIS SOB O PONTO DE VISTA POLÍTICO.

A. O espaço virtual necessita de uma tecnologia de criptografia uniforme para regulamentação do comércio eletrônico

Sob o ponto de vista político, a regulamentação da tecnologia que se encontra por trás das assinaturas digitais deve possuir parâmetros destinados a permitir o emprego amplo das assinaturas digitais. Como seu uso representa um modo de identificar quem se encontra por trás de um determinado computador, a solução ideal clama por uma tecnologia confiável e uniforme. A criptografia pode ser essa tecnologia. Por outro lado, há que superar alguns obstáculos.

1. Razões segundo as quais a criptografia deve ter a preferência na tarefa de identificar pessoas no *ciberespaço*

Um elemento importante, que se relaciona a tudo que já foi dito acerca do comércio eletrônico e de suas implicações, é a identidade. A criptografia é uma solução que confere mais segurança às transações do comércio eletrônico. O *ciberespaço* carece

de um método seguro para identificação. Mais de uma solução encontra-se disponível.¹⁵³ O modelo da chave pública criptografada é uma boa solução porque é mais segura do que, por exemplo, um simples código (número-chave), que “viajará”¹⁵⁴ no espaço.

Há outras soluções propostas. Como exemplo, pode-se citar o uso de uma nova técnica conhecida como “biometria”¹⁵⁵, também empregada para certificação.¹⁵⁶ O método baseia-se nas características das pessoas. Primeiramente, “escaneam-se” as impressões digitais, rosto ou outros dados pessoais. A seguir, esses dados são criptografados e produzem um resultado. Futuramente, se o interessado necessitar de uma certificação, ele, simplesmente, oferecerá seus dados para comparação com o resultado criptografado. Ainda uma promessa, trata-se de um método que também poderá ser usado junto com o sistema de assinaturas digitais, tornando o procedimento ainda mais seguro.

2. Criptografia, privacidade e exportação da criptografia forte

Outros dois assuntos importantes relacionados ao Direito Comercial no *ciberespaço* são a privacidade¹⁵⁷ e o debate acerca da política norte-americana sobre a

¹⁵³ Conforme HILLER, Janine S. e COOK, Don Lloyd. *From Clipper Ships to Clipper Chips: The Evolution of Payment Systems for Electronic Commerce*; 17 J.L. & Com. 53 (1997).

¹⁵⁴ Códigos trafegam pela Internet e podem ser interceptados, daí não serem a melhor opção para a segurança do comércio na rede.

¹⁵⁵ Definição encontrada na revista "Computer World", October 12, 1998; Biometrics literally means "life measurement". In the realm of security, it refers to automated methods for identifying people based on their unique physical characteristics or behavior traits. Types of biometrics methods include fingerprint scanning, iris scanning, handwritten analysis, handprint recognition and voice recognition.

¹⁵⁶ JUENEMAN, R.R. e ROBERTSON Jr., R.J. *Biometrics and Digital Signatures in Electronic Commerce*; 38 Jurimetrics J. 427 (1998).

¹⁵⁷ Um artigo que cobre o tema da privacidade no *ciberespaço* de forma abrangente é KANG, Jerry. *Cyberspace Privacy: A Primer and Proposal*; 26-WTR Hum. Rts. 3 (1999);

política de exportação de criptografia forte. Há um projeto de lei no Congresso Norte-Americano ¹⁵⁸ que aborda esta última questão.

A criptografia forte é uma importante ferramenta para se garantir a privacidade ¹⁵⁹ no *ciberespaço*. Por outro lado, se o governo exigir o registro público de todas as chaves privadas, o uso da criptografia representará uma enorme ameaça à privacidade na esfera pública. De qualquer modo, essa proposta está sendo considerada inconstitucional segundo a Quarta Emenda à Constituição dos Estados Unidos. ¹⁶⁰

Information privacy is an individual's claim to control the terms under which personal information is acquired, disclosed, and used. My thesis is that cyberspace threatens information privacy in extraordinary ways, and without much collective deliberation, we may be in the process of surrendering our privacy permanently as we enter the next century.

¹⁵⁸ Security And Freedom through Encryption (SAFE) Act (H.R.850), section 3 (exports of encryption), [http://thomas.loc.gov/cgi-bin/query/D?c106:5:./temp/~c106LALPea:](http://thomas.loc.gov/cgi-bin/query/D?c106:5:./temp/~c106LALPea:;), visitado em 3 de março de 1999.

¹⁵⁹ KANG, Jerry. *Information Privacy in Cyberspace Transactions*; 50 Stanford Law Review 1193 (April 1998);

The principal privacy-protecting technology is encryption. In basic terms, encryption uses a cryptographic algorithm and a key to encode a message - plaintext - into something incomprehensibly garbled - ciphertext. Once communicated to the intended recipient, the ciphertext is decoded back into plaintext. If the cryptographic algorithm is strong, and the key properly selected and kept secret, it is infeasible for an unauthorized party to intercept the ciphertext and decrypt it back into plaintext. The basic concept of encryption lies at the heart of multiple privacy-promoting technologies.

¹⁶⁰ Não existe a exigência legal de depósito, ou registro público das chaves privadas nos Estados Unidos, embora alguns setores do governo defendam esta idéia: SULLIVAN, Kathleen. *Sullivan Testifies on Encryption*. <http://www.law.stanford.edu/faculty/sullivan/testi980317.shtml>, visitada em 21 de abril de 1999;

In U.S. Senate testimony on March 17, 1998, Kathleen Sullivan argued that the third-party encryption key escrow requirement proposed by the Department of Justice "involves serious constitutional tradeoffs." Sullivan, Stanford's Stanley Morrison Professor of Law, testified before the Senate Judiciary Committee's subcommittee on the Constitution, with Professor Richard Epstein of the University of Chicago Law School, on behalf of Americans for Computer Privacy, as part of the hearings on "Privacy in the Digital Age: Encryption and Mandatory Access." Encryption key escrow legislation, the subject of the hearings, would require Internet encryption users to deposit the key for their encrypted Internet communication with a third party. The government could then compel that third party to surrender encryption keys upon suspicion of criminal activity by the user. "Mandatory key escrow," Sullivan noted, "inverts [the] usual presumptions by requiring that citizens take affirmative steps to facilitate government surveillance." She compared the escrow scheme to the government requiring us "to live in glass houses, conduct all our conversations loudly and exclusively in English, carry all our personal belongings in clear plastic bags, or keep all of our possessions in unlocked

Os Estados Unidos adotaram uma política contrária à exportação de criptografia forte.¹⁶¹ Por detrás dessa posição, encontra-se o medo de que essa poderosa ferramenta possa ser usada por traficantes de drogas e terroristas. Como a criptografia forte é um meio importante de implementar os títulos de crédito no *ciberespaço*, através de uma solução confiável, que são as assinaturas digitais, essa posição dos Estados Unidos pode ser inconsistente por contrariar aqueles que anseiam por leis uniformes, específicas, para o *ciberespaço*. Também torna-se mais difícil conseguir um modelo-padrão para as transações comerciais. Se o governo não mudar essa posição, aparecerão vários modelos, cada país adotando seu próprio padrão. Os tribunais vêm decidindo em ambas direções: ora validando as restrições,¹⁶² ora considerando-as ofensivas à Primeira Emenda à Constituição dos Estados Unidos (emenda que garante a liberdade de expressão).¹⁶³

B. Endosso – como uma nota promissória eletrônica pode circular no espaço virtual

cabinets or drawers." As a method for preserving privacy, Sullivan argued, encryption may be considered "reasonable within the broad contours of our customs and traditions" and therefore deserving of full Fourth Amendment protection.

¹⁶¹ MAINLAND, Richard R. *Congress holds the key to encryption regulation: Many advocate for the removal of export restrictions on encryption products; the courts, as well as legislators, are divided*; 4/20/98 Nat'l L.J. B9, col. 2 (1998);

With law enforcement and intelligence concerns in mind, the federal government has for some years imposed restrictions on the export of encryption products, requiring that manufacturers provide for key recovery-or at least commit to providing such capability before exporting encryption products above 56 bits.

¹⁶² *Karn v. Department of State*, 925 F. Supp. 1 (D.D.C. 1996);

Courts found no violation of the First Amendment in the decision of the Department of State saying that a disk containing source code for encryption software was a defense article, requiring an export license.

¹⁶³ *Bernstein v. Dept. of State*, 1996 U.S. Dist. Lexis 18974 (N.D. Cal. 1996);

In this case, a source code for encryption software was found to be protected speech under the First Amendment. And so, the governmental requirement for an export license for Mr. Bernstein to publish his source code on the Internet was found to be unconstitutional restrains on his protected speech.

Este artigo aborda a análise do endosso por duas razões: primeiro, por causa do instituto legal que admite a circulação de notas promissórias; segundo, porque o risco de fraude está sempre presente. Há implicações criminais no caso de fraude a um banco mediante o uso de um título endossado irregularmente. A Suprema Corte dos Estados Unidos¹⁶⁴ pronunciou-se sobre essa questão, cujas implicações, através de uma análise legal, podem ser estendidas às notas promissórias eletrônicas.¹⁶⁵

¹⁶⁴ Caso da Suprema Corte dos Estados Unidos: 462 U.S. 356 (1983). Há, ainda, um caso antigo que ilustra a importância do endosso das notas promissórias: 1 WL 866 U.S. Tenn. (1875).

¹⁶⁵ O risco de fraude é alto e existem implicações criminais nos Estados Unidos, conforme a nossa análise abaixo;

The risk of fraud is high because one can transfer a fraudulent promissory note (for example, using false data about one's identity) in exchange for money. There are always rights embodied in a written instrument. Those rights may refer to a third party beyond "creditor" and "debtor." Since most of the negotiable instruments are negotiated with financial institutions, such as banks, one important legal issue is the one related to criminal implications of electronic promissory notes. In other words, what are the criminal implications, in the U.S., of obtaining money from a bank under false pretenses (using electronic promissory notes, for example). There are criminal sanctions, imposed by the Bank Robbery Act, 18 U.S.C. § 2113(b), in "[w]hoever takes and carries away, with intent to steal or purloin, any property or money or any other thing of value exceeding \$100 belonging to, or in the care, custody, control, management, or possession of any bank, credit union, or any savings and loan association." The question is to know if this provision is limited to thefts of tangible property. If so, the theft of a written negotiable instrument embodying rights of credit, would be excluded. This question has been addressed by the Supreme Court in *Nelson Bell v. United States*, 462 U.S. 356 (1983). The facts of this case are related to fraud in which the defendant altered the endorsement on a \$ 10,000 check (which analysis does not differ from an analysis of the same situation with a promissory note) in order to cause a loss to a bank. It is an important case for two reasons. First, it recognizes that, in the past, common-law larceny had excluded non-tangible property: "In the 13th century, larceny was limited to trespassory taking: a thief committed larceny only if he feloniously 'took and carried away' another's personal property from his possession. The goal was more to prevent breaches of the peace than losses of property, and violence was more likely when property was taken from the owner's actual possession. [B]ell's argument in favor of the narrower reading of § 2113 (b) relies principally on the statute's use of the traditional common-law language 'takes and carries away.' He cites the rule of statutory construction that when a federal criminal statute uses a common-law term without defining it, Congress is presumed to intend the common-law meaning." Second, it affirms that there is a congressional goal of protecting bank assets: "The congressional goal of protecting bank assets is entirely independent of the traditional distinction on which Bell relies. To the extent that a bank needs protection against larceny by trick, it also needs protection from false pretenses. We cannot believe that Congress wished to limit the scope of the amended Act's coverage, and thus limit its remedial purpose, on the basis of an arcane and artificial distinction more suited to the social conditions of 18th century

Como as notas promissórias eletrônicas foram criadas para o *ciberespaço*, tais documentos deveriam poder circular no *ciberespaço*, simplesmente porque uma nota promissória assinada digitalmente pode ser usada como *data input* para gerar outra assinatura digital. O risco de fraude existiria se a nota promissória eletrônica circulasse no *ciberespaço* e no mundo real. Aí haveria um sério risco de duplicação numa operação fraudulenta. As notas promissórias eletrônicas somente podem circular no *ciberespaço* e, conseqüentemente, somente podem “viver” no *ciberespaço*. Uma nota promissória somente é retirada do *ciberespaço*, para ser executada, uma vez que os tribunais não aceitam “ações judiciais eletrônicas”.

Por outro lado, não se admite a conversão de uma nota promissória tradicional num título eletrônico, o que também se constituiria numa porta aberta para as fraudes. Alguém que pudesse “escanear” uma nota promissória tradicional, poderia ser tentado a convertê-la numa nota promissória eletrônica, descontando-a num banco após o endosso. Em seguida, poderia tentar negociar o documento original (em papel) com outro banco.

A regulação dessas hipóteses acima consta de “Modelos Propostos” discutidos na letra “D” deste trabalho.

C. Os certificados estrangeiros devem ser reconhecidos mundialmente para possibilitar a circulação de notas promissórias eletrônicas

England than the needs of 20th century America.” Of course the legal analysis held by the Supreme Court in this case would be applicable to a situation involving electronic promissory notes, which can be inferred from the synopsis:

Defendant was convicted in the United States District Court for the Southern District of Florida of violating the Bank Robbery Act. The United States Court of Appeals for the Fifth Circuit, 649 F.2d 281, reversed, but that Court sitting en banc, 678 F.2d 547, ultimately affirmed the conviction. Certiorari was granted. The Supreme Court, Justice Powell, held that

Não é difícil compreender por que o comércio global necessita ter suas próprias leis para ser aceito mundialmente.¹⁶⁶ Os títulos de crédito do comércio eletrônico não deveriam encontrar barreiras como as de um país que não reconhece a validação emitida por uma “C.A.” estrangeira. Caso contrário, uma das mais importantes características do *ciberespaço* – a sua capacidade de aproximar os países¹⁶⁷ e seus mercados¹⁶⁸ - perderia o reconhecimento legal.¹⁶⁹ Muitos países já têm suas leis (ou seus costumes) regulando as

the Bank Robbery Act was not limited to common-law larceny, but also proscribed the crime of obtaining money under false pretenses. Affirmed.

¹⁶⁶ O *ciberespaço* é um ambiente internacional. A doutrina é bastante uniforme neste sentido. BIEGEL, Stuart. *The Emerging and Specialized Law of the Digital Revolution*, Los Angeles Daily Journal, January 25, 1996;

An important feature of cyberlaw is its international nature and scope. Cyberspace is an international medium, and the Internet is a completely global entity. The World Wide Web, for example, enables persons to move seamlessly and effortlessly from a "web site" in the U.S. to a web site in Asia. Proverbial net surfers can literally bounce around from France to Tanzania to Peru to Iceland with the click of a mouse. Electronic mail (e-mail) can be sent overseas as easily as it can be sent to the person next door.

¹⁶⁷ STARKE, J. *Introduction to International Law*, 9th ed. (1984);

[B]y reason of technological developments countries have become geographically more knit together.

¹⁶⁸ A Internet é responsável não só pela aproximação de mercados, como também pela aproximação de idéias. Alguns autores defendem que a supressão deste canal de transmissão de idéias viola direitos humanos: STEINER, Henry J. e ALSTON, Philip *International Human Rights in Context*, Clarendon Press, Oxford, p. 401;

Electronic communication through e-mail or the Internet [m]ade possible the instant diffusion of information to a vast audience. These technologies have made it almost impossible to contain knowledge of new, serious human rights violations within any part of the world, however remote and isolated.

¹⁶⁹ Acerca de várias outras implicações jurídicas do comércio eletrônico: PUTNAM, Melanie. *The Internet Guide to International Law Resources*, 10 Internet L. Researcher 3 (January 1999);

Even small law offices may discover that neighborhood clients are now doing business half-way around the globe. [T]he chances for being involved in an international situation are becoming more common. Has your client been traveling abroad? Was your client arrested or involved in an accident overseas? Is your client trying to open up a branch office in another country? Does your client's company have to serve papers abroad? [S]uddenly, treaty research has become as intriguing as a spy novel. Need to refer to The Hague Convention? Which one? The look-up trail begins here.

assinaturas digitais. “C.As” de cinco continentes¹⁷⁰ já podem ser encontrados no *ciberespaço*. A lógica da “Lei Alemã para Assinaturas Digitais”¹⁷¹ serve de parâmetro para a permissão da circulação de notas promissórias eletrônicas, pois essa nova Lei reconhece a validade dos certificados estrangeiros emitidos por “C.A.s” da União Européia ou de um país participante do “Certification Authorities from the European Union”, ou de um país membro do “European Economic Area”:

¹⁷⁰ Esta é a lista das Autoridades de Certificação disponíveis na Internet no dia 5 de fevereiro de 1999:

África. Todas na África do Sul: Binary Surgeons, Thawte Consulting e South African Certification Authority.

Ásia. Japão: Initiative for Computer Authentication Technology (ICAT), Thawte CA sponsored by MEDIX Inc. e Verisign Japan KK. Coréia: SoftForum.

Europa. European Union Projects: AD AEQUITATEM - Spain (Part of the INFOSEC AEQUITAS Project.) e ICE-TEL Project. Bélgica: Belsign e Isabel (Interbank Standards Association Belgium). Alemanha: PCA of the German Research Network, DFN - PCA, IN-CA: Individual Network e.V., c't - Krypto-Kampagne, TC TrustCenter, IKS Certification Authority, GeFökoM CA e Rus Test Certification Authority. Espanha: Internet Publishing Services, Siscer, e Fundación para el Estudio de la Seguridad de las Telecomunicaciones. Itália: Certification Authority Tin (Telecom Italia Net) e Societ` Interbancaria per l'Automazione S.p.A. Irlanda: Eurotrust (Baltimore Technologies) e Software and Systems Engineering Limited. Reino Unido: Eurosign, The Global Trust Register e TrueTrust. Suécia: COST.

América do Sul. Brasil: Certisign e Novaware Meta-Certificates.

América do Norte. Canadá: Entrust - Certification Products, Keywitness, OnWatch Key Management Centre and Xcert. Estados Unidos: ARINC (airlines and aircraft operators), BBN (Certification Products), Certco (Certification Products), Frontier Technologies (Certification Products), GTE Cybertrust (Certification Products), IBM World Registry, MIT Internet PCA Registration Authority, Skylight Software Inc.- Certification Products, SUN Certification Authorities, TradeWave Corporation - Austin, Texas, TradeAuthority Online Certification Authority for TradeVPI Products, Verisign, Verisign SET Protocol Certification Authority and WebVision - Certification Products.

Oceania. Austrália: Certificates Australia Pty Limited, Signet as part of the Australian National Public Key e Authentication Framework.

¹⁷¹ Conforme o texto da lei alemã: *German Digital Signature Act*, § 15, encontrada na Internet em <http://www.horns.netplace.de/iukdg/sigge.htm>, visitada em 31 de janeiro de 1999.

§ 15: Certificates Issued by Other Countries

(1) Digital signatures capable of being verified by a public signature key certified in another Member State of the European Union or in another State party to the Agreement on the European Economic Area shall be deemed equivalent to digital signatures under this Act insofar as they show the same level of security.

(2) Paragraph (1) above shall also apply to other states insofar as relevant supranational or intergovernmental agreements have been concluded.

A idéia de não se impor obstáculos aos certificados estrangeiros, nem mesmo através de formalidades (como a exigência de outra certificação emitida por um “C.A.” patricio) está expressa nas nossas propostas de emendas à L.U.G. (Título I, Artigo 2), discutidas no próximo capítulo.

**D. O espaço virtual necessita de nova regulamentação para títulos de crédito:
uma proposta de emendas à Lei Uniforme de Genebra para notas
promissórias eletrônicas**

Pode-se concluir que a mudança do papel para a gravação eletrônica representada por *bits* requer mudanças no Direito Comercial capazes de proporcionar uma regulamentação efetiva. Essas mudanças não implicam em abolir todo o antigo sistema legal. Algumas leis podem ser ajustadas e aplicadas ao *ciberespaço*.

Considerando a análise do capítulo II deste trabalho, o uso de assinaturas digitais não se opõe à “Lei Uniforme de Genebra”. Como um documento com assinatura digital

pode ser legalmente considerado como um documento escrito, as exigências da L.U.G., apresentadas no item “I.C” estarão satisfeitas.

Para a L.U.G. aceitar as notas promissórias eletrônicas, torna-se necessária uma legislação para regular as assinaturas digitais. Além dessa legislação sobre assinaturas digitais, poucas emendas devem ser feitas na L.U.G., as quais, modestamente, estão propostas abaixo:

LEI UNIFORME DE GENEVRA - NOTAS PROMISSÓRIAS ELETRÔNICAS

TÍTULO I - Dos Documentos Eletrônicos

Artigo 1 - Cada Alta Parte Contratante deverá legislar acerca de assinaturas digitais, emissão de certificados eletrônicos para a validação de documentos eletrônicos e credenciamento de Autoridades de Certificação eletrônicas, únicas competentes para a emissão dos certificados eletrônicos.

Artigo 2 - A certificação de um documento eletrônico emitida por Autoridade de Certificação devidamente registrada em uma das Altas Partes Contratantes será reconhecida por todas as demais Altas Partes Contratantes, sem a necessidade de nova certificação.

Artigo 3 - Todo documento eletrônico digitalmente assinado e certificado por uma Autoridade de Certificação tem a mesma validade de um documento não eletrônico escrito e assinado para todos os termos desta Lei Uniforme.

Artigo 4 - Toda e qualquer assinatura lançada em um documento eletrônico só é válida se for uma assinatura digital devidamente certificada por um certificado eletrônico emitido por uma Autoridade de Certificação legalmente credenciada.

TÍTULO II - Da Nota Promissória Eletrônica

Artigo 1 - Um documento eletrônico que satisfaz todas as formalidades estabelecidas por esta Lei para as notas promissórias e que está acompanhado de uma assinatura digital devidamente certificada é uma nota promissória eletrônica.

Artigo 2 - A nota promissória eletrônica só pode ser transferida no *ciberespaço*. A única forma válida de transferência da nota promissória eletrônica é o endosso eletrônico. O endosso eletrônico só é válido se for efetuado através de assinatura digital.

Artigo 3 - A nota promissória eletrônica não pode ser convertida em nota promissória não-eletrônica para efeitos de circulação. Tal conversão é nula de pleno direito.

Artigo 4 - Aquele que paga uma nota promissória eletrônica deve receber a nota promissória eletrônica digitalmente assinada pelo último possuidor da nota, que valerá como prova do pagamento.

TÍTULO III - Da Execução da Nota Promissória Eletrônica

Artigo 1 - A nota promissória eletrônica somente poderá ser impressa para efeitos de sua execução judicial. Todas as demais impressões da nota promissória eletrônica acarretam em nulidade de pleno direito.

Artigo 2 - O Judiciário poderá aceitar a nota promissória eletrônica como título válido para promover a execução judicial, sem a exigência da impressão da nota.¹⁷²

¹⁷² Este dispositivo é importante para o caso de algumas jurisdições vierem a optar por um processo eletrônico, no qual todo o processo somente existiria em computador.

Artigo 3 - O executado somente poderá provar o pagamento da nota promissória eletrônica através da apresentação do documento eletrônico descrito no Artigo 4 do Título II desta Lei.¹⁷³

Artigo 4 - Uma versão impressa do documento eletrônico exigido pelo Artigo 3 deste Título III pode ser apresentada pelo executado e será aceita pelo Judiciário.

TÍTULO IV - Regras Complementares

Artigo 1 - As notas promissórias eletrônicas são válidas apenas para emissão e circulação no *ciberespaço* e não podem ser convertidas em papel para efeitos de circulação, o que acarreta nulidade absoluta.

Artigo 2 - As notas promissórias eletrônicas não podem ser convertidas em notas promissórias não-eletrônicas por qualquer método tecnológico disponível. Qualquer conversão é nula de pleno direito.

Artigo 3 - As notas promissórias eletrônicas emitidas ao portador são nulas de pleno direito.¹⁷⁴

Artigo 4 - A Autoridade de Certificação manterá uma listagem da cadeia de endossos em cada título eletrônico. No caso de um título eletrônico ser indevidamente endossado mais de uma vez por um possuidor do título, os endossos seguintes ao primeiro serão nulos de pleno direito e a Autoridade de Certificação não certificará a

¹⁷³ Trata-se do recibo eletrônico: a nota promissória eletrônica digitalmente assinada pelo último credor da nota.

¹⁷⁴ Este artigo é necessário dado o enorme risco de fraude no *ciberespaço* se não fosse possível acompanhar toda a cadeia de transferência da nota promissória eletrônica através das assinaturas digitais dos endossantes.

assinatura digital do endosso fraudulento, sem prejuízo das demais sanções civis e criminais que cada Alta Parte Contratante houver por bem estabelecer para a fraude.

IV. CONCLUSÃO

As inovações ocorridas no Direito Comercial estão intimamente ligadas às práticas do comércio. Os usos e costumes das pessoas que fazem comércio têm sido uma importante fonte do Direito Comercial. Fatores como os riscos das viagens durante o final da Idade Média e a diversidade de moedas foram alguns dos responsáveis pelo desenvolvimento dos títulos de crédito, documentos necessários para o comércio. Mais de quatrocentos anos depois que apareceram os primeiros títulos de crédito, o comércio do mundo real se depara com novos mercados trazidos pelo “mundo virtual”. Aproximando os clientes e derrubando barreiras geográficas, o comércio eletrônico desafia o Direito Comercial. Trata-se de um novo mercado, um mundo global, constituído de *bits* e *bytes*, e, apesar disto, alguns conceitos permanecem atuais. Métodos de pagamentos, concessão de crédito e toda espécie de circulação de riquezas continuarão existindo no *ciberespaço*. O Direito acompanha os novos fatos sociais a fim de os regular. Atualmente, algumas práticas rotineiras do comércio eletrônico estão sendo reguladas.

O *ciberespaço* muda alguns dos paradigmas da nossa economia escrita para a *cibereconomia*. No mundo real, muitos conhecimentos e transações são reduzidos a documentos escritos. Evidentemente, o Direito se baseia em grande parte desse paradigma escrito para estabelecer parâmetros legais. O *ciberespaço* tem outro paradigma – a mídia digital – que necessita de novos parâmetros legais.

Através deste trabalho, procurou-se demonstrar que o *ciberespaço* não somente requer novos métodos e novas abordagens para sua regulamentação, mas também chega a oferecer algumas soluções destinadas a adaptar as instituições escritas legais, tradicionais, às instituições *ciberlegais*.¹⁷⁵ A assinatura digital obtida através de criptografia forte assimétrica é uma inovação técnica desenvolvida para o *ciberespaço*. Com uma legislação efetiva, a assinatura digital desempenhará, para o Direito Comercial, o papel de uma “ponte” entre o mundo real e o mundo virtual.

Este trabalho propõe uma aplicação prática e pragmática da assinatura digital na implementação, não somente das notas promissórias eletrônicas, mas também da negociabilidade e circulação de tais documentos. A solução de negociabilidade eletrônica proposta aqui, feita de acordo com o Direito Comercial Norte-Americano e Europeu, é pragmática. Este artigo demonstra a implementação legal do endosso eletrônico. O endosso foi escolhido porque é o instituto que possibilitará a negociabilidade das notas promissórias. No último item deste trabalho, procurou-se demonstrar a aplicabilidade das notas promissórias eletrônicas sob o U.C.C. e à L.U.G. com alguns ajustes.

Esta solução produzirá muitos efeitos práticos na confiabilidade do comércio eletrônico ao redor do mundo, pois seus participantes sentir-se-ão seguros ao fazer negócios e negociar seus títulos com a garantia do amparo legal.

O modelo de legislação proposto para a L.U.G. também se baseia no conceito de que o *ciberespaço* é diferente do mundo real. O *ciberespaço* é diferente a ponto de

¹⁷⁵ O Prof. Biegel discute esta questão em seu novo livro: BIEGEL, Stuart. *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*, capítulo 2, MIT Press (forthcoming - 2000/2001);

[I] take the position that cyberspace is different enough to merit a new set of rules across the board. [T]he inquiry therefore focuses on the middle ground, with answers invariably

requerer um novo conjunto de regras para, efetivamente, realizar sua regulação. Essas novas regras, algumas vezes, poderão ser usadas não somente para regular as relações no próprio *ciberespaço*, mas também servirão para regular a interface legal entre o *ciberespaço* e o mundo real. As leis do *ciberespaço* realizariam esses dois papéis, pois regulariam como os documentos eletrônicos seriam assinados digitalmente no *ciberespaço*; por outro lado, também regulariam a maneira pela qual esses documentos eletrônicos, assinados digitalmente, seriam trazidos ao mundo real. As leis sobre assinaturas digitais poderiam estabelecer parâmetros legais para regular a maneira como os documentos eletrônicos seriam convertidos de *bits* do *ciberespaço* para documentos escritos, em papel, com validade legal.¹⁷⁶

As leis sobre assinaturas digitais são exemplo de uma espécie que somente encontrará aplicação se as relações jurídicas envolverem o *ciberespaço*. Tais leis realizam duas funções: a regulação do próprio *ciberespaço* e a regulação da interface entre o *ciberespaço* e o mundo real. Essas leis pertencem a uma nova disciplina jurídica: o Direito Virtual, também conhecido como *Ciberdireito*.¹⁷⁷

depending to the great degree on whether and to what extent cyberspace *can* be regulated at this point in time.

¹⁷⁶ Mais uma vez cabe ressaltar que a escolha pela análise do endosso das notas promissórias pode ser aplicada, em parte, a outros títulos de crédito, como por exemplo os cheques. Estes têm grande importância como método de pagamento nos Estados Unidos: Congressional Budget Office (1996), *Emerging Electronic Methods for Making Retail Payments*, US Government Printing Office, Washington DC;

1984: Checks approximately 57%, Cash approximately 36%, Credit/debit Cards approximately 7%,

1995: Checks approximately 69%, Cash approximately 17%, Credit/debit Cards approximately 14%.

¹⁷⁷ Inúmeras escolas de direito norte-americanas oferecem a matéria "Cyberlaw." Alguns exemplos: UCLA School of Law: Law 598 Cyberspace Privacy, <http://www.law.ucla.edu/classes/archive/S97/598/>, visitada em 23 de dezembro de 1998, University of California at Berkeley School of Law: Law 276.1 - Cyberlaw (oferecida em *Fall*

1999), <http://www.sims.berkeley.edu/BCLT/courses/fall99/cyber.html>, visitada em 20 de setembro de 1999.