PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ

Fabiele Behrens

A Assinatura Eletrônica como Requisito de Validade dos Negócios Jurídicos e a Inclusão Digital na Sociedade Brasileira

DISSERTAÇÃO DE MESTRADO

CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS

Programa de Pós-Graduação em Direito Econômico e Social

Curitiba, 28 de julho de 2005.

CCJS – Centro de Ciências Jurídicas e Sociais

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ

Fabiele Behrens

A Assinatura Eletrônica como Requisito de Validade dos Negócios Jurídicos e a Inclusão Digital na Sociedade Brasileira

DISSERTAÇÃO DE MESTRADO

Dissertação apresentada ao Programa de Pós-graduação em Direito Econômico e Social da PUC-PR como requisito parcial para obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. Antônio Carlos Efing

Curitiba–PR
Julho de 2005

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ

Fabiele Behrens

A Assinatura Eletrônica como Requisito de Validade dos Negócios Jurídicos e a Inclusão Digital na Sociedade Brasileira

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre em Direito pelo Programa de Pós-graduação em Direito Econômico e Social da PUC-PR. Aprovada pela Comissão Examinadora abaixo assinada.

Prof. Dr. Antônio Carlos Efing
Departamento de Direito – PUC – PR
(orientador)

Prof. Dr. João Marques de Carvalho
Departamento de Engenharia Elétrica e Informática - UFCG-PA –
(convidado)

Prof. Dr. Edson José Rodrigues Justino
Departamento de Informática - PUC-PR-
(membro)

Profa. Dra. Cinthia Obladen de Almeida Freitas
Departamento de Informática – PUC-PR –
(suplente)

Curitiba, 28 de julho de 2005

Fabiele Behrens

Graduou-se em Direito pela Pontifícia Universidade Católica do Paraná, em 2000. Autora de artigos sobre Direito e Tecnologia; integrante do Grupo de Pesquisa em Direito, vinculado ao Mestrado em Direito Econômico e Social da PUC-PR; professora de Direito dos cursos de Administração de Empresas, Ciências Contábeis e Processamento de Dados da Faculdade FACET e do curso de Direito da Faculdade Dom Bosco, ambas de Curitiba.

Ficha Catalográfica

Behrens, Fabiele

A Assinatura Eletrônica como Requisito de Validade dos Negócios Jurídicos e a Inclusão Digital na Sociedade Brasileira / Fabiele Behrens; orientador: Antônio Carlos Efing, - Curitiba: PUC, Centro de Ciências Jurídicas e Sociais.

v. 134f.: il. 29,7 cm

1. Dissertação (mestrado) – Pontifícia Universidade Católica do Paraná, Departamento de Direito.

Inclui referências bibliográficas.

1. Introdução. 2. Avanços tecnológicos e a criptografia. 3. Aspectos jurídicos da documentação eletrônica. 4. Inclusão digital. 5. Conclusão. I. Efing, Antonio C. (Antonio Carlos). II. Pontifícia Universidade Católica do Paraná. Departamento de Direito. III. Título.

DEDICATÓRIA

Aos meus pais Marilda Aparecida Behrens, João Carlos Behrens e ao meu marido José Molinari Pinto, por todo amor, dedicação, carinho e apoio nesta caminhada.

AGRADECIMENTOS

A Deus, pela luz, pela força, coragem e perseverança ao longo de todo este período, bem como, pelas possibilidades e vitórias que colocou em meu caminho.

Aos meus pais e ao meu marido, por me ensinarem a transpor barreiras com fé, amor, força e dedicação, e, principalmente, por sempre acreditarem na conclusão desta dissertação.

Ao meu orientador por sua competência, compreensão e auxílio pela elevada expressão como profissional no meio jurídico.

A minha amiga Fernanda Schaefer Rivabem, pelas leituras, correções, paciência e carinho. Agradeço, por me ensinar, mesmo que indiretamente, a "reduzir palavras" e dizer tudo.

A secretária do Mestrado e amiga Eva Curelo pelas orientações, pelos gestos de afeição e habitual delicadeza e apoio nos mais variados momentos dessa caminhada.

A todos os professores, funcionários, e alunos do Mestrado em Direito Econômico e Social da PUC-PR, e todos aqueles que, direta ou indiretamente, contribuíram para a realização desta dissertação, dando-me força, incentivo e principalmente, acreditando ser possível trabalhar o tema da assinatura eletrônica e da inclusão digital no Direito.

RESUMO

Behrens, Fabiele. **A assinatura eletrônica como requisito de validade dos negócios jurídicos e a inclusão digital na sociedade brasileira.** Curitiba, 2005. 134p. Dissertação de Mestrado – Centro de Ciências Jurídicas e Sociais, Pontifícia Universidade Católica do Paraná.

As novas tecnologias permitiram a criação de diversas modalidades negociais, focos de discussões e formalizações por meio de contratos eletrônicos, envolvendo empresas e cidadãos na utilização de meios digitais. As transações eletrônicas podem ser protegidas pela assinatura digital, concretizada por meio da certificação digital. Este procedimento não se encontra totalmente amparado pela legislação brasileira, passando a ser um tema de preocupação de juristas e legisladores que buscam sua tutela adequada. Os contratos digitais utilizam programas de certificação digital, sem a necessidade do contato pessoal e da assinatura manual dos contratantes, gerando discussões sobre a sua validade. Ao Direito coube o desafio de amparar e acompanhar o desenvolvimento destas novas tecnologias, e por meio da criação de normas, esta busca não irá, apenas, reparar danos e impedir abusos, mas protegerá os cidadãos de práticas que, por ventura, firam interesses individuais e coletivos. A tecnologia traz diferentes formas de acesso e oportunidades para cidadãos e empresários, estes acontecimentos também geram aspectos negativos como a exclusão social criada pelo aumento da distância entre as classes sociais, pela impossibilidade e dificuldade de acesso ao mundo digital. Assim, há a necessidade da criação e implantação de projetos que visam a expansão e oportunidade de alcance por todos os cidadãos, buscando a inclusão digital. O acesso à tecnologia vem revestido como direito fundamental devendo ser garantido e promovido pelo Estado, e, ao Direito cabe proporcionar o equilíbrio social e o desenvolvimento à todos os cidadão, empresários e envolvidos nas relações contratuais eletrônicas.

Palavras-chave

Criptografia; assinatura digital; negócios jurídicos; contratos eletrônicos; inclusão digital.

ABSTRACT

Behrens, Fabiele. **An electronic signature as a requirement for validating legal business and the digital inclusion in Brazilian society.** Curitiba, 2005. A 125 page Masters Degree Dissertation – Center for Juridical and Social Sciences, Pontifícia Universidade Católica do Paraná.

New technologies have promoted the creation of various business modalities, focuses of discussion and formalizations in the way of electronic contracts, involving companies and citizens using digital means. Electronic transaction can be protected by digital signatures, implemented by digital certification. This procedure is not totally supported by Brazilian legislation, and is becoming a topic of concern of jurists and legislators who seek adequate tutelage. The digital contracts use digital certification programs, without the need of personal contact, nor the manual signature of the contractors, which generates arguments regarding its validity. Law had the challenge of supporting and accompanying the development of this new technology, and in creating new norms, such a search will not only repair damage and impede abuse, but also protect citizens from practices which, by chance might jeopardize individual and collective interests. Technology brings us new forms of access and opportunity for citizens and businessmen. Such occurrences also generate negative aspects such as the social exclusion caused by the increasing distance between social classes, by the impossibility and the difficulty in accessing the digital world. Hence, the need to create and implant projects that aim at expansion and allow such an opportunity to be within the reach of all citizens seeking digital inclusion. Access to technology is covered as a fundamental right which should be guaranteed and provided for by the State, and Law is to offer social balance and development to all citizens, businessmen and those involved in the electronic contracting relationships.

Key words

Cryptography; digital signature, juridical business, electronic contracts, digital inclusion.

Sumário

1
INTRODUÇÃO

A revolução tecnológica gerou a entrada da sociedade na era digital provocando grandes transformações na economia e nas formas de comunicações e de relações humanas. Face a este desenvolvimento os mais diversos segmentos econômicos e sociais vêm sendo desafiados a adaptar-se e re-estruturar conceitos e princípios diante das dinâmicas inovações concretizadas por meio dos mais diversos métodos tecnológicos. Esses processos tecnológicos têm provocado reações nas pessoas, profissionais e empresas na busca de compatibilidade com o novo meio.

Atualmente, diversas modalidades de materialização dos negócios jurídicos estão sendo discutidas e formalizadas, em especial, os contratos eletrônicos, que geram obrigações entre empresas e/ou pessoas por intermédio de mecanismos de transmissão de dados e de utilização de programas informáticos. Alguns pontos[1] podem ser discutidos, embora não se esgotem nestas identificações, pois são inúmeras as possibilidades que existem e podem ser criadas a qualquer instante. Ao Direito cabe o papel de buscar segurança para as relações desenvolvidas dentro deste ambiente digital.

Uma das soluções apontadas pelos estudiosos do Direito e por especialistas da área de informática para garantir a segurança dos negócios jurídicos, almejada, é a utilização da assinatura digital como meio de validar os instrumentos digitais de contratos. A assinatura digital é, no momento, reconhecida como a possibilidade do envio seguro de um documento por meio da aplicação do método criptográfico assimétrico.

O processo da assinatura digital advém de um ramo da matemática aplicada que utiliza complexas equações interdependentes para transformar mensagens em códigos ininteligíveis, e a partir de um procedimento reverso, recuperar o formato original. Assim possibilita o desenvolvimento de políticas de

[1] Como os métodos criptográficos, a assinatura digital, os negócios jurídicos, os contratos eletrônicos e a inclusão digital.

segurança que garantem a integridade do conteúdo que trafega nas redes digitais, dando certeza e confiabilidade às informações transmitidas.

Sua aplicação se dá sob a produção e emissão de senhas que, quando obtidas corretamente pelo usuário, permitirão o acesso ao conteúdo até então cifrado. Este procedimento de cifrar uma identificação, aplicá-la a um documento e posteriormente recuperá-la é o que se denomina de assinatura digital[2].

A criptografia pode ocorrer sob duas formas, a convencional ou simétrica e a de chaves públicas e privadas, ou assimétrica. Na forma convencional uma mesma chave (senha) é utilizada tanto para encriptar como para desencriptar (codificar e decodificar) um arquivo ou documento. Na forma assimétrica são representadas duas chaves, uma privada e outra pública, que são complementares uma à outra. Uma vez codificada com a chave privada, apenas quem tem a chave pública poderá decifrar a codificação, assim como realizar a operação inversa[3]. Cada uma das formas tem uma função e aplicação específica e possível que varia conforme a necessidade dos usuários e os fins por eles almejados.

O processo de transações eletrônicas, os envolvidos devem se resguardar por meio da assinatura digital de cada participante. Esta assinatura é consolidada pelo procedimento da certificação digital, perante uma Autoridade Certificadora, que será uma entidade pública ou privada responsável e garantidora da validade da assinatura. São métodos novos, nem sempre completamente protegidos pela legislação que encontra extrema dificuldade em se manter atualizada em face às novas tecnologias, e que merecem uma atenção especial de juristas e legisladores, para que as relações jurídicas sejam adequadamente tuteladas.

Inafastável, portanto, a capacidade de segurança resultante da assinatura digital. Função que, a princípio, é de responsabilidade das Autoridades Certificadoras, que geram a autenticação digital, pelo qual fica assegurada a identidade do proprietário das chaves. Esta garantia é conferida por meio do

---

[2] BUCHMANN, J. A. **Introdução a criptografia**. Rio de Janeiro **:** Berkeley Brasil, 2002. p. 25.
[3] VOLPI NETO, A. **Comércio eletrônico**: direito e segurança. Curitiba:Juruá, 2002. p. 58-60.

certificado digital, que contém: nome do usuário, validade, chave pública, número de série, a assinatura digital da autoridade[4].

Face a esse novo panorama das relações jurídicas, o presente trabalho buscou investigar os referenciais teórico-práticos sobre a assinatura digital envolvendo a técnica da criptografia, a compreensão sobre a sua aplicação e o potencial de segurança nas relações jurídicas. Bem como, apontar alguns problemas e indicar possíveis soluções, especialmente pela aplicação da criptografia assimétrica (assinatura digital).

Neste contexto, que visa também a facilitação de acesso à população aos novos recursos tecnológicos, a segurança é um fator de incontestável importância, pois cabe ao Estado e às empresas a proteção e manutenção da inviolabilidade de dados em seus sistemas.

Ao observar a ocorrência de inúmeros fatos jurídicos em ambiente digital, essa pesquisa optou por uma de suas formas de negócios jurídicos, a dos contratos eletrônicos que para a sua instrumentalização requerem programas de certificação digital, que afastam a necessidade de contato pessoal entre os contratantes. Com a finalidade de abordar esta temática, realizou-se uma fundamentação teórica sobre a distinção entre documento escrito ou verbal e documento eletrônico, e esse como forma de materialização dos negócios jurídicos.

A respeito dos contratos eletrônicos, buscou-se analisar os princípios que envolvem sua validade jurídica. No Brasil, a assinatura digital vem sendo muito difundida, trazendo grande preocupação aos legisladores que buscam a regulamentação do comércio eletrônico e do reconhecimento da assinatura digital como validade dos negócios jurídicos, em especial, os contratos eletrônicos.

O Direito tem sido constantemente desafiado a acompanhar o envolvimento social com estas novas tecnologias. A ciência jurídica, está sendo provocado a criar normas, que não apenas devem reparar danos ou impedir comportamentos abusivos, mas que evitem práticas que atentem contra os interesses individuais e coletivos, produzindo regras suficientemente flexíveis para que sejam capazes de acompanhar o desenvolvimento tecnológico.

---

[4] MARTINS, G. M. **Formação dos contratos eletrônicos de consumo via Internet**. Rio de Janeiro: Forense, 2003. p. 76-81.

A evolução tecnológica torna ainda mais evidente a diferença de acesso a recursos eletrônicos e informacionais, aumentando a distância entre as diferentes classes sociais, deixando transparecer os problemas econômicos e não apenas comerciais. A exclusão digital é uma realidade que precisa ser pelo Direito combatida, para que se possa manter o equilíbrio social e proporcionar a todos as mesmas oportunidades de acesso e desenvolvimento cultural.

Alguns projetos governamentais têm se preocupado com a questão da inclusão da população no uso de recursos digitais, por ser a tecnologia de informação e o comércio eletrônico importantes ferramentas de evolução e modernização. Neste contexto, seria a inclusão digital o acesso à maximização da tecnologia visando à redução nas desigualdades tecnológicas no Brasil.

Com a finalidade de apurar a situação da sociedade brasileira com relação à inclusão digital, buscou-se localizar historicamente as transformações na sociedade, em especial, a revolução tecnológica e seus desmembramentos. Ainda, em se tratando de mudança e de evolução, traçou-se um panorama sobre os paradigmas atuais salientando o paradigma da complexidade, sua fundamentação e aplicação na sociedade do conhecimento. Bem como, pesquisar e apresentar aspectos relevantes a respeito da inclusão digital e da possibilidade de difundir a assinatura digital e sua possível disponibilização à população em geral.

O questionamento sobre a segurança e o acesso da população em geral aos recursos criptográficos tem sido objeto de investigação em vários países desenvolvidos. No Brasil, apenas recentemente (1999), tiveram início os debates sobre o assunto, e a criação de normas a respeito do ambiente digital caminha a passos lentos. Ainda assim, vale aqui destacar os principais projetos que aguardam votação e as leis brasileiras em vigor.

O século XX caracterizou-se por ser um período de transição entre a Revolução Industrial e a Revolução Tecnológica, que hoje toma conta de toda a sociedade. No início do século XXI as novas tecnologias começam a se expandir por todos os setores da vida social (comércio, indústria, educação, saúde), os seus recursos multiplicam-se a cada dia visando trazer consigo facilidades e benefícios para toda a humanidade. No entanto, todo esse movimento de fomento ao acesso de novas tecnologias traz também consigo problemas sociais, políticos, econômicos e jurídicos que desafiam os profissionais das mais diversas áreas do

conhecimento a procurar soluções interdisciplinares adequadas, que, ao mesmo tempo permitam o desenvolvimento tecnológico e impeçam abusos e a exclusão social.

Nota-se que a Internet serve como exemplo de acesso irrestrito, que sob o formato de mídia está indiscutivelmente aplicada a toda sociedade do conhecimento, assim como nas atividades econômicas e comerciais. Ressalte-se que a inclusão digital está intimamente condicionada à situação econômica da população e por isso, já se pode observar certa preocupação governamental em proporcionar e subsidiar o acesso das pessoas carentes a esses meios de comunicação e comércio, uma vez que as barreiras territoriais, desde o advento da Internet, deixaram de existir[5]. Buscando demonstrar a movimentação governamental existente, o presente trabalho apresentou alguns dos principais projetos que visam o aumento da participação dos cidadãos no mundo digital e as perspectivas de futuros projetos e metas do governo.

Face a este panorama a presente dissertação tem por objetivo geral: apurar as possibilidades de segurança jurídica à assinatura digital e o aumento do seu alcance junto à população pela garantia da inclusão digital. E por objetivos específicos: - Localizar historicamente as transformações na sociedade, em especial a revolução tecnológica e seus desmembramentos. - Investigar os referenciais teórico-práticos sobre a assinatura digital envolvendo a técnica da criptografia, a compreensão sobre a sua aplicação e o potencial de segurança nas relações jurídicas. - Apontar alguns problemas e buscar possíveis soluções, especialmente, pela aplicação da criptografia assimétrica (assinatura digital); - Pesquisar e apresentar aspectos relevantes a respeito da inclusão digital e da possibilidade de difundir esta técnica e sua disponibilização para a população em geral.

Porém, várias outras questões jurídicas podem ser levantadas a respeito do ambiente eletrônico. Em particular, a assinatura digital vem sendo alvo de muitas discussões e debates. Assim, essa dissertação visa investigar a temática com a finalidade de construir uma análise crítica sobre a aplicação e a validade da

[5] SILVEIRA, S. A. & CASSIANO, J. (orgs.). **Software Livre e Inclusão Digital**. São Paulo: Conrad, 2003. p. 21-24.

assinatura digital, bem como sobre a possibilidade de acesso e a utilização por toda a população brasileira.

2
OS AVANÇOS TECNOLÓGICOS E A CRIPTOGRAFIA

> *"Estamos vivendo a abertura de um novo espaço de comunicação, e cabe apenas a nós explorar no plano econômico, político, cultural e humano. Que tentemos compreendê-lo, pois a verdadeira questão não é ser contra ou a favor, mas sim reconhecer as mudanças qualitativas".*
>
> Pierre Lévy

2.1
O desenvolvimento dos computadores

O computador foi criado, inicialmente, com a função de realizar cálculos simples e complexos. Portanto, a princípio, o computador não passava de uma máquina de calcular em tamanho diferenciado (gigantescos para os padrões atuais) e para estes fins era utilizado. O uso dos computadores começou a ser ampliado a partir da Segunda Guerra Mundial, quando foram aplicados para difusão de informações.

Por volta de 1945 foi lançado o ENIAC (*Eletronic Numerical Integrator and Calculator*), cuja função principal era a avaliação e o cálculo da trajetória de mísseis, tinha a dimensão de *"100 m², possuía 18 mil válvulas, sendo capaz de realizar 4.500 operações por segundo"*[6]. Em meados de 1951, a *Remington Rand* apresentou o UNIVAC, computador que aos números somou as palavras, segundo Sergio Amadeu da SILVEIRA (2001, p.11) seu espaço de memória não era superior ao de *"uma miniagenda eletrônica encontrada hoje nas bancas dos camelôs nas ruas das grandes cidades"*, ou seja, sua memória tinha capacidade para armazenar nada mais que 1.024 palavras.

---

[6] SILVEIRA, S. A. **Exclusão Digital**: A miséria na era da informação. São Paulo: Fundação Perseu Abramo. 2001, p. 11.

A IBM iniciou sua participação no mercado de computadores em 1953, quando disponibilizou o IBM 701 que possibilitava a armazenagem de 4.096 palavras. Esses computadores apresentavam dimensões que, muitas vezes, atingiam uma sala inteira. Não contavam com monitor e teclado, com isso não apresentavam as características de interatividade, ou mesmo de meio de comunicação que existem nos computadores mais modernos[7].

A mudança estava só por começar. Em 1971, *Ted Hoff* deu um passo importante para a evolução do computador, semelhante aos dos dias atuais, com a invenção do processador. Esta peça utilizada nos equipamentos possibilitou o aumento da capacidade de processamento das máquinas[8]. Sem contar que, alguns anos antes (por volta de 1965), foi apresentada a Lei Moore, ao demonstrar a realidade da rápida mudança no ambiente eletrônico, como destaca Sergio Amadeu da SILVEIRA (2001, p.12): *"Gordon Moore, então diretor de pesquisa e desenvolvimento da Fairchild Semiconductor ao analisar a evolução dos chips de silício, acabou concluindo que o poder de processamento dos computadores dobraria a cada 18 meses, sem alterar o seu custo*", e demonstra a "essência" da teoria de Moore quando complementa apresentando que *"as placas dos computadores são cada vez menores e o numero de operações possíveis cada vez maiores*". Tal lei pode ser aplicada até à atualidade, pois, frente às modificações e novidades quase diárias, há cada vez mais possibilidades e maior armazenamento em equipamentos cada vez menores.

Um avanço expressivo foi a criação e comercialização dos microcomputadores domésticos. A invenção de Steven Wozniak e Steve Jobs, o Apple II em 1978, apresentava em sua configuração o monitor colorido e o *drive* para disquete. A IBM precursora da tecnologia computacional, não pretendia ficar para trás e em parceria com Bill Gates, desenvolveu o PC[9] e mais tarde o PC-XT, contendo em sua configuração o MS-DOS[10]. A partir desta época o progresso, as melhorias e as novidades quanto a equipamentos e configurações são quase diárias, e passam a fazer parte do cotidiano das pessoas em todo mundo.

---

[7] SILVEIRA, S. A., 2001, op. cit., p. 11.
[8] Ibid., p.12.
[9] PC, abreviação de *Personal Computer*.
[10] Um dos mais famosos sistemas operacionais desenvolvido pela Microsoft.

2.2
A criação da Internet

Durante a Guerra Fria, em 1957, a União Soviética lançou o primeiro satélite - *SPUTNIK*, demonstrando seu domínio e poderio tecnológico. Acontecimento que assombrou seus inimigos e pressionou os Estados Unidos da América, que sob a presidência de *Dwight Eisenhower* criou a *Advanced Research Projects Agency* (ARPA). As principais metas dessa agência giravam em torno de pesquisas e projetos militares buscavam a recuperação do poder tecnológico americano. Um desses projetos, a ARPA *Npaul baranetwork* teve como parceiro a RAND *Corporation*[11], que contratou para participar alguns acadêmicos e cientistas, com o objetivo de reforçar e melhorar suas atividades[12].

Por volta de 1962, na eminência de uma guerra, a empresa parceira da ARPANET, juntamente com *Paul Baran*[13], emitiu um relatório que descrevia o funcionamento de um sistema que tinha por finalidade evitar a interrupção da comunicação no caso de um ataque nuclear. Com essa proposta, demonstrava possibilidades de evitar que os dados e informações já armazenados em seus computadores fossem perdidos, devido ao ataque a um dos pontos de controle de informações. Assim, por meio da interligação de pontos formava uma espécie de rede eletrônica[14].

Por volta de 1969, para a satisfação dos pesquisadores envolvidos, a ARPANET tornou possível a interligação de quatro centros universitários americanos: Stanford, Berkeley, UCLA e Utha[15]. Nesse momento, surgiram os fundamentos e princípios da Internet. A tecnologia desenvolvida foi liberada para utilização e aplicação nas universidades, propiciando a circulação de estudos, trabalhos e pesquisas acadêmicas. A possibilidade da troca de dados passou a ser

---

[11] Empresa especialista em desenvolvimento tecnológico para defesa militar, que associada a ARPA *Network* ou também chamada ARPANET, passou a produzir maior resultados e avanços tecnológicos em pesquisas.
[12] SILVEIRA, S. A.. 2001, op. cit., p. 12-13.
[13] *Paul Baran*, nascido na Polônia, professor do curso de Engenharia Eletrônica da Universidade de Drexel. Casou-se e passou a morar nos Estados Unidos da América, onde lecionava na UCLA.
[14] Ibid., p.13.
[15] Ibid., p.13.

aperfeiçoada, interligando outros sistemas já existentes, momento em que *Robert Kahn*[16] lançou o TCP/IP- *Transmission Control Protocol/Internet Protocol*[17]- [18].

O aumento da ligação de várias redes compactadas em apenas uma[19], ficou fortalecido em 1989, especialmente, na época da queda do muro de Berlim e do bloco soviético[20]. Nesse mesmo ano foi criado um novo sistema hipermídia o WWW – *World Wide Web*[21], ou apenas denominado *Web*, no Laboratório de Física de Genebra[22] [23].

Outro passo determinante para a evolução da Internet, foi a criação da BITNET[24]. Por volta de 1993, outro grande passo ocorreu com a criação do navegador[25] *Mosaic*, e a utilização de uma linha telefônica, dando mais agilidade e acessibilidade aos usuários[26]. A rede passou a crescer cada vez mais, e se tornar uma realidade mundial. Alguns anos depois, foi lançado no mercador os navegadores *Netscape* e *Explorer*, sendo este último, atualmente o mais utilizado. Nesse sentido, a rede passou a crescer cada vez mais tornando rápida a troca de

---

[16] Robert Kahn, também participante da *Advanced Research Projects Agency (ARPA)*, do Departamento de Defesa Norte-Americano.

[17] ISAGUIRE, K. R.. **Internet**. Responsabilidade das empresas que desenvolvem os sites para web-com. Curitiba: Juruá, 2002, p.17.

[18] TCP/IP significa Protocolo de controle de transmissão/ Protocolo de Internet, após esta criação qualquer rede de computadores poderia configurar como padrão de envio de informações este protocolo. Ou seja, mesmo usando equipamentos diferentes estava assegurada a conexão e troca de dados.

[19] No Brasil, em 1981, realizou-se a primeira ligação de computadores em diferentes terminais (semelhante ao modelo Minitel francês), porém apenas em 1989 ocorreu a primeira ligação de várias redes em uma só. SILVEIRA, S. A., 2001, op. cit., p. 14.

[20] Ibid., p.14.

[21] "*A World Wide Web é uma função da Internet que junta, em um único e imenso hipertexto ou hiperdocumento (compreendendo imagens e sons), todos os documentos e hipertextos que a alimentam*". *"Hipertexto é um texto em formato digital, reconfigurável e fluido. Ele é composto por blocos elementares ligados por links que podem ser explorados em tempo real na tela. A noção de hiperdocumento generalizada, para todas as categorias de signos (imagens, animações, sons etc), o principio da mensagem em rede móvel que caracteriza o hipertexto".* LÉVY, P. **Cibercultura.** Trad: Carlos Irineu Costa. São Paulo: Ed. 34, 1999, p. 27.

[22] A criação foi de *Tim Bernes-Lee*.

[23] CORRÊA, G.T.. **Aspectos jurídicos da Internet.** São Paulo: Saraiva, 2002, 2 ed., p.11.

[24]" Sigla de Because It's Time Network (Bitnet). Rede educacional internacional que liga computadores em aproximadamente 2.500 universidades e institutos de pesquisa no mundo todo. A Bitnet não usa o protocolo TCP/IP, mas pode trocar mensagens de correio eletrônico com a Internet. Até o início dos anos 90, a Bitnet tinha alguma importância na conectividade mundial, mas foi definitivamente suplantada pela maior abrangência da Internet. A principal aplicação da Bitnet tem sido a manutenção de listas de distribuição. A diferença mais visível entre Bitnet e Internet está nos endereços dos servidores". Disponível em: http://www.culturatura.com.br/termos/internet/1.htm. Acesso em 10 set 2005.

[25] Também denominado *browser*, ou seja, um programa com a finalidade de acessar a Internet.

[26] ISAGUIRE, K. R., 2002, op. cit., p. 18.

dados, de comunicação, de arquivos, de informações, um fato juridicamente relevante.

Gustavo Testa CORRÊA (2002, p.8) conceitua Internet como

> *Um sistema global de rede de computadores que possibilita a œomunicação e a transferência de arquivos de uma máquina a qualquer outra máquina conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento.*[27]

Assim, fica evidenciada a utilização da Internet como instrumento de comunicação, de comércio, de economia, de sociabilização e até mesmo de relacionamentos. Novas tecnologias vão sendo criadas a cada dia, ou melhor, a cada hora, conferindo à rede maior rapidez e melhor acesso, principalmente, com lançamento da transmissão de dados via banda larga, por cabos e até pela utilização de freqüências de rádio[28].

Juntamente com sua criação e desenvolvimento, a Internet permitiu a criação de novas formas de negócios, modificando institutos jurídicos já existentes e enraizados no ordenamento brasileiro. Outra grande mudança que adveio juntamente com a evolução da rede foi a insegurança gerada no sistema, levando à criação de novos conceitos e formas de se conferir tranqüilidade, confiança e certeza aos negócios realizados.

2.3
Avanços na tecnologia criptográfica (histórico)

A criptografia é uma Ciência muito antiga. Do início de sua existência, o homem busca garantir a segurança em suas comunicações. A evolução das trocas de informações fica mais facilmente identificada a partir da descoberta da

[27] CORRÊA, G. T., 2002, op. cit., p. 8.
[28] ISAGUIRE, K. R., 2002, op. cit., p. 18.

escrita. Na realidade, não se pode precisar o momento e local da criação da criptografia, mas, estudos apontam que as maiores probabilidades giram em torno do Egito, da China, da Índia e da Mesopotâmia. Assim, por exemplo, na civilização egípcia podem ser encontrados evidências sobre a utilização de forma de escrita secreta, evitando a leitura de mensagens por pessoas indevidas[29].

O passado da humanidade foi permeado por civilizações que aplicaram o método da criptografia em diferentes períodos. Um dos exemplos mais conhecidos, data de 475 a.C., quando os gregos de Esparta utilizaram o primeiro sistema criptográfico aplicado à mensagens militares, denominado como "ESCÍTALA". Este sistema era composto por um bastão de madeira envolto por uma tira fina de pergaminho, que apresentava a escrita da mensagem secreta. Ao ser enviada esta tira era solta da madeira original, resultando num emaranhado de letras cuja leitura só poderia ser possível se fosse enrolada num bastão de idêntico tamanho e espessura. Este foi o sistema precursor do método criptográfico de transposição[30].

O Imperador Júlio César, por não confiar em seus mensageiros, utilizava a troca de letras por símbolos, chamado método de substituição[31]. As letras das palavras eram substituídas por outras. Por exemplo, a letra A era substituída pela D, B por E, e assim por diante. Na elaboração, era necessário que o emitente produzisse uma listagem específica para que receptor, de posse desta, conseguisse desvendar a mensagem encriptada[32].

Na antigüidade, se destacam os persas, tibetanos, iraquianos e egípcios, entre outros, como povos que utilizaram o método para manter a privacidade e a segurança de suas escritas. Mas, por longos mil anos, as técnicas criptográficas caíram no esquecimento, passando a ser consideradas como arte negra ou ocultismo. Esse fato prende-se à utilização de uma espécie de criptografia para ocultar magias, presságios, maldições e encantamentos, como os contidos em hieróglifos egípcios.

---

[29] MARCANCINI, A. T. R.. **Direito e informática. Uma abordagem sobre criptografia**. Rio de Janeiro: Forense, 2002, p.10

[30] **Criptografia clássica**. Disponível em: <http://members.fortunecity.es/ criptografia/ criptografiaclasica.html>. Acesso em 17 mar. 2004.

[31] MARCANCINI, A. T. R., 2002, op. cit., p.10.

[32] Ibid., p.10.

A Criptologia enquanto Ciência teve seu início entre os árabes, por volta do ano 600 d.C.. Mas, os ocidentais apenas começaram a utilizar a criptografia na Idade Média, Ciência que continuam desenvolvendo até os dias atuais.

Foi durante a II Guerra Mundial que a criptografia teve seu auge, quando 46.000 mil pessoas (na Grã-Bretanha e nos Estados Unidos) estavam envolvidas em interceptar e desencriptar mensagens codificadas. Na Alemanha essas mensagens eram codificadas pela máquina cifradora denominada ENIGMA. Os ingleses e americanos após diversas tentativas conseguiram criar a máquina que denominaram CONVERSOR M-209, equipamento que, finalmente, conseguiu decifrar as mensagens enviadas pelo método ENIGMA[33].

A utilização da criptografia nas telecomunicações, foi iniciada por volta da década de 1960, quando a empresa IBM, visualizando um rápido desenvolvimento tecnológico, deparou-se com a necessidade de criar mecanismos que garantissem a segurança nas comunicações. Narra Gustavo Testa CORRÊA (2002, p.77-78)

> *Desses estudos resultou em 1971 o desenvolvimento do algoritmo Lúcifer pelo cientista Horst Feistel, utilizado inicialmente pelo Loyds Bank of London. A versão definitiva de tal programa foi elaborada entre 1972 e 1974 pelo pesquisador especialista em teoria da informação, disciplina essencial para a moderna criptografia, Walter Tuchman, também da IBM. O objetivo de Tuchman foi eliminar as fraquezas do programa anterior, utilizando critérios que tornariam seus trabalhos mais seguros. E assim nasce o algoritmo-padrão chamado DES, até hoje utilizado.*

A criação mais significativa no âmbito da criptografia foi o invento de Philip Zimmermann denominado de *Pretty Good Privacy,* comumente chamado de PGP. Esta invenção apresenta-se na forma de um *software* comercial, produzido pela NAI- *Network Associates Inc.*[34]. Na verdade, este inventor, por volta de 1991, além de desenvolver o programa, disponibilizou-o à rede mundial

---

[33] LOPEZ, M. J. L.. **Criptografia y seguridade em computadores**. Disponível em: <http://www.kriptopolis.com>. Acesso em 03 ago. 2003.

[34] A princípio um programa de computador, mas passou a ter um sentido maior o da parceria em busca da segurança nas relações via Internet.

(Internet) gratuitamente[35]. Mas, a evolução da tecnologia trouxe em 1997 um problema referente ao programa, como indica Paulo Sá ELIAS (2004, p.49)

> *O software de criptografia PGP – Pretty Good Privacy – por exemplo, com mais de 7 milhões de usuários no mundo, apresentou uma 'falha de programação' considerada por Philip Zimmermman, que desenvolveu o software, constrangedora. Porém, muito difícil de ser explorada. A falha permitiu a alteração da chave pública criada pelo software, abrindo a possibilidade de se conhecer e alterar conteúdos criptográficos.*
> *A vulnerabilidade foi descoberta pelo pesquisador alemão Ralf Senderek, com base na característica técnica conhecida como ADK (implantada no PGP, em 1997) – exigida por clientes corporativos no objetivo de conseguir uma alternativa para decifrar mensagens profissionais trocadas entre empregados no caso da indisponibilidade para se decifrar o arquivo, como, por exemplo, no caso da morte do empregado ou em razão do esquecimento da frase-senha.*

Na realidade a falha encontrada pelos estudiosos foi corrigida, possibilitando que o programa PGP mantenha assegurada a confiança e a tranqüilidade aos seus usuários. Em virtude desta adaptação e melhoria, este programa continua sendo muito utilizado entre os usuários da Internet.

Com os avanços informático-tecnológicos algumas formas de criptografia ficaram obsoletas, outras evoluíram juntamente com a geração de computadores desenvolvidos. A necessidade de rapidez e eficiência na capacidade de criptografar e decifrar mensagens, motivada pela busca de segurança, força o desenvolvimento de programas especializados, fatos que exigem contínua pesquisa e criação incessante.

2.4
Conceitos de Criptografia

Os métodos criptográficos foram muito difundidos e aplicados em exercícios e estratégias militares, pois, possibilitavam o envio de mensagens a

[35] Assim, qualquer pessoa interessada em proceder o *download* deste programa, poderia encontrá-lo disponível na Internet possibilitando sua difusão.

locais distantes, sem que o inimigo a decifrasse caso rendessem o mensageiro. Este também foi o primeiro estímulo ao desenvolvimento da Criptoanálise, ou seja, o método de quebrar o código que possibilita a leitura da mensagem enviada e a implantação da segurança.

A análise etimológica da palavra criptografia *"deriva de criptologia, que se origina do grego 'KRYPTÓS LÓGOS', que significa 'palavra escondida'"*[36]. Esta técnica pode ser denominada como a arte de cifrar ou codificar, possibilitando ao conhecedor do código o acesso à mensagem enviada.

Na atualidade, as Ciências Exatas, enquanto Área do Conhecimento, são responsáveis pelo estudo da Criptografia, sob a forma de uma ramificação da Criptologia. Outro desdobramento da Criptologia é a Criptoanálise, que trata do método de decifrar as mensagens, sem a utilização de senhas[37].

O significado da criptografia é unânime entre vários autores, como Augusto Tavares Rosa MARCACINI (2002, p.09) que define como *"a arte de escrever em cifra ou em código, de modo a permitir que somente quem conheça o código possa ler a mensagem"*. Marlon Marcelo VOLPI (2001, p.06) ainda a conceitua como *"a ciência da transformação de dados de maneira a torná-los incompreensíveis sem o conhecimento apropriado para sua tradução"*. Gustavo Testa CORRÊA (2002, p.77) descreve criptografia como *"uma 'máscara' colocada sob determinado arquivo, tornando-o irreconhecível para aqueles que lhe 'olhassem na rua', ou seja, enquanto estivesse trafegando na Rede"*, e, complementa que *"essa máscara seria algo lógico, relacionado a fórmulas matemáticas, e só alguém que possuísse a fórmula matemática certa poderia desmascará-la e, assim, lê-la"*.

Outros autores também definem criptografia, como Jean Carlos DIAS (2002, p.90-91) ao apresentá-la como *"o meio de codificação/decodificação, ou seja, a fórmula para permitir a tradução de códigos de linguagem comum"* e, acrescenta, que *"impediria, assim, que terceiros, alheios ao emitente e ao destinatário, pudessem tomar conhecimento da mensagem"*. Ainda Katya Regina ISAGUIRE (2002, p.65) afirma que *"a criptografia é um método já conhecido de*

---

[36] VOLPI, M. M.. **Assinatura Digital. Aspectos técnicos, práticos e legais**. Axcel Books: Rio de Janeiro, 2001, p. 6.
[37] MARCACINI, A. T. R., 2002, op. cit., p. 09.

outras épocas e utiliza chaves que conferem a condição ao usuário da exclusividade de conhecimento da informação".

O conceito de criptografia pode ser interpretado como a possibilidade de camuflar determinado arquivo ou documento. Esta camuflagem pode ser reconhecida sob a forma lógica, pela utilização de fórmulas matemáticas, na qual, apenas quem possui a fórmula decodificadora pode ler os dados criptografados. Com isso, algoritmos matemáticos programados em softwares[38], por sua complexidade, transformam documentos legíveis em um emaranhado de caracteres numéricos sem nenhum sentido, sendo possível sua leitura, apenas, com a utilização da chave (senha) adequada. O ato de tornar impossível a leitura da mensagem ou o arquivamento denomina-se encriptar. O processo inverso, que permite a compreensão do documento, denomina-se como desencriptar.

A finalidade principal da criptografia é estabelecer um padrão entre o emissor e o receptor, possibilitando o envio de mensagens sob a forma de codificações. Tal mensagem tem características incompreensíveis à terceiros que a recebessem, sendo possível sua leitura, apenas ao receptor correto, pois este conhece o padrão utilizado na mensagem, permitindo conhecer o conteúdo do que foi enviado.

2.5
Formas de Criptografia

A evolução da tecnologia, assim como da criptografia, desenvolveu dois métodos diferentes de cifragem, a criptografia simétrica e a criptografia assimétrica.

[38] Denominado PGP "P*retty Good Privacy*".

2.5.1
Criptografia Simétrica

O método da criptografia simétrica, também chamado de método convencional, foi um dos primeiros métodos utilizados para buscar mecanismos de segurança na troca de informações. Segundo Marlon Marcelo VOLPI (2001, p.08), o método de criptografia simétrica pode ser entendido como *"o uso de uma chave secreta, a qual o emissor usa para codificar a informação, e, posteriormente, o destinatário utiliza para decifrá-la"*. Augusto Tavares Rosa MARCACINI (2002, p.21) esclarece que *"consiste num método que se utiliza de uma mesma senha, seja para cifrar, seja para decifrar a mensagem"*. Ainda pode ser identificado por Gustavo Testa CORRÊA (2002, p.78) como *"um outro método criptográfico baseado em senhas de acesso para abrir arquivos*".

Nota-se que a conceituação do método de criptografia simétrica, muitas vezes, se confunde com a sua aplicação, que consiste na utilização de uma chave (senha) para cifrar e a mesma chave para decifrar a mensagem ou o documento. Existem vários métodos simétricos diferentes como: Cifra de César[39], Cifras de Substituição[40], Transposição Alfabética[41], Substituição por Código. Este último foi o mais utilizado[42], no qual as letras são substituídas por códigos numéricos. Marlon Marcelo VOLPI (2001, p.11) exemplificou a aplicação este método da seguinte forma

Sabido – 12035

---

[39] **Cifra de César** consiste na substituição de letras do alfabeto, na qual cada letra utilizada é substituída pela terceira letra seguinte. Porém o emissor poderá optar por outro número de letra para a substituição. Pode ser exemplificado pela palavra: DIREITO - GMUHMXR, quando utilizando o padrão de número 3 que na realidade é a senha para a leitura do texto. MARCACINI, A.T. R., 2002, op. cit., p. 19.

[40] **Cifras de Substituição,** neste método "*preserva-se a ordem dos símbolos, apenas disfarçando-os*". Assim pode-se apresentar como original as letras do alfabeto e como senha outra letra correspondente, por exemplo, a letra A equivale a R, B a X, C a F, D a S, E a Z. A palavra CADA ficaria encriptada sob a seguinte forma FRSR. VOLPI, M. M., 2001, op. cit., p. 9.

[41] **Transposição Alfabética,** utiliza-se da *"reordenação dos símbolos através de uma tabela montada a partir de uma palavra chave... apresenta uma maior complexidade, tornando-se um meio menos sujeito a quebra"*. Ibid., p.10.

[42] Principalmente no período da II Guerra Mundial.

Sábio – 12040

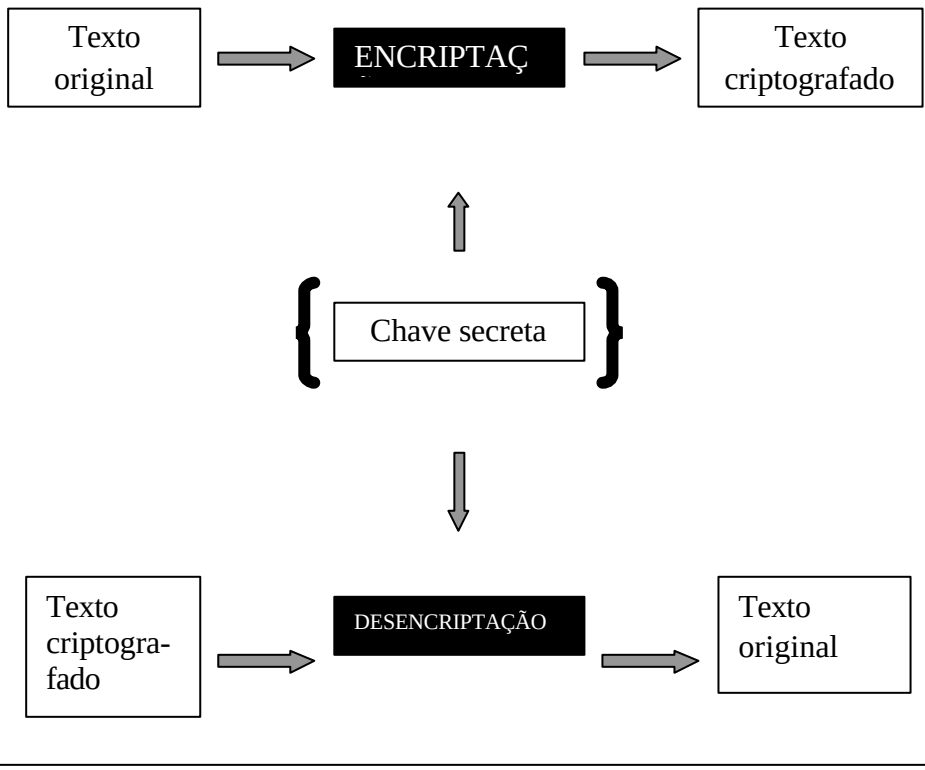
Sabonete – 12045

Sabor – 12050

Com isso nota-se que o método simétrico utiliza a mesma senha para codificar (encriptar) e para decodificar (desencriptar). Assim, as partes interessadas no envio da informação e em seu recebimento devem atender a compatibilidade na senha (chave) utilizada.

A criptografia simétrica pode ser assim representada [43]

Fig. 01 CRIPTOGRAFIA SIMÉTRICA



[43] Figura com base em Ângelo VOLPI NETO, **Comércio eletrônico**. Direito e Segurança. Curitiba: Juruá, 2002, p.59.

A Figura 01 representa o funcionamento da criptografia simétrica, no qual o emissor, proprietário do texto original o encripta com a utilização de uma chave secreta (senha ou código). Ao receber o texto criptografado, o receptor, de posse da chave secreta (senha ou código) tem a possibilidade de desencriptá-lo e ler a mensagem. Porém, este método carrega certa insegurança em sua aplicação, pois por meio de operação, ou divulgação da chave, ou interceptação da senha, as mensagens podem ser decifradas.

Outro aspecto negativo relaciona-se à autenticidade do documento, pois, segundo Augusto Tavares Rosa MARCACINI (2002, p.23)

> *A autenticidade que a criptografia simétrica permite obter tem aplicação restrita à segurança das comunicações. O receptor, e somente ele, sabe ter recebido a mensagem do emissor, pois, em tese, estes dois seriam as únicas pessoas no mundo a conhecer a senha, e isto assegura que um terceiro não está se fazendo passar pelo remetente. Contudo, este sistema não permite demonstrar para outra pessoa que a mensagem efetivamente provém do suposto emissor, e isto por uma razão bastante simples: o próprio receptor também poderia ter encriptado a mensagem, vez que também conhece a senha. Disto se extrai que a criptografia convencional não permite a criação de assinaturas digitais, nem permite que o documento eletrônico cifrado, por si só, possa servir como prova da manifestação da vontade.*

As limitações para a utilização do método da criptografia convencional estão intimamente vinculadas ao envolvimento do remetente com o destinatário, que precisam se preparar previamente para sua utilização. Para seu funcionamento é necessário que os envolvidos conheçam a chave, pois, quando a mensagem já criptografada chega ao destinatário, só poderá abri-la e decodificá-la aquele que possui a senha. Além disso, o método simétrico não tem grande eficiência quando utilizado em conexões sem a adequada segurança.

Com isso, o método de criptografia simétrica carrega muitos perigos e inseguranças, uma vez que o usuário ao ter acesso à senha pode criar novas mensagens, ou modificá-las conforme seus interesses próprios. Ao analisar a segurança do método, observa-se a fragilidade quanto à combinação da chave que

será utilizada, pois esta poderá ser desvendada ou divulgada contra a vontade de uma ou de todas as partes.

As dificuldades e inseguranças do método de criptografia simétrica geraram a necessidade da criação de um novo método que carregasse, além da capacidade de segurança a possibilidade de autenticidade. Assim, por volta do ano de 1976, *Whitfield Diffie* e *Martin Hellman*, publicaram um artigo com o título "*New directions in cryptography*", no qual propunham a utilização de uma nova forma de criptografia, pelo método assimétrico[44].

2.5.2
Criptografia assimétrica

O método assimétrico ou criptografia de chave pública teve o início de sua utilização em 1976[45]. Segundo esse método, cada usuário possui um par de chaves (uma pública e uma privada), ou seja, uma disponível ao público e outra mantida sob seu sigilo. Esse avanço possibilita a troca de informações num ambiente seguro. Assim, se uma dessas chaves for utilizada para criptografar uma mensagem, a outra servirá para desencriptar. Ensina Augusto Tavares Rosa MARCACINI (2002, p.24) que

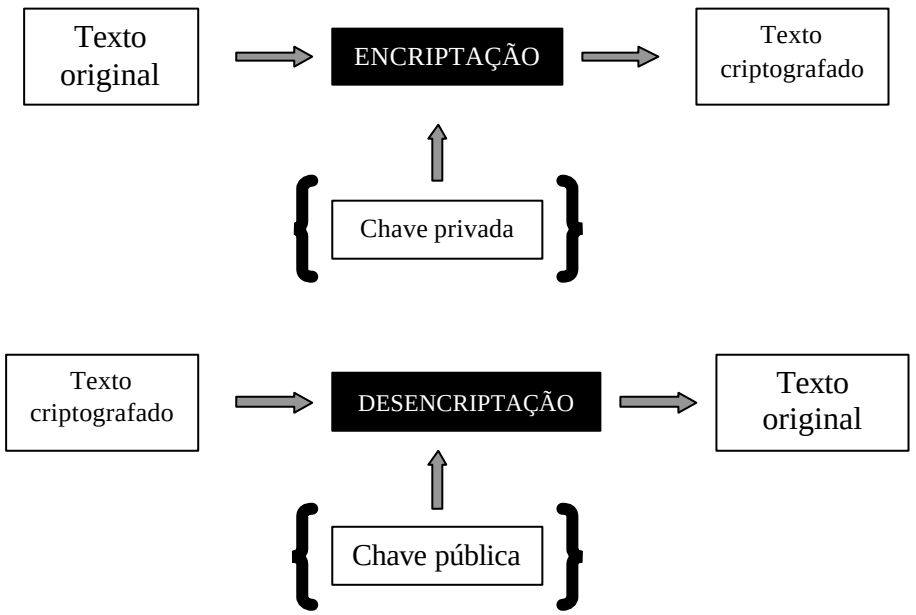
> ***Encriptando a mensagem com a chave pública, geramos uma mensagem cifrada que não pode ser decifrada com a própria chave pública que a gerou. Só com uma chave privada poderemos decifrar a mensagem que foi codificada com a sua correspondente chave pública. E o contrário também é verdadeiro: o que for encriptado com o uso da chave privada, só poderá ser decriptado com a chave pública.***

[44] MARCACINI, A. T. R., 2002, op. cit., p. 24.
[45] Apresentado no *National Computer Conference* (1976). ISAGUIRE, K. R., 2002, op. cit., p. 67.

Jean Carlos DIAS (2002, p.91) aponta sua aplicação como um sistema mais complexo no qual *"existe um par de chaves, sendo uma das chaves privada e outra pública. A chave privada codificaria a mensagem e a chave pública a decodificaria"*, e ainda acrescenta que "a *chave privada é secreta e por isso possibilita tanto a identificação do emitente da mensagem como garante o sigilo das comunicações"*.

A criptografia assimétrica pode ser, assim, representada[46]

Fig. 02 CRIPTOGRAFIA ASSIMÉTRICA



[46] Figura com base em Ângelo VOLPI NETO, **Comércio eletrônico**. Direito e Segurança. Curitiba: Juruá, 2002, p.59.

A Figura 02 demonstra o funcionamento da criptografia assimétrica, na qual o emissor do texto original, por meio de um programa o encripta utilizando uma chave privada. O receptor do texto, recebe e utiliza uma chave pública para desencripta-lo, possibilitando sua leitura, porém não poderá modificar o conteúdo. Com este procedimento o receptor passou a ter segurança do conteúdo do documento recebido, bem como, tem o real conhecimento de quem foi o emissor. Augusto Jun DEVEGILI & Aline Sueli de Salles SANTOS (2004, p.204-205) de forma didática, descrevem o funcionamento das trocas de chaves

> *A criptografia assimétrica difere da criptografia simétrica pela utilização de um par de chaves no lugar de uma única chave secreta. Este par é composto por uma chave pública, de conhecimento geral, e uma chave privada, de posse exclusiva da pessoa que a gerou. A característica da criptografia assimétrica é que informações encriptadas com uma chave pública só podem ser decriptadas com a chave privada equivalente e vice-versa. Para que Alice envie uma mensagem confidencial a Bob, ela deve encriptar essa mensagem com a chave pública de Bob que, de posse de sua chave privada, consegue decriptá-la. Como, em tese, ninguém tem acesso à chave privada de Bob ninguém pode decriptar a mensagem.*

A explicação permite observar que cada parte envolvida obtém uma chave diferente da outra e com funções diferentes. A primeira chave, a utilizada pelo emissor é a chave privada, a qual além de encriptar a mensagem permite a alteração do conteúdo. Cabe ressaltar que o único conhecedor desta forma de chave secreta é o seu titular. Outra é a chave pública, esta é enviada ao receptor visando a desencriptação e a leitura do texto, e pode ser distribuída livremente, ou seja, qualquer pessoa que a recebe tem permissão para a visualização do documento, mas não há possibilidade de alteração do mesmo. Assim não há a possibilidade de adulteração da informação.

Este par “chave pública/chave privada” tem entre si uma relação matemática e computacional, gerada através de programas utilizando cálculos algorítmicos. Estes programas, por sua complexidade e segurança, carregam

dispositivos que impossibilitam a eventual duplicação ou falsificação das chaves[47].

Nesse processo, várias vantagens podem ser identificadas, uma delas é destacada por Marlon Marcelo VOLPI (2001, p.15)

> *Uma vantagem para o usuário de um método de criptografia por chave pública é a possibilidade de um maior controle no envio de suas mensagens cifradas. Isto ocorre porque o emissor não precisa mais possuir uma chave secreta para cada destinatário. Basta somente que ele tenha a chave privada em sua exclusiva posse e a chave pública em posse de seu(s) receptor(es). Assim, ele poderá ter certeza de que, mesmo que mais de uma pessoa possua a chave pública, não será possível utilizá-la em nome do emissor.*

Ou seja, várias pessoas poderão ter conhecimento do conteúdo da mensagem, por meio da chave pública. Porém, apenas o emissor, possuidor da chave privada poderá escolher para quem enviar a mensagem encriptada sem modificar sua chave originária, além de poder modificar o texto.

O objetivo principal do método é a utilização visando a segurança e privacidade da informação. Mas isso gera uma outra função, essencial para a troca de informações eletrônicas, a autenticidade. A autenticidade, neste prisma, refere-se ao processo que o destinatário de uma mensagem deverá realizar para verificar a identidade de quem a enviou, além de assegurar a integridade da mensagem recebida. Assim, como a criptografia é utilizada para se atingir privacidade e segurança, a assinatura digital[48] também é utilizada para a verificação da autoria de uma mensagem.

Face ao apresentado, o método de criptografia assimétrica, é considerado um dos melhores sistemas de segurança, em virtude da chave privada

---

[47] MARCACINI, A. T. R.. 2002, op. cit., p. 24-27.

[48] A utilização do termo digital refere-se ao fato de que "digitalizar uma informação consiste em traduzi-la em números. Quase todas as informações podem ser codificadas desta forma". Assim, "a digitalização permite um tipo de tratamento de informações eficaz e complexo, impossível de ser executado por outras vias". LÉVY, P. 1999, op cit., p. 52-53.

ser de conhecimento apenas do seu titular e da autoridade certificadora que a emitiu. Porém, não se pode deixar de lado que sempre há a possibilidade da quebra de um sistema criptográfico, que pode ocorrer tanto no método simétrico quanto no assimétrico. A vantagem do assimétrico é que para sua quebra há a necessidade de se arcar com um alto custo, bem como, com um elevado tempo. Essas dificuldades tornam "quase" impossíveis à execução de qualquer forma de interceptação e leitura dos documentos criptografados.

O método de criptografia assimétrica tem como principal utilização a sua aplicação na assinatura digital, que tem por finalidade criar a possibilidade de assegurar um documento ou mensagem.

2.6
A assinatura digital

Por longo tempo, as assinaturas escritas são utilizadas em transações comerciais, financeiras e legais para identificar a concordância ou aceitação dos termos descritos em documentos. Face à necessidade de identificar um documento em papel, utiliza-se a assinatura manual, por meio de escritos únicos e especiais de cada pessoa. A esta são determinadas algumas características como indica Angelo VOLPI NETO (2002, p.50) "*Identificativa: indica quem é o autor do documento. Declarativa: significa assumir o conteúdo do documento pelo seu autor. Probatória: permite identificar se o autor da firma é efetivamente aquele que foi identificado como o próprio naquela assinatura*".

Antes mesmo de se falar em assinatura digital, é preciso compreender o significado do termo assinatura, que para Dinemar ZOCCOLI (2000, p.178)

> *Provém do latim assignare (que significa 'firmar com seu nome ou sinal'). O qual é formado com base no latim signum (sinal, marca, símbolo). 'Firmar', por sua vez provém do latim firmare e significa, originalmente, tornar-se seguro, estável, definitivo, fixo, corroborado, confirmado, ratificado. 'Assinatura' refere-se ao 'ato ou efeito de assinar' ou ao próprio 'nome escrito, firma' em si. Portanto, assinar alguma coisa tem o sentido genérico de apor-lhe um sinal, marca ou símbolo pessoal, com o fim de dar-lhe segurança, estabilidade, fixidez, corroboração, confirmação, ratificação.*

Nota-se que o indivíduo ao assinar está conferindo segurança a certo documento. O caráter individual carrega o valor de estabilidade e a capacidade de assegurar a validade daquele movimento escrito, a assinatura. A sua imutabilidade permite impingir a capacidade de verificação e ratificação, confirmando como verdadeiro e realizado a próprio punho.

Flavia LOZZI citada por ZOCCOLI (2000, p.178), destaca que

> *A aposição da assinatura é um gesto que contém um forte significado simbólico, suficiente, por si só, para fazer entender sua função: declarar própria as firmações externadas, sob as quais a firma vem aposta. Aquele que de próprio punho escreve seu nome ao sinal de uma declaração, se dá conta da solenidade do compromisso assumido, porque sabe que deixou um símbolo inconfundível da sua vontade de assumi-lo: a folha sobre a qual imprimiu a assinatura terá a custódia do que foi escrito, evidenciando eventuais tentativas de alteração, e fará testemunho frente a todos sobre o vínculo contraído, uma vez que o signatário dificilmente poderá esquivar-se do reconhecimento da firma como sua.*

A posição e a importância que a assinatura implementa em certo documento, pode ser destacada como a ocorrência da identificação da autenticidade conferida mediante o significado dado. Ou seja, a partir do momento em que se assina um documento, junto àquela "escrita do nome" está

também consignando o valor que ela carrega, da autenticidade, da segurança, e até mesmo da responsabilidade sobre o assumido e determinado naquele documento.

As assinaturas escritas à mão são amplamente aceitas como quase impossíveis de serem forjadas, pois as falsificações podem, facilmente, ser reconhecidas por especialistas em escrita. Mas existem outros meios[49] de assinatura em documentos como a mecânica, podendo se efetivar por meio da marca d'água, carimbo, e outros procedimentos aplicados em papel, normalmente utilizados junto à assinatura manuscrita.

A evolução da informática trouxe a necessidade de se conferir esta mesma autenticidade às assinaturas em meio digital, apostas nos documentos e mensagens enviadas. Inicialmente, eram apenas utilizadas as assinaturas eletrônicas que se efetivavam por meio de senhas, sinais, reconhecimento de voz, assinatura com caneta digital, entre outros. Estas formas de identificação eletrônica continuam sendo aplicadas, porém em virtude da insegurança que carregam pela fácil manipulação por terceiros, foi desenvolvido um novo processo denominado assinatura digital.

Dinemar ZOCCOLI (2000, p.180) ao analisar a aplicação da assinatura digital em documentos eletrônicos, ensina que, *"o termo 'assinatura' pode ser entendido como um 'lacramento' personalizado de seu conteúdo. O 'lacre', no caso, visa garantir a integridade, enquanto o fato de apresentar atributo de personalização permite garantir a integridade"*. Ou seja, a assinatura digital é o fechamento e a garantia conferida ao documento. É forma de reconhecimento da autenticidade desenvolvida para atender às necessidades de segurança. No momento, é o mecanismo digital utilizado para inserir confiança, segurança e autenticidade em documentos recebidos e enviados via Internet.

Um dos principais aspectos que permitem a diferenciação entre a assinatura digital e a assinatura manuscrita é a validade, como destaca Marlon Marcelo VOLPI (2001, p.53)

[49] Assinatura ainda pode ser representada por marca, desenho, sinete, carimbo, entre outros.

> *Um dos pontos determinantes na diferenciação entre a assinatura convencional e a assinatura digital é o aspecto da expiração da validade da última. Uma assinatura convencional representa a marca da vontade do signatário, independente do meio em que se origina. Entretanto, uma assinatura digital é confeccionada em meio a elementos diversos, que podem vir a facilitar sua adulteração, de acordo com a evolução da tecnologia.*

Ao analisar o funcionamento do mundo digital, nota-se que uma de suas principais características é o fato de que o documento emitido original não apresenta nenhuma diferença em relação à sua cópia, não há a assinatura manuscrita e nem mesmo uma impressão em papel. Assim, fácil seria a realização de eventuais fraudes e má-fé nos atos praticados. Outro aspecto, que pode ser levantado, é a possibilidade de interceptação e alteração dos documentos movimentados via Internet. Para tentar evitar estas ocorrências foi desenvolvida a assinatura digital.

O funcionamento da assinatura digital mantém a estrutura da utilização de chaves públicas e privadas, como esclarece Maurício MATTE (2001, p.38)

> *[...] em fechar um documento com uma chave privada, utilizando-se as técnicas de criptografia para cifrar esta, que somente poderá ser aberta com outra chave, denominada pública, ou vice-versa. A chave pública, é disponibilizada para as partes interessadas em realizar atos (no caso contratos), sendo que a chave privada é de responsabilidade e conhecimento exclusivo do proprietário (que pode ser uma pessoa física, jurídica ou um computador).*

Assim, define-se a assinatura digital, como sendo *"o resultado de uma operação matemática, utilizando algoritmos de criptografia assimétrica"* (MARCACINI, 2002, p.32). Ou seja, a assinatura digital não se confunde com o método de criptografia assimétrica, pois suas finalidades são diferentes. A da

assinatura digital é a de conferir confiabilidade ao conteúdo enviado na mensagem ou documento, por meio do envio de uma marca peculiar ao emitente. Isto ocorre em virtude do alto grau de segurança, pela possibilidade em verificar quem o enviou e o assinou. Augusto Jun DEVEGILI & Aline Sueli Salles SANTOS (2004, p.205) explicam e exemplificam a aplicação da assinatura digital da seguinte forma *"se Alice encripta um documento com sua chave privada, qualquer pessoa pode usar a chave pública de Alice para decriptar o documento, verificando portanto, que este realmente foi assinado por Alice".*

Um dos aspectos mais relevantes para o Direito concerne à validade do documento eletrônico, pois, uma vez assinado o documento, não mais poderá este ser alterado, sem que a assinatura eletrônica seja invalidada. Esta é a função que vem como garantidora da integridade do documento digital. Nesse sentido afirma Augusto Tavares Rosa MARCACINI (2003) que "a*s assinaturas digitais assim produzidas ficam de tal sorte vinculadas ao documento eletrônico 'subscrito' que, ante a menor alteração da assinatura, se torna inválida"*[50].

Assim, a técnica possibilita, além da identificação da autoria, a "*imutabilidade lógica*"[51] do documento. A assinatura digital, pela forma como se dá sua aplicação, traz, na verdade, a presunção de autenticidade, pelo fato de que, uma vez modificado o documento ou não combinando os dados necessários para a verificação, não há possibilidade da validação da assinatura.

Renato OPICE BLUM e Sérgio Ricardo Marques GONÇALVES (2001, p.297) destacam algumas características e finalidades da assinatura digital

> *Autentica o documento e é capaz de gerar conseqüências jurídicas, pois prova ao destinatário que o subscritor assinou o documento, tornando-o uma manifestação inequívoca da sua vontade.*
> *Não pode ser falsificada, pois somente o subscritor tem esta chave que lhe permite assiná-lo (esta presunção depende do autor manter sua chave em sigilo e de acordo com ditames que lhe foram impostos pela autoridade certificadora);*

---

[50] MARCACINI, A. T. R. **O documento eletrônico como meio de prova**. Disponível em: <www.advogado.com/internet/zip/tavares.htm>. Acesso em 03 ago. 2003.

[51] Ibid., não paginado. Define "*imutabilidade lógica*" como a possibilidade de "*que o documento continua podendo ser alterado, sem deixar vestígios no meio físico onde está gravado (esta, aliás, é uma importante característica do documento eletrônico, que vai, permitir desvinculá-lo do meio físico e transmiti-lo, via Internet); entretanto, a posterior alteração do documento invalida a assinatura, o que faz com que o documento deixe de ter valor como prova*".

> *Não pode ser usada de novo, pois ela se amolda ao documento em sua essência e, como tal, não pode ser transferida;*
> *Impede que o documento seja modificado em qualquer de suas características depois de assinado pelo autor, em virtude de se amoldar ao conteúdo existente no momento em que foi aposta ao texto;*
> *Não pode ser contestada se utilizar sistema aprovado e estiver com sua certificação válida. Torna-se uma prova de que o signatário marcou o documento*.[52]

Nesse sentido, percebe-se que existe um rigor maior no procedimento da utilização, pois, é ele que permite verificar a autenticidade do documento. A assinatura digital oferece recursos para inibir a falsificação, impossibilita a transferência e a duplicação do documento, bem como, reforça os mecanismos para impedir a violação dos documentos. A possibilidade de identificação e criação destas finalidades e características é proveniente da forma como a assinatura digital é concebida.

2.7
Criação da assinatura digital

Na atualidade, para a concretização da assinatura digital, faz-se necessária a utilização de novas tecnologias ligadas aos cálculos matemáticos. A evolução dessas tecnologias possibilita o desenvolvimento de mecanismos que trazem cada vez mais segurança em sua aplicação, Marlon Marcelo VOLPI (2001) ensina que podem ser identificadas as seguintes técnicas aplicadas à assinatura digital, dentre outras: a **Checksum,** a **Checagem de Redundância Cíclia (CRC),** a **Função Hash**[53]**,** os **Algoritmos RSA** e os **Algoritmos DAS (Digital**

[52] OPICE BLUM, R. da S.; GONÇALVES, S.R.M. As assinaturas eletrônicas e o direito brasileiro. In: SILVA JUNIOR, R. L. e WAISBERG, I. (org.) **Comércio eletrônico**. São Paulo: RT, 2001, p. 297.
[53] Um dos mais utilizado nos últimos tempos.

Signature Algorithm)[54]**.** Todas estas técnicas trabalham sobre algoritmos de autenticação, por meio da aplicação de um processo lógico-matemático, levando ao alcance da assinatura pretendida[55]-[56].

Uma vez que a assinatura eletrônica tem sua segurança pautada em chaves, há a necessidade de se compreender como ocorre esse processo. Deve-se observar que, a assinatura tem sua caracterização e formação por meio de um emaranhado de números, letras e símbolos, ordenados em conformidade com o programa executado.

O procedimento para criação da assinatura digital, mais usual, atende à seguinte forma: o autor do documento, utiliza um *software*[57], que realiza operações resumindo os dados formadores do documento, que têm por objetivo, em geral, enviar a terceiro. Para esta descrição, optou-se por apontar as técnicas mais utilizadas.

A *função hash*[58] é a mais comum. Seguindo a operação, o autor utiliza sua chave privada com o objetivo de encriptar o documento a ser enviado, assim aplicando à assinatura digital. Uma peculiaridade desta técnica, é que cada documento ou arquivo recebe uma assinatura digital diferenciada, ou seja, seu autor não poderá repeti-la[59].

Para cada pessoa que irá utilizar a assinatura digital, é criada uma espécie de selo eletrônico que é constituído por uma série de dados (letras, algarismos e símbolos), cuja aplicação na mensagem ocorre em dois momentos: por meio da função *"hash"* encriptada pela chave privada do remetente; e quando

---

[54] Para maior aprofundamento técnico-matemático consultar VOLPI, M. M., 2001, op. cit., p. 18-28.
[55] Estas técnicas também trabalham por meio de encriptação da própria assinatura.
[56] VOLPI, M.M., 2001, op. cit., p. 18-28.
[57] Que contém sua programação com algoritmos próprios.
[58] "*Um bom algoritmo hash possui duas propriedades muito importantes: - Os valores que são gerados são tão únicos e tão difíceis de serem duplicados, que nem mesmo alguém com um conjunto de supercomputadores e alguns séculos para processar conseguiria encontrar dois conteúdos diferentes que produzissem o mesmo valor hash. – Ser realmente de sentido único, ou seja, não ter a menor possibilidade de se reconstruir a mensagem original a partir do código hash gerado (também conhecido como message digest*)". Ibid., p.22.
[59] Ou seja, este procedimento é diferente da assinatura manuscrita, que deve ser repetida da mesma forma, ou com características próprias da grafia do autor. Esta modificação a cada assinatura traz segurança para os envolvidos, pois em tese ninguém poderá manipular o envio de documentos modificados.

o destinatário desencripta a mensagem com a chave pública do remetente e usa, novamente, a função "*hash*", comparando-a com a enviada pelo destinatário[60].

Dando continuidade ao procedimento, o documento é enviado ao receptor[61], contendo a assinatura digital. Este último, utilizando uma chave pública, realiza a desencriptação que permite o reconhecimento da autenticidade do documento recebido. Para esta operação, o receptor, utiliza os mesmos algoritmos aplicados pelo software do autor, aplicando a *função hash*, que procede ao resumo do documento recebido. Esses *códigos hash* criados são denominados como *message digest*. Depois de resumido, o documento recebido é comparado ao enviado e se compatíveis, resulta na verificação da autenticidade do documento.

Releva destacar que mesmo em se tratando da aplicação de um algoritmo de conhecimento de todos, para ser decifrado é necessária a obtenção das chaves correspondentes a sua criação.

Outra técnica, muito utilizada, é a do *algoritmo RSA*. O funcionamento do RSA segundo Marlon Marcelo VOLPI (2001, p.24), ocorre da seguinte forma *"... utilizando-se o algoritmo RSA, cria-se uma assinatura com base no conteúdo da mensagem. A partir de então, envia-se a mensagem concatenada à assinatura. Ao chegar no destinatário, a assinatura é decifrada e comparada com o conteúdo da mensagem. Se ambos ainda forem iguais, a mensagem é genuína"*.

Porém, esta técnica tem por desvantagem o fato do longo tempo para o envio e a grande exigência no processamento. Outra desvantagem prende-se ao aumento significativo do que foi enviado, uma vez que o arquivo se apresentará com o dobro do tamanho do original, pois soma ao original o conteúdo criptografado[62].

Em busca da solução para este problema, a técnica do *algoritmo RSA* se uniu à *função hash* para o desenvolvimento da assinatura digital. Com esta somatória, a cifragem não ocorre sobre o conteúdo todo, mas apenas sobre a *message digest*, ou seja, sobre os *códigos hash* criados. Assim, a possibilidade de verificação da autenticidade ocorre com o confronto da *message digest* enviada na

---

[60] BRASIL, A. B.. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=1782>. Acesso em 17 mar 2004.
[61] Também chamado de destinatário.
[62] VOLPI, M.M., 2001, op. cit., p. 25.

mensagem com o *valor hash* do receptor da mensagem, dando certeza ao seu conteúdo[63].

Outra técnica muito difundida é a dos *Algoritmos DSA (Digital Signature Algorithm),* sua fórmula base é diferente da técnica anterior. Segundo Marlon Marcelo VOLPI (2001, p.26) *"ele aplica um sistema de chave pública irreversível"*. Há uma grande complexidade de cálculos que envolvem esta técnica, mas não se pode deixar de lado que ao receber a mensagem também faz parte do processo a *função hash*[64]. Essa técnica exigiu o desenvolvimento de cálculos de grande complexidade, porém, dentro do seu funcionamento complexo e de sua aplicação aproveita as propriedades da *função hash.* Cabe ressaltar que esta utilização ocorre no momento da recepção da mensagem.

Para o usuário a semelhança entre as duas principais técnicas, ou seja, o DAS e o RSA, é muito grande. Na verdade, sua opção por uma ou outra se efetivará em sua aplicação. Nesse sentido, Augusto Tavares Rosa MARCACINI & Marcos COSTA (2004, p.69) esclarecem

> *Do ângulo econômico, devemos ressaltar que a utilização da criptografia é hoje algo muito barato, gratuito até, se considerarmos que os algoritmos RSA, DSA... têm uso liberado, sem reserva de direitos ou patentes, e existem diversos softwares livres, de código aberto, que implementam eficientemente as funções de cifrado, assinatura e gerenciamento de chaves.*

Face à evolução da tecnologia, sua agilidade e necessidade de segurança, novos métodos, certamente, serão desenvolvidos, gerando uma gama de opções aos usuários que escolherão conforme suas necessidades.

---

[63] Ibid., p.25.
[64] Ibid., p.27.

2.8
O Certificado digital e a autoridade certificadora

A assinatura digital é realizada por meio da criptografia assimétrica pautada no método de chaves públicas e privadas. Cabe o questionamento sobre a segurança de quem foi o real emissor da chave pública.

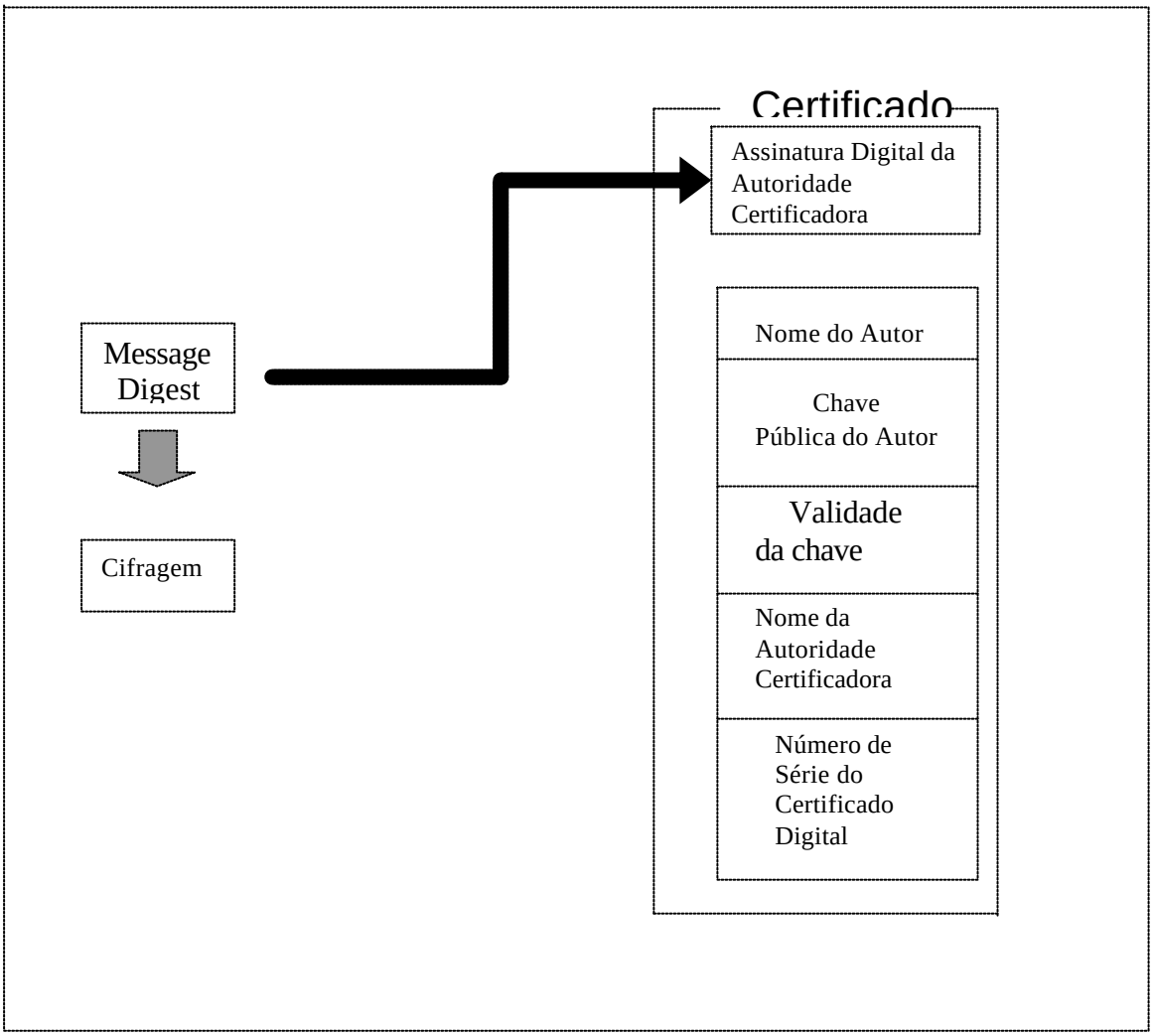
Um meio efetivo de responder a este questionamento relaciona-se à segurança sobre quem a enviou, por meio da verificação do certificado digital. Ou seja, o atestado que uma Autoridade Certificadora emite informando e garantindo que determinado indivíduo ou empresa detém certo par de chaves. Assim o certificado permite identificar quem emitiu a chave pública.

Augusto Tavares Rosa MARCACINI, Marcos COSTA & Pedro Antonio Dourado REZENDE (2003) facilitam e esclarecem o entendimento de certificado digital

> *Há grande confusão sobre o que seja um certificado digital. Um certificado digital é uma declaração de seu emissor, realizada por meio eletrônico e formato digital padronizados, quanto à titularidade de uma chave pública, nele transportada. Não se pode confundir, pois, entre o que está sendo declarado (a eficácia da declaração), o que está sendo transportado (a chave pública), e o meio eletrônico pelo qual são produzidos tais declarações e transportes (a ICP), do qual a entidade certificadora participa apenas como endossante ou avalista.*

Assim, o certificado digital é uma garantia da capacidade e viabilidade de determinada chave pública, conferindo confiança sobre quem é o autor e emissor da mesma. Bem como, determina a responsabilidade da autoridade certificadora para avalização e endosso dos certificados.

Marlon Marcelo VOLPI (2001, p.37) demonstra que o certificado digital tem sua aplicação resumida da seguinte maneira [65]



Segundo o fluxograma representado na fig. 03, há uma chave pública inserida no certificado digital. Por meio desta chave, é permitida a verificação da validade da assinatura digital do documento enviado, ou a possibilidade de que este seja decifrado, em virtude do modo que foi enviado. A veracidade da informação dada a respeito da assinatura está sob a responsabilidade da Autoridade Certificadora.

[65] Fonte: VOLPI, M. M. **Assinatura Digital:aspectos técnicos, práticos e legais**. Rio de Janeiro: Axcel Books, 2001, p. 37.

Assim, por meio de outros processos de segurança, a Autoridade Certificadora é a responsável pela emissão e criação das chaves públicas e privadas, envolvidas na encriptação e desencriptação do documento[66]. O certificado digital ocorre sob a forma de aplicativos de *software* que permitem a identificação de quem é o seu usuário. Esta Autoridade deve ser reconhecida e habilitada por lei. O objetivo principal é conceder as chaves e possibilitar a consulta dos certificados emitidos a qualquer pessoa e a qualquer tempo.

Michael FROOMKIN (1996, p.83) define Autoridade Certificadora como *"um órgão, público ou privado, que procura preencher a necessidade de uma terceira parte de confiança no comércio eletrônico que fornece certificados digitais, atestando algum fato acerca do sujeito do certificado*"[67]. Assim, a Autoridade Certificadora trabalha na comprovação, por meio de emissão de um certificado, de que o assinante daquele documento digital é realmente e seguramente a pessoa com quem a outra parte está se relacionando.

Não se pode deixar de lado a importância da conceituação de certificado. Segundo Michael FROOMKIN (1996, p.102) *"um certificado é uma afirmação emitida por uma Autoridade de Certificação que provê a confirmação independente de um atributo afirmado por uma pessoa titular de assinatura digital*"[68]. Assim, o certificado é o documento cuja fonte oficial cria a certeza de que aquela pessoa é o titular daquela assinatura digital e da chave pública utilizada e, por conseguinte, também da correlata chave privada. Pode ser considerado um documento notarial[69], cujo conteúdo é composto pelo nome e demais elementos identificadores da pessoa titular, pela chave pública que lhe é atribuída e pela assinatura digital e chave pública da autoridade certificadora[70].

Outra atividade comumente realizada pelas Autoridades Certificadoras prende-se à elaboração e à disponibilização de uma lista informativa contendo um

---

[66] CERTISIGN. Certificadora Digital Ltda. Disponível em <http://www.certisign.com.br>. Acesso em 26 mar. 2004.

[67] "*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 certicate*." FROOMKIN, M.. **The essential role of trusted third parties in electronic commerce**. Oregon Law Review, 1996, 75 v., p. 83.

[68] "*A Certificate is a digitally signed statement by a CA that provides independent confirmation of an attribute claimed by a person proffering a digital signature*". Ibid., p.102.

[69] Aquele produzido, autenticados ou reconhecido por Cartórios – Tabeliães.

[70] CERTISIGN, 2004, op. cit.

rol de certificados que foram revogados, pelos mais diversos motivos, ou seja, que foram cancelados e, assim, perderam sua validade. Essas informações formam a denominada Lista de Certificados Revogados. Um dos motivos mais comuns de inserção de certificados nesta lista é a perda ou extravio da chave privada pelo seu detentor.

Face ao aspecto positivo da verificação de uma assinatura digital, denota-se um alto grau de certeza jurídica à autenticidade, à autoria e à integridade do documento no qual seja ela aplicada. Em especial, porque comprova seguramente que o documento não foi alterado desde seu envio e que a assinatura foi utilizada por seu titular.

2.9
Capacidade de segurança

O comércio eletrônico, bem como, as trocas de documentos, apresentam certa resistência quanto à sua execução, no Brasil e no mundo todo, motivada pela falta de segurança das informações existentes na Internet. Com a finalidade de viabilizar e difundir cada vez mais a assinatura digital e de criar normas reguladoras, há também a necessidade de tecnologias de segurança aplicadas aos envolvidos.

As tecnologias de segurança permitem a realização de vários atos seguros dentro da capacidade tecnológica, como o envio de valores por meio de envelopes eletrônicos ou mensagens sigilosas. A segurança dos seus conteúdos impossibilita o acesso a terceiros não envolvidos na relação. Gustavo Testa CORRÊA (2000, p.82) citando Daniel BERNSTEIN, esclarece que "(...) *o desenvolvimento continuado da criptografia promete fazer possível com que o mundo da Internet ofereça privacidade, segurança e comunicação protegida entre bilhões de pessoas mundialmente*".

Ainda, seguindo as contribuições de Gustavo Testa CORRÊA (2002, p.82) ao analisar a criptografia sob o prisma da segurança, destacam-se as seguintes possibilidades a serem alcançadas

- *tornar original uma mensagem enviada por correio eletrônico, mediante a utilização de assinaturas digitais;*
- *tornar documentos pessoais inacessíveis e, assim privados;*
- *verificar a identidade de outra pessoa online, que esteja acessando a rede;*
- *verificar a fonte provedora de um arquivo que está sendo copiado; em outras palavras, tornar o 'download' mais seguro;*
- *proteger transações financeiras;*
- *habilitar o fluxo de caixa digital na Internet;*
- *proteger a propriedade intelectual;*
- *evitar opiniões ilegais e puni-las;*
- *proteger a identidade e a privacidade de todos.*

Tais aspectos demonstram que a criptografia é o método mais aplicável na busca de um ambiente digital mais seguro. Ao analisar essas indicações destaca-se uma conseqüência de cunho jurídico e prático, referente a assinatura do documento. Uma vez assinado nada mais poderá alterá-lo sem invalidar a assinatura presente, garantindo a integridade do documento. Ou seja, a capacidade de tornar um documento sigiloso, seguro e inviolável torna-se inerente às assinaturas digitais, pois oferece uma arma considerada vitoriosa no combate a eventuais problemas de invasões na rede.

Face às possibilidades, características e necessidades que envolvem a assinatura digital, segundo Dinemar ZOCCOLLI (2000, p.190) pode-se eleger, as principais propriedades como *'[...] conferir autenticidade ao documento, pois quando alguém utiliza a chave pública devidamente certificada de determinada pessoa, conseguindo decifrar um documento eletrônico dela recebido, esse alguém tem a garantia de que foi, realmente, essa pessoa indicada quem produziu o referido documento* , pois, somente quando há um documento eletrônico assinado se tem a certeza e a confiança de quem o emitiu.

Outra propriedade destacada por Dinemar ZOCCOLLI (2000, p.190) diz respeito a *"[...] não-falsificabilidade, pois somente o proprietário deve*

conhecer sua chamada chave privada e somente ela, nenhuma outra, é capaz de fazer par com sua chave pública certificada;". A aplicação da assinatura digital por meio da criptografia assimétrica, permite a criação de inúmeros pares de chaves, porém nenhum par será idêntico a outro. O autor indica ainda a "[...] *possibilidade de autocertificação quanto à integridade do documento eletrônico, uma vez que, havendo qualquer alteração de seu conteúdo cifrado (ainda que seja de um único bit em bilhões),*" que resulta na *"negativa a autenticação, pouco importando que se faça uso da chave pública correta (aquela que faz par com a chave privada, usando um processo de cifragem criador da firma*[71] *digital)*".

Outras propriedades são acrescidas por ZOCCOLLI (2000, p.190) como "[...] *não-reutilizabilidade, uma vez que a firma digital é gerada a partir de um cálculo efetuado em função do conteúdo específico de cada documento, não havendo possibilidade de transferência da firma digital, de um documento para outro;*" bem como a possibilidade do "[...] *não-repúdio, uma vez que a pessoa que recebe um documento eletrônico portador de firma digital não necessitará, em nenhuma hipótese, de ajuda ou intervenção do autor para reconhecimento de sua firma digital – garantindo-se, assim, a autenticidade, uma vez que não será possível o autor, eventualmente, sustentar uma negativa de autoria*".

Face às colocações do referido autor, pode-se concluir que os aspectos técnicos que envolvem a assinatura digital, os aplicativos e resultados provenientes dela, geram segurança e confiança em sua utilização.

[71] O autor ora citado compreende firma digital no mesmo sentido que trata a assinatura digital.

3
ASPECTOS JURÍDICOS DA DOCUMENTAÇÃO ELETRÔNICA

3.1
Breve introdução: fato, ato e negócio jurídico

Ao observar as condições de segurança e confiança oferecidas pela assinatura digital com a certificação eletrônica por uma autoridade competente, destaca-a a possibilidade de serem identificadas nas mais variadas formas de fatos jurídicos. Aqui se denota a necessidade da diferenciação entre negócio, ato e fato jurídico visando esclarecer o posicionamento dos documentos eletrônicos na esfera jurídica. Os fatos jurídicos, são definidos por Francisco AMARAL (2003, p.343) como os *"acontecimentos que produzem efeitos jurídicos, causando o nascimento, a modificação ou a extinção de relações jurídicas e de seus direitos"* e por este motivo são relevantes ao Direito.

Nota-se que os fatos jurídicos podem ser identificados em todas as ocorrências que geram efeitos no âmbito jurídico. Assim, frente às repercussões geradas, estes fatos passam a receber atenção e conseqüências determinadas pelas normas jurídicas. Destaca, Fábio ULHOA COELHO (2003, p.278-279) que *"toda norma jurídica, inclusive a de direito civil, pode ser descrita como a indicação de um evento ao qual liga uma conseqüência. O evento descrito como pressuposto é um fato jurídico"*.

Para Francisco AMARAL (2003, p.343) os fatos jurídicos são denominados *"positivos, quando implicam uma ação ou declaração de vontade, e negativos, quando consistem em uma abstenção ou omissão"*. Pode-se indicar como exemplo de positivo a celebração de um contrato e como negativo o silêncio (não manifestação) que gera a possibilidade de prorrogação automática de acordos.

A doutrina tradicional[72] apresenta a seguinte classificação para os fatos jurídicos: *voluntários, naturais* ou *humanos* são aqueles que decorrem da vontade humana; e *involuntários* aqueles que mesmo sem a presença da vontade consciente *"poderão produzir repercussões que atingirão o patrimônio jurídico de determinadas pessoas conforme as peculiaridades daquelas ocorrências"*[73].

Assim, Fábio ULHOA COELHO (2003, p.278) indica que *"se fato jurídico é a conduta de um sujeito de direito, chama-se ato jurídico"*. Ou seja, é a ação pela qual os indivíduos, sujeitos de direito, criam resultados estabelecidos em norma e com isso passam a ser considerados espécies de fato jurídico.

Os atos jurídicos provêm da efetivação da vontade dos sujeitos de direito, porém, tais atos, para serem jurídicos, devem apresentar certo revestimento decorrente do Direito positivado[74]. Caio Mário da Silva PEREIRA (2004, p.475) ensina que

> *Não são todas as ações humanas que constituem atos jurídicos, porém apenas as que traduzem conformidades com a ordem jurídica, uma vez que as contravenientes às determinações legais vão integrar a categoria dos atos ilícitos, de que o direito toma conhecimento, tanto quanto dos atos ilícitos, para regular-lhes os efeitos, que divergem, entretanto, dos destes, em que os atos jurídicos produzem resultados consoantes com a vontade do agente, e os atos ilícitos sujeitam a pessoa que os comete a conseqüência que a ordem legal lhes impõe (deveres ou penalidades).*

Dentre os atos jurídicos existentes podem ser apontados os atos que possuem *"a intenção de gerar a conseqüência prevista na norma jurídica (isto é, produzir certo efeitos), denomina-se negócio jurídico"*[75]. Nesse sentido pode-se definir os atos jurídicos como uma espécie de ato humano com caráter volitivo[76] que fundamenta a concretização da regra jurídica que geram a eficácia jurídica.

---

[72] Nesta doutrina tradicional podem ser destacados Caio Mário Pereira da Silva, Francisco Amaral, entre outros.
[73] DIAS, J. C., 2002, op. cit., p. 22-23.
[74] PEREIRA, C.M.S. **Instituições de Direito Civil.** Introdução ao Direito Civil. Teoria Geral de Direito Civil. 20ª ed., Rio de Janeiro: Forense, 2004, v. 1, p. 475.
[75] ULHOA COELHO, F. **Curso de Direito Civil.** São Paulo: Saraiva, 2003, v 1., p. 279.
[76] No sentido de estar inserido na manifestação da vontade, ou própria e claramente manifestado.

A análise doutrinária do negócio jurídico relaciona-se diretamente com o estudo da declaração de vontade destinada ao alcance de certo objetivo ou efeito jurídico. Francisco AMARAL (2003, p.371) a define como "a *declaração de vontade privada destinada a produzir efeitos que o agente pretende e o direito reconhece"*.

Ao examinar os negócios jurídicos não se pode descartar a necessidade do reconhecimento do suporte fático que carregue relevância ao mundo do Direito, para isso, faz-se necessária a incidência de uma norma jurídica. Com isso, busca preencher todos os elementos essenciais para este suporte. Assim, em se tratando da validade, destacam-se como elementos: a capacidade do agente, a legitimidade de partes, o consentimento livre, o objeto determinado e possível e a forma prescrita ou não vedada em lei[77].

Porém, à real produção do negócio jurídico é necessário, também, a presença de fatores determinantes de eficácia, Antonio Junqueira de AZEVEDO (1986, p.65) os interpreta como *"algo intrínseco ao negócio, algo que dele não participa, que não integra, mas contribui para a obtenção do resultado visado"*.

Algumas vezes o negócio jurídico também recebe a denominação de ato jurídico *stricto sensu*[78]- [79], porém, na verdade, tal denominação refere-se a ação de vontade sob uma estrutura simples, ou seja, é voluntário. Mas no negócio jurídico a vontade tem por objetivo a normatividade e a vinculação, que se traduzem na manifestação e na limitação imposta pelos interesses das partes.

O direito privado, ao contemplar a autonomia da vontade, aponta um dos seus princípios. A autonomia da vontade indica que aos sujeitos de direito, cabe a liberdade no pacto sobre seus interesses, como indica Fábio ULHOA COELHO (2003, p.289) *"a vontade do sujeito só produz efeitos por ele pretendidos quando a lei o determina. Os efeitos de direito, assim, são sempre produzidos pela norma, ao atribuir conseqüências aos fatos jurídicos"*.

---

[77] Conforme determina o artigo 104 do CCB/2002: *"A validade do negócio jurídico requer: I- agente capaz; II – objeto lícito, possível, determinado ou determinável; III – forma prescrita ou não defesa em lei"*.

[78] Denominação dada pela doutrina tradicional.

[79] Inicialmente pode-se conceituar ato jurídico *"lato sensu"* como ato que *"abrange as ações humanas, tanto aquelas que são meramente obedientes à ordem constituída, determinantes de conseqüências jurídicas ex lege, independentemente de serem ou não queridas como aquelas outras declarações de vontade, polarizadas no sentido de uma finalidade, hábeis de produzir efeitos jurídicos"*.PEREIRA, C.M.S., 2004, op. cit., p. 475.

Nota-se que a vontade manifestada pelos sujeitos, objetivo do alcance do negócio jurídico, alcançará apenas os resultados oriundos da permissão decorrente das normas. Estes podem ser produzidos pela norma de forma direta quando trata de fatos independentes da vontade dos sujeitos, e, indireta quando aponta fatos ligados a vontade dos envolvidos[80].

Sobre a declaração de vontade contida nos contratos eletrônicos ensina Jorge José LAWAND (2003, p.138)

> *Ora, a declaração de vontade emitida eletronicamente não é outra coisa senão uma mensagem de dados, com variedades de configurações, dependendo do sistema [...] aliada a métodos de assinatura eletrônica, como a criptografia com chaves duplas[81], que contém a vontade de comprometer-se do seu iniciador e signatário num caso concreto.*

Assim, mais uma vez fica clara a importância não só da declaração da vontade das partes, mas também da garantia dessa vontade por meio da assinatura digital nos documentos eletrônicos. Principalmente, pelo motivo dos envolvidos não estarem fisicamente presenciando a assinatura destes documentos. Com isso a assinatura digital é a responsável pela garantia da manifestação da vontade nos documentos eletrônicos, uma vez que não permite sua alteração, violação ou mesmo acesso sem a autorização (envio da chave pública) do emissor.

3.2
Documento eletrônico como forma de materialização do negócio jurídico

[80] ULHOA COELHO, F., 2003, op. cit., p. 290.
[81] No mesmo sentido de utilizar uma chave pública e outra privada, ou criptografia assimétrica.

Os documentos podem ser considerados como meio de prova da existência de certo negócio jurídico nele contido, no entanto, não será sob este enfoque que serão analisado nesse trabalho. Os documentos, no presente estudo, foram considerados como forma de materialização de manifestação da vontade em negócios jurídicos, no sentido da certeza, segurança e confiança deles extraídas, em virtude da assinatura digital.

Antes de analisar o conceito de documento eletrônico deve-se destacar que a doutrina jurídica traz várias referências sobre a terminologia do que é documento. Assim, Moacir Amaral SANTOS (1997, p.385) define documento como a representação de um fato com o objetivo de fixá-lo, garantindo sua permanência e idoneidade, permitindo sua reprodução.

Marco Aurélio GRECO (2000, p.207) define documento como "*qualquer base de conhecimento, fixada materialmente e disposta de maneira que se possa utilizar para consulta, estudo, prova, etc.*". O citado retrata o documento como forma de materialização de conhecimento que proporciona a oportunidade de examinar seus conteúdos.

José Frederico MARQUES (1997, p.233) descreve documento como *"a prova histórica real consistente na representação física de um fato"*. Conceito que define o documento sob o enfoque de sua exteriorização e materialização.

Ao apresentar sua definição de documento Humberto THEODORO JUNIOR (2001, p. 393) amplia a definição, defendendo que documentos "*não são apenas os escritos, mas toda e qualquer coisa que transmita diretamente um registro físico a respeito de algum fato, como os desenhos, as fotografias, as gravações sonoras, filmes cinematográficos, etc.".* Com sua contribuição abrange outras formas de documentos como gráficos, fonográficos, fotográficos e outros.

Ana Paula LORENZONI (2005, p.142) esclarece que

> *[...] o documento se consubstancia numa coisa, fixada materialmente. Por isso, a dificuldade de separar o conteúdo do seu suporte físico. Esse vínculo que nos permite unir a informação ao elemento coisa – res, algo tangível, palpável passa a ser confundido com seu próprio suporte, que é mero instrumento.*

Aponta de forma crítica os conceitos arraigados à tangibilidade dos documentos que por ventura afastam a sua real importância que é o conteúdo.

Face a essas conceituações e definições nota-se que o documento público ou privado[82], a princípio, tem por função básica manter, seja qual for sua forma, o registro fiel, confiável e seguro de um fato ou negócio jurídico. Porém, esta função deve se aperfeiçoar, no sentido de abarcar novas finalidades e concepções, provenientes do desenvolvimento tecnológico, como no caso dos documentos eletrônicos.

O documento eletrônico, também denominado de documento digital ou informático, é produzido por meio da utilização de computador[83]. Ou seja, é a formação de um documento com o uso de uma nova tecnologia. Este documento, ainda, pode ser considerado como aquele que se encontra inserido e gravado em formato digital, ao alcance dos envolvidos, apenas, com a utilização do computador e de um programa adequado, em especial com a utilização da assinatura digital conferindo segurança e confiança aos dados armazenados.

Para a compreensão do conceito de documento eletrônico Augusto Tavares Rosa MARCACINI (2002, p.67) sustenta que se deve analisá-lo com um grau significativo de abstração. Assim, observando-se o documento tradicional, pode ser identificado um apanhado de átomos, micro-partículas que unidas formam um objeto (papel) com a possibilidade de transmissão de informações. E, por outro lado, o documento eletrônico reconhecido pela formação de uma seqüência de bits, que por meio do computador e do programa adequado permite a transmissão de informações.

Assim, ao se conceituar o documento digital, pode-se defini-lo como uma espécie de representação da realidade, sob o aspecto gráfico, sonoro,

---

[82] Não se pode deixar de lado a existência de duas formas de documentos os públicos e os privados. Caio Mario da Silva PEREIRA (2004, p.594) define os públicos como *"os que constam dos livros e notas oficiais, ostentando igual força publica as certidões e os translados que o oficial público extrai dos instrumentos e documentos lançados em suas notas (art 217,CCB), bem como as certidões fornecidas pelas autoridades competentes, de atos ou fatos existentes nas repartições e departamentos administrativos. O mesmo vigor de documento público conservam as certidões passadas pelos escrivães judiciais, dos documentos e atos processuais existentes ou ocorridos nos processos que lhes são afetos, se originais se houverem produzido em Juízo, como prova de alguns atos (arts.216 e 218, CCB)...Os requisitos do instrumento público estão mencionados em detalhes no art. 215 do Código Civil"*. E por documentos privados ou particulares entende como *"aqueles escritos elaborados pelos próprios interessados, totalmente escrito e por estes assinados, ou somente assinados, sendo escrito por outrem ou datilógrafos, digitados ou impressos"*.

[83] ISAGUIRRE, K.R., 2002, op. cit., p. 55.

impresso ou qualquer outra forma, desde que permita garantir certeza, impossibilidade de mudança (no caso de mudança passa a ser identificáveis) e determinação dos sujeitos.

O conceito jurídico de documento trata da representação material que visa produzir ou reproduzir certa manifestação do pensamento e da vontade da parte, nas mais variadas formas possíveis, bem como, sendo referende aos mais variados assuntos. E, tal manifestação do pensamento pode ou não prescindir de uma assinatura, conforme ensina Giuseppe CHIOVENDA (1994, p.83)

> *O escrito, como ato destinado a reproduzir o pensamento, só é perfeito, em regra, quando traz a assinatura da pessoa de que provém. Sem embargo, pode haver escrito importante sem assinatura, sendo, por isso, imperfeita (minuta de contrato, de cartas de apontamento escrito interrompido por impedimento, e outros): mesmo esse escrito pode servir de prova; prova por certo o fato de que determinada pessoa escreveu determinadas palavras [...] Outras vezes o escrito não está firmado porque, por sua natureza, não requer assinatura alguma (anotações de registro, por exemplo).*

Por analogia o documento eletrônico pode ser considerado como uma espécie de representação material de certa manifestação do pensamento, porém, fixada num ambiente eletrônico. Ou seja, não há visualização deste documento sob a forma escrita, e nesse sentido afirma Katya Regina ISAGUIRRE (2002, p.55) que *"os documentos eletrônicos propriamente ditos são aqueles que se formam e são entabulados por meio de processos eletrônicos, como a Internet"*.

Portanto, inafastável o fato de que, em nenhuma das análises sobre a definição de documento indica-se apenas a necessidade da utilização de papel, ou seja, fixou-se no aspecto material do conhecimento ou da informação. A questão do papel foi apenas uma questão de usos e costumes, e assim aderiu à noção de documento erroneamente.

Ana Paula LORENZONI (2005, p.144) define documento eletrônico como *"aquele que se encontra memorizado em forma digital, sendo percebido pelo homem somente com o auxílio de um programa de computador"*. Assim,

retrata a forma com que se pode identificar e possibilitar a leitura de um negócio jurídico formatado e armazenado digitalmente.

Em face da volatilidade carregada pelos documentos eletrônicos, faz-se necessário garantir sua integridade e a sua procedência antes de lhe atribuir qualquer valor. Conforme estudado no capítulo anterior, essas garantias podem ser obtidas por meio do emprego de um par de chaves, provenientes de um método assimétrico de criptografia, fornecida pela Autoridade Certificadora.

Augusto Tavares Rosa MARCACINI (2002, p.66) define documento eletrônico como aquele que

> *Não se prende ao meio físico em que está gravado, revestindo-se de autonomia em relação a ele. O documento eletrônico é, então uma seqüência de bits que, traduzida por meio de um determinado programa de computador, seja representativa de fato. Da mesma forma que os documentos físicos, o documento eletrônico não se resume em escritos: pode ser um texto escrito, como também pode ser um desenho, uma fotografia digitalizada, sons, vídeos, enfim, tudo que puder representar um fato e que esteja armazenado em um arquivo digital.*

Adotando o conceito comparativo elaborado por Augusto Tavares MARCACINI (2002, p.66) pode-se traçar um paralelo entre as características do documento físico e do documento eletrônico, quanto à sua representação. Ao analisar o meio físico, leva-se a afirmar que o documento pode ser definido como aquele representado de forma tangível, ou seja, em papel, como indica Augusto Tavares Rosa MARCACINI (2002, p.68) *"único"*, apenas dando possibilidade a cópias ou reproduções. E o documento eletrônico também único, porém em ambiente diferente, mas também passível à cópias sem a alteração do original devido a aplicação da assinatura digital.

Pode-se definir documento eletrônico, de acordo com a contribuição de Newton DE LUCCA (2001, p.44) como *"o meio real de representação de um fato, não o sendo porém, de forma gráfica*" no qual *"a diferença residirá, portanto, tão-somente, no suporte do meio real utilizado, não mais representado pelo papel e sim por disquetes, disco rígido, fitas ou discos magnéticos etc.*". Assim, uma vez que vem em substituição aos documentos em papel, a

preocupação aqui trazida retrata a questão da validade jurídica do mesmo, ou seja, se a contratação eletrônica terá ou não valor jurídico, como por exemplo, quanto à compra e venda de um imóvel, a qual requer a emissão de uma escritura pública com as devidas formalidades, que podem perfeitamente ser emitidas eletronicamente.

Ao analisar as possíveis relações jurídicas realizadas ou a serem concretizadas em ambiente eletrônico, nota-se a necessidade de serem assegurados elementos básicos como a privacidade, a segurança de dados, a confidencialidade de documentos, a autenticidade dos documentos eletrônicos.

Analisando a autenticidade, Francesco CARNELUTTI (2002, p.204) define como a *"[...] verdade da indicação do autor, e singularmente, da subscrição, ou seja, a correspondência entre o autor aparente e o autor real[...]"*. Entende-se a autenticidade como a verdade consubstanciada pelos documentos.

É a assinatura digital que permite garantir que aquele documento ou contrato eletrônico realmente provém do indivíduo que se diz autor, conforme destaca Dinemar ZOCCOLLI (2000, p.186)

> *Daí a necessidade de se instituir formas juridicamente tuteladas de "autenticação" dos documentos eletrônicos. Entenda-se o ato de "autenticar" (ou "certificar") como sendo um procedimento tendente a determinar, com máxima segurança, autenticidade, a integridade de conteúdo e a tempestividade de um determinado documento eletrônico. Ou seja, em outras palavras, "autenticar" significa conferir o cumprimento dos requisitos exigíveis à confiabilidade da prova documental.*

Para que se proceda a relação jurídica digital, uma das primeiras necessidades, por meio da identificação segura, é a verificação da capacidade jurídica das partes envolvidas. Principalmente por ser um requisito de validade dos contratos, é de fundamental importância para a concretização do pretendido, seja uma contratação ou negociação eletrônica.

Face ao objetivo do desenvolvimento da confiança nos documentos eletrônicos, a autenticidade e a impossibilidade de adulteração, são consideradas

requisitos básicos e imprescindíveis para a validade de um contrato eletrônico[84]. Na verdade, esta é a busca de todos os usuários da assinatura digital em suas relações jurídicas.

Em conformidade ao já apresentado no Capítulo 2 do presente estudo cabe a contribuição de Marcus Alexandre da SILVA (2005) ao definir que *"o documento eletrônico constitui-se como a troca de informações entre duas ou mais partes, através de sistemas que utilizam conceitos criptográficos de chaves públicas e privadas, e não se perfaz com sua materialização no papel, mas sim, com sua execução no mundo virtual"*.

Uma característica de diferenciação entre o documento eletrônico e o documento em papel trata, como já analisado anteriormente, da aplicação da assinatura. Ora, um documento eletrônico não possibilita a assinatura tradicional, ou seja, escrita; porém há a possibilidade da aplicação de uma forma própria, ou seja, da assinatura digital.

A possibilidade de se implementar validade, confiança e segurança de armazenamento e recuperação por intermédio da criptografia assimétrica, é cabível ao reconhecimento jurídico da utilização do documento eletrônico, principalmente, pela ampla utilização na Internet. Este reconhecimento dos documentos eletrônicos concretiza e efetiva as formas mais modernas de realização dos negócios jurídicos, os contratos eletrônicos.

3.3
Contratos eletrônicos

Para analisar os contratos eletrônicos como meio de aplicação da assinatura, há a possibilidade do reconhecimento das garantias de segurança e

[84] MARTINS, G. M. **Contratos eletrônicos via internet:** problemas relativos à sua formação e execução. São Paulo: Revista dos Tribunais, jun. 2000, p. 92-106, 776 v., p. 101.

confiança dos negócios jurídicos[85]. Decorrente das modificações das formas de contratação, em virtude da utilização das novas tecnologias de telecomunicação e informática, os negócios jurídicos deixaram de ser concretizados apenas por meio de fax, escrita, por telefone ou oral, passando a serem realizados e efetivados com o emprego de computadores em ambiente virtual.

Ao analisar os documentos eletrônicos podem ser identificadas três formas de contratação: intersistêmicas, interpessoais e interativas. Por contratações **intersistêmicas** entende-se aquelas nas quais *"a comunicação eletrônica se estabelece entre sistemas aplicativos previamente programados, estando ausente a ação humana no momento em que a comunicação se realiza[86]"*. Ou seja, aqueles pautados em protocolos padrão de documentos, normalmente aproveitados em redes fechadas com a utilização de aplicativos específicos[87].

Outra forma de contratação eletrônica é a **interpessoal**, a qual Manoel J. Pereira SANTOS (2000, p.195) define como sendo aquela *"em que a comunicação eletrônica se estabelece para a formação da vontade e para a instrumentalização do contrato, não sendo apenas forma de comunicação da vontade já constituída ou forma de execução de contrato concluído previamente"*. É a forma mais difundida entre a grande maioria dos internautas, pois é a contratação efetivada nos *Chat rooms*[88] ou por *e-mail*[89] nos quais qualquer pessoa poderá concretizá-la, ou seja, tanto pessoas físicas quanto jurídicas podem utilizar estes meios.

A terceira das formas de contratação eletrônica é a **interativa,** que segundo Manoel J. Pereira SANTOS (2000, p.195) são as que "r*esultam de uma relação de comunicação estabelecida entre uma pessoa e um sistema aplicativo*

---

[85] Ressalta-se que nesse trabalho não se buscou estudar a Teoria Geral dos Contratos, mas sim desenvolver um panorama do reconhecimento de validade dos contratos eletrônicos.

[86] SANTOS, M.J.P. Contratos eletrônicos. In: ROVER, A. J. (org.). **Direito, Sociedade e Informática**: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000, p. 194.

[87] Exemplo desse aplicativo é o EDI – *Eletronic Data Interchange* -, que possibilita a comunicação entre vários computadores, com a utilização de protocolos que permitem o envio e o processamento de informações. É comumente utilizada nas transações eletrônicas entre pessoas jurídicas, realizando transações em atacado. Ensina Manoel J. Pereira dos SANTOS (2000, p.194) que "*neste caso, utiliza-se o ambiente digital como ponto convergente de vontades preexistente, ou seja, houve uma negociação prévia, na qual se definiram as regras que regularão a comunicação entre as partes e as transações a serem realizadas na rede (Protocolo de Padrões de Documentos)*".

[88] Entende-se por *Chat-rooms* as salas de conversação inseridas e utilizadas para troca de informações via Internet.

[89] Contratação por *e-mail*, no sentido de possibilidade da realização por correio eletrônico.

previamente programado". Esta forma é comumente utilizada e disponibilizada em estabelecimentos virtuais, nos quais são vinculadas ofertas e que permitem a compra e venda, podendo ser comparada com as modalidades de contratação à distância, como o *telemarketing*, fax, e reembolso postal. Nesta forma ocorre comumente a consumação dos contratos de adesão, no qual um *click*[90] é suficiente para a caracterizar a aceitação do contrato.

Porém, qualquer que seja a forma de contratação, um ponto elas têm em comum, a sua efetivação por meio de uma rede de computadores[91], como, por exemplo, a Internet.

Outra distinção que deve ser realizada ao se estudar os contratos eletrônicos é a existente entre os contratos concluídos por computador e os contratos executados por computador. No primeiro "o *computador atua como mecanismo que intervém no processo de formação e manifestação da vontade negocial, mediante a elaboração de dados que são fornecidos pelas partes como etapa do processo de desenvolvimento da relação jurídica de natureza contratual"*[92]. Ou seja, este é parte do processo de contratação e não um meio como na segunda maneira a ser apontada. No segundo, *"o computador atua como simples meio de comunicação de um acordo de vontades já aperfeiçoado ou como forma de implementar os ajustes contratados, como ocorre com a transferência eletrônica de fundos"* [93]. Neste último o computador é um instrumento de troca de dados e informações pertinentes a formação dos contratos, ou melhor, *"o contrato principal é concluído de forma tradicional e pelo computador realizam-se transações ou operações acessórias ou complementares ao acordo principal"*[94]. Com estas contribuições pode-se concluir que a real caracterização dos contratos, ao observar os elementos de sua elaboração, provém da forma como eles foram formados, pelo modo de instrumentalização caracterizado pela utilização dos computadores com esta finalidade apenas.

---

[90] O ato do *click* refere-se a forma de aceitação, por meio da escolha de determinado ícone da *home-page* com o apertar da tecla do *mouse*.
[91] Manoel J. Pereira dos SANTOS (2000, p.195) ainda completa que *"essas redes podem assumir diferentes designações em função de sua estrutura e de sua dimensão. As redes que interligam as redes internas (LAN – Local Área Network) das diferentes organizações chamadas WAN (Wide Área Network)"*.
[92] Ibid., p.196.
[93] Ibid., p.196.
[94] Ibid., p.196.

Por este motivo, Manoel J. Pereira dos SANTOS (2000, p.197) conceitua os contratos eletrônicos como sendo *"negócios jurídicos que utilizam computadores como mecanismo responsável pela formação e instrumentalização do vínculo contratual"*. Analisando esta conceituação e relacionando-a com as formas de contratação já abordadas, nota-se que as interpessoais e as interativas são as formadoras dos contratos eletrônicos.

Nos documentos eletrônicos, também, identificou-se a possibilidade de geração de certeza, segurança e confiança, principalmente com a aplicação da assinatura digital, para os negócios jurídicos. Uma das formas de negócio jurídico é representada pelos contratos, em especial os contratos eletrônicos, conforme ensina Fabio ULHOA COELHO (2000, p.37) como sendo *"a celebração por meio da transmissão eletrônica de dados. A manifestação da vontade dos contratantes (oferta e aceitação) não se veicula nem oralmente, nem por documento escrito, mas pelo registro em meio virtual (isto é, despapelizado)"*. Conceito compatível ao já apresentado no item anterior sobre os documentos eletrônicos.

Também define contrato eletrônico Semy GLANZ (1998, p.72) determinando-o como *"aquele celebrado por meio de programas de computador ou aparelhos com tais programas, dispensam assinatura ou exigem assinatura codificada ou senha"*. Face a esta conceituação, determina-se a diferença existente entre contratos eletrônicos e informáticos[95].

Portanto, os contratos podem ser definidos como negócios jurídicos, tendo por natureza jurídica a bilateralidade ou a pluralidade. Para sua concretização há o acordo de vontades relativamente autônomas, com interesses contrapostos, porém, harmonizados, gerando uma relação obrigacional seguida de uma modificação econômica.

Ao analisar a conceituação de contratos eletrônicos pode-se observar a multilateralidade, ou seja, a manifestação da vontade de mais de uma pessoa, que inicialmente, será apresentada sob a forma de acordo ou pacto. Porém a

---

[95] Sobre contratos informáticos, Sheila do Rocio Cercal Santos LEAL (2003, p.74) ensina que *"estes se caracterizam por possuírem objeto contratual voltado ao ambiente digital"* E ainda complementa citando alguns exemplos como "*contratos de fornecimento de conteúdos a Websites, contratos de desenvolvimento de Websites, contratos de criação e veiculação de anúncios publicitários em Internet, contratos de hot-sites, contratos de compra e venda de domínios de Internet"*.

manifestação da vontade apresenta uma autonomia relativa como explica Jean Carlos DIAS (2002, p.54) pois

> *A autonomia da vontade deixou de ser uma liberdade absoluta estando jungida ao dirigismo contratual ou intervenção estatal na vontade contratual onde o Poder Público intervém limitando o conteúdo contratual ao mesmo estabelecendo certos requisitos que atingem a formação execução ou mesmo extinção do* (sic) *contratos.*

Na realidade este dirigismo contratual ocorre em virtude da necessidade de garantias e de segurança nas relações contratuais, em face de princípios como o da boa-fé e da função social do contrato.

Assim as partes ajustam seus acordos, formando um vínculo, ao qual as partes pactuam a obediência e o objeto, conforme visto, os contratos eletrônicos apresentam os mesmo elementos dos contratos em papel, com especificidades próprias de sua realidade, a digital.

3.3.1
Princípios dos contratos eletrônicos

3.3.1.1
Princípio da boa-fé objetiva

Ao analisar os contratos eletrônicos, assim como quaisquer outras espécies de contratos, podem ser observadas duas ou mais partes que passam a se relacionar, que permanecem por determinado tempo vinculadas juridicamente. Sobre esta relação deve-se estabelecer uma forma de conduta, a qual deve ser caracterizada por aspectos como a lealdade, a honestidade, a sinceridade,

confiança, cooperação mútua e a boa intenção, em qualquer que seja a fase do contrato.

Com a finalidade de garantir esta forma de relação, Alcio Manoel de Sousa FIGUEIREDO (2004, p.52) afirma que *"o princípio da boa-fé consiste em regra de conduta de interesse social e de segurança nos negócios jurídicos"*.

Ainda sobre o princípio da boa-fé como critério para a relação jurídica, em especial no desenvolvimento dos contratos, Fernanda SCHAEFER (2004, p.45) esclarece que

> *A boa-fé objetiva é uma cláusula geral, um standard de conduta ativa das partes contratantes e, por isso, não depende de prévio consenso ou de expresso acordo. Fundamenta-se no comportamento social e juridicamente justo, solidário e desejado, cuja conseqüência é a confiança e a lealdade entre as partes que se efetivam nas fases negociais, de execução e extinção do negócio jurídico. É fonte de deveres laterais de conduta e causa limitadora do exercício de direitos subjetivos que dá flexibilidade ao sistema contratual para reconhecer soluções mais justas aos dinâmicos casos.*

Em se tratando de situações jurídicas caracterizadas pela agilidade de execução, não há melhor representação que os contratos eletrônicos, ou qualquer outra forma de negócio jurídico via ambiente digital. Quando se trata de boa-fé, sem dúvida alguma, toca-se na legítima expectativa dos contratantes, desde que desenvolvidas dentro dos limites[96] e condutas exigíveis e aceitáveis.

Pode-se identificar que do princípio da boa-fé objetiva podem derivar alguns deveres[97] relacionados aos contratos, como, por exemplo, dever de cooperação, de lealdade, de informação, conforme destaca Paulo NALIN (2000, p.96) espera-se *"do contratante, estando em curso a execução da prestação, que atue de modo diligente e leal, vindo a satisfazer a confiança depositada na declaração de vontade originalmente emitida, quando da formação do negócio"*.

A boa-fé objetiva foi expressamente reconhecida pelo artigo 422 do Código Civil Brasileiro, ao traçar que *"os contratantes são obrigados a guardar,*

[96] Tem-se por limites os princípios, os costumes, a doutrina e as normas jurídicas.
[97] Em especial os deveres de conduta.

assim na conclusão do contrato, como em sua execução, os princípios de probidade e da boa-fé". Trata-se de dispositivo legal que passa a identificar um princípio que traça certa orientação para *"uma linha teleológica de interpretação"*[98] dos contratos.

Sobre a importância da boa-fé objetiva Paulo NALIN (2000, p.126) adverte que *"o atual prestígio da boa-fé objetiva decorre da compreensão do sentido complexo da relação jurídica obrigacional e da pluralidade de seus múltiplos deveres, que põe em evidência a necessidade de ser fiscalizado o comportamento do sujeito contratante"*.

Partindo da idéia apresentada por Antônio Carlos EFING (2003, p.90) de que *"o princípio da boa-fé permeia todas as ações humanas, sendo regra ínsita aos próprios valores éticos e morais da sociedade"*, pode-se afirmar que aos contratos eletrônicos, que cabe perfeitamente sua aplicação e observação não só para as relações contratuais civis, mas em especial para as relações de consumo[99], ainda que uma das partes contratantes esteja fora do território nacional em ambiente virtual.

3.3.1.2
Princípio da autonomia da vontade e da autonomia privada

Em busca da melhor forma de apresentar este tema, faz-se necessária a distinção entre a autonomia da vontade e a autonomia privada[100].

---

[98] MARQUES, C. L. **Contratos no Código de Defesa do Consumidor**: o novo regime das relações contratuais. São Paulo: RT, 2 ed, 1995, p. 83.

[99] Não se pode deixar de reconhecer que mesmo não havendo uma legislação específica para os contratos eletrônicos, considera-se que as regras de Direito Civil e de Direito do Consumidor são perfeitamente aplicáveis a eles.

[100] Preleciona Francisco AMARAL (2003, p.347) ao apontar que: *"A autonomia da vontade, como manifestação de liberdade individual no campo do direito [...] A autonomia privada constitui-se, portanto, em uma esfera de atuação do sujeito no âmbito do direito privado, mais propriamente*

Assim, a autonomia da vontade compreende aspectos subjetivos, trata da possibilidade de realizar atos revestidos pela forma e efeitos determinados pelas partes, ou seja, referente-se ao comportamento. Caracteriza-se pela possibilidade que as partes tem em acordar, podendo determinar o sujeito, o conteúdo e o objeto do contrato, conforme suas próprias estipulações, observando, obviamente, as limitações legais, assim, nem mesmo o Estado poderia intervir nas determinações, mesmo que resultassem em acordos injustos.

A autonomia privada reflete-se no real poder existente entre as partes, em busca da criação, modificação ou extinção de negócios jurídicos, porém dentro dos limites estipulados em lei e não apenas por suas vontades[101], como, por exemplo, ao reconhecer um negócio jurídico como fonte de normas jurídicas. É princípio norteador do direito contratual que vem limitado por outros princípios como a função social do contrato[102]. Assim, a vontade fica submissa a regras de justiça, de ordem pública[103] e de boa-fé como indica Guilherme Magalhães MARTINS (2003, p.47) "*a boa fé, neste quadro, delimita e reestrutura a autonomia privada, na medida em que a adequação das expectativas da parte contratante repousa, ainda que de modo mediato, no respeito à dignidade humana, de maneira que se tutele a pessoa humana*".

---

um espaço que lhe é concedido para exercer a sua atividade jurídica. Os particulares tornam-se, desse modo, e nessas condições, legisladores sobre seus próprios interesses".

[101] Ainda sobre a autonomia privada cabe o esclarecimento de Lucimar de PAULA (2004, p.90) ao demonstrar que *"o princípio pode ser aplicado nas relações contratuais em que as partes encontram-se em igualdade (material) de forças*".

[102] BIEWAGEN, M. Y. **Novo Código Civil:** princípios e regras de interpretação dos contratos. São Paulo: Saraiva, 2003, p. 42. Nesta obra esclarece que "*o atendimento à função social é possível de ser enfocado sob dois aspectos: um, individual, relativo aos contratantes, que se valem do contrato para satisfazer seus interesses próprios, e outro, público, que é o interesse da coletividade sobre o contrato, embora, [...] essa dicotomia seja apenas aparente, pois, qualquer enfoque que se adote, encontrar-se-á o mesmo resultado, isto é, a prevalência do interesse público sobre o particular".*

[103] "*Ordem pública como conjunto de normas jurídicas que regulam e protegem os interesses fundamentais da sociedade e do Estado e as que, no direito privado, estabelecem as bases jurídicas fundamentais da ordem econômica".*

3.3.1.3
Princípio da equivalência funcional

O princípio da equivalência funcional protege os contratos eletrônicos, possibilitando a esses a mesma força e eficiência contidas no contrato realizado em papel ou verbalmente. Trata-se, segundo Fabio ULHOA COELHO (2000, p.39) de princípio que concede ao documento eletrônico a mesma função e capacidade do documento escrito em papel.

Sobre este princípio destaca a Lei Modelo da UNCITRAL[104] (que trata sobre o comércio eletrônico), em seu artigo 5º que *"não se negarão efeitos jurídicos, validade ou eficacia à informações apenas porque esteja na forma de mensagem eletrônica"*. Aqui fica demonstrada a possibilidade de validar contratos eletrônicos, em especial àqueles realizados em ambiente digital.

Na realidade esta proteção gera efeitos diretos e inafastáveis também sobre os documentos eletrônicos, mensagens eletrônicas, e-mails, entre outros, para que possam ser comparados e que seja-lhes reconhecida a mesma validade conferida às mensagens escritas ou verbais.

Este princípio também compõe o sistema jurídico brasileiro, sendo previsto como no Projeto de Lei 672/99 artigo 5º [105], Projeto de Lei 1.589/99 em seu artigo 3º[106], Projeto de Lei 4.906/01 artigo 28[107], projetos que serão melhor analisados no item 3.4.

Assim, nota-se que este princípio é o mecanismo garantidor dos contratos eletrônicos, concedendo a estes os mesmos efeitos jurídicos já existentes e aplicados aos contratos realizados por escrito ou verbalmente.

---

[104] UNCITRAL – *United Nations Commision on International Trade Law*. Esta Lei será oportunamente tratada no item seguinte.

[105] PL 672/99 – artigo 5º - *"Serão reconhecidos os efeitos jurídicos, validade ou eficácia à informação sob a forma de mensagem eletrônica e àquela a que se faça remissão mediante a utilização dessa espécie de mensagem*".

[106] PL 1.589/99 – artigo 3º - *"O simples fato de ser realizada por meio eletrônico não sujeitará a oferta de bens, serviços e informações a qualquer tipo de autorização prévia*".

[107] PL 4.906/02 – artigo 28 – "*A expedição do documento eletrônico equivale: I – à remessa por via postal registrada, se assinado de acordo com os requisitos desta lei, por meio que assegure sua efetiva recepção; e "II - à remessa por via postal registrada e com aviso de recebimento, se a recepção for comprovada por mensagem de confirmação dirigida ao remetente e por este recebida"* .

3.3.1.4
Princípio da aplicação das normas jurídicas existentes aos contratos eletrônicos

Como já apresentado no item 3.3, sobre os contratos eletrônicos e sua equiparação aos contratos escritos ou verbais, pode-se apontar que a diferença existente entre os dois é o meio pelo qual é concretizado, criado e concluído. Assim, o contrato eletrônico não deixa de ser entendido como contrato, quaisquer que sejam as partes, o conteúdo ou o objeto pactuado, pois, não apresentam nenhuma forma diversa dos contratos "tradicionais", ou seja, o negócio jurídico estabelecido não tem diferenciação, a não ser pelo meio utilizado[108].

Sabe-se que a legislação brasileira, ainda está em fase de desenvolvimento, apreciação e estudo, porém ao Direito não se permite deixar abandonados os fatos ocorridos no âmbito digital. E o Direito, na busca pela garantia de segurança aos negócios jurídicos via digital, estabeleceu o princípio da aplicação das normas jurídicas existentes aos contratos eletrônicos, como ensina Jorge José LAWAND (2003, p.59-60)

> *A Internet não cria espaço livre, alheio ao Direito. Ao contrario, as normas legais vigentes aplicam-se aos contratos eletrônicos basicamente da mesma forma que a quaisquer outros negócios jurídicos. A celebração de contratos via Internet se sujeita, portanto, a todos os preceitos pertinentes do Código Civil Brasileiro (Código Civil).*

Assim, o princípio da aplicação das normas jurídicas já existentes aos contratos eletrônicos, sugere que frente às ocorrências relativas aos contratos eletrônicos, cabe a aplicação da legislação vigente, sobre todos as matérias que já se encontram resguardadas pelo Direito. Face a este princípio fica reconhecida a

---

[108] LAWAND, J.J. **Teoria geral dos contratos eletrônicos.** São Paulo: Ed. Juarez de Oliveira, 2003, p. 47.

possibilidade da aplicação dos preceitos do Código de Defesa do Consumidor ao tratar de relação de consumo e do Código Civil quando se tratar de relação civil.

Porém, não se pode deixar de apontar que mesmo face às necessidades jurídico-tecnológicas, o Direito está sendo provocado a regular estas novas realidades. Ao meio jurídico caberá a adaptação de seus institutos e conceitos, frente a mudança que vem ocorrendo. Assim, parece possível a efetivação de uma legislação brasileira específica sobre o comércio eletrônico, que deverá ser orientada por princípios constitucionais e princípios contratuais já existente.

3.4
Panorama histórico do desenvolvimento legislativo no Brasil

O mundo virtual carrega como premissa a necessidade da inovação devido ao meio competitivo em que se encontra. Esta evolução rápida trouxe, em paralelo, a preocupação no âmbito do Direito, que, por meio de discussões, incertezas e questionamentos, busca a proteção dos participantes nas relações virtuais.

As situações que envolvem os documentos eletrônicos, o fato de deixar de ser escrito e passar a ser digital, a possibilidade de eliminação de volumes de papel, a necessidade de segurança, confiança, validade e autenticidade implementada aos negócios jurídicos, entre outras descritas nos capítulos anteriores, passam a ser razões para a criação de novas regras de Direito, que visem regulamentar a assinatura digital como meio de validade dos negócios jurídicos.

Assim, compete ao Direito regular a relação entre indivíduos, proporcionando a devida segurança e confiança às relações jurídicas frente às possibilidades promovidas pelo desenvolvimento das telecomunicações e da informática.

O questionamento sobre a segurança e o acesso da população em geral a esses recursos tem sido objeto de investigação em vários países desenvolvidos, preocupação que também não passa desapercebida pelo legislativo brasileiro e por diversos setores da sociedade civil. Mas, apenas recentemente, no Brasil tiveram início os debates sobre o assunto e a criação de leis a respeito do ambiente virtual ainda caminha a passos lentos. Ainda assim, vale aqui destacar as principais leis brasileiras em vigor e os principais projetos em trâmite.

Uma das primeiras leis criadas e aceitas no Brasil foi a **Lei Modelo das Nações Unidas sobre Comércio Eletrônico**. Em 1996, a ONU[109], por meio da Comissão das Nações Unidas para Leis do Comércio Eletrônico (UNCITRAL), elaborou o modelo recepcionado no Brasil. É lei que busca certa uniformização das legislações já existentes no âmbito internacional, apresentando a assinatura digital, de forma aberta e flexível, tornando possível a sua atualização sem a necessidade de alteração na legislação.

Essa Lei Modelo da UNCITRAL por ser precursora da regulamentação do comércio eletrônico indica em seu artigo 1º que "*aplica-se a qualquer tipo de informação na forma de mensagem de dados usada no contexto de atividades comerciais*", assim delimitando seu alcance à área do comércio.

Mais especificamente quanto à assinatura traz em seu artigo 7°, que

> *1) Quando a Lei requeira assinatura de uma pessoa, este requisito considerar-se-á preenchido por uma mensagem eletrônica quando:*
> *a) For utilizado algum método para identificar a pessoa e indicar sua aprovação para a informação contida na mensagem; e*
> *b) Tal método seja tão confiável quanto seja apropriado para os propósitos para os quais a mensagem foi gerada ou comunicada, levando-se em consideração todas as circunstâncias do caso, incluindo qualquer acordo das partes a respeito.*
> *2) Aplica-se o parágrafo 1º tanto se o requisito nele mencionado esteja expresso na forma de uma obrigação, quanto se a Lei simplesmente preveja conseqüências para a sua ausência.*

[109] ONU - Organização das Nações Unidas.

Face a esta disposição nota-se uma referência à necessidade de identificação e de aplicação de um método confiável, bem como a sua utilização conveniente e apropriada frente a aprovação das partes envolvidas. O método mais adequado (conforme o explicado no Capítulo 2. Item 2.3) é a assinatura digital, o qual corresponde às exigências da Lei Modelo UNCITRAL. Assim, pode-se interpretar o artigo antes mencionado como a possibilidade de substituição da assinatura manuscrita por um método de identificação aceitável pelas partes.

E, mais uma vez a Lei Modelo faz referência a aplicação da assinatura digital, em seu artigo 8º

> ***1)*** *Quando a Lei requeira que certa informação seja apresentada ou conservada na sua forma original, este requisito se considerará preenchido por uma mensagem eletrônica quando:*
> *a) Existir garantia fidedigna de que se preservou a integridade da informação desde o momento da sua geração em sua forma final, como uma mensagem eletrônica ou de outra forma; e*
> *b) Esta informação for acessível à pessoa à qual ela deva ser apresentada, caso se requeira a sua apresentação.*
> ***2)*** *Aplica-se o parágrafo 1) tanto se o requisito nele mencionado esteja expresso na forma de uma obrigação quanto se a Lei simplesmente preveja conseqüências para o caso de que a informação não seja apresentada ou conservada em sua forma original.*
> ***3)*** *Para os propósitos da alínea (a) do parágrafo 1):*
> *a) Presume-se íntegra a informação que houver permanecido completa e inalterada, salvo a adição de qualquer endosso das partes ou outra mudança que ocorra no curso normal da comunicação, armazenamento e exposição;*
> *b) O grau de confiabilidade requerido será determinado à luz dos fins para os quais a informação foi gerada assim como de todas as circunstâncias do caso.*

Dessa forma, a lei está totalmente ligada à aplicação da assinatura digital pela exigência de confiabilidade e integridade nas informações enviadas e recebidas, bem como pela possibilidade de garantia do documento original, que

pode ser realizado por meio da certificação junto a Autoridade Certificadora[110]. Augusto Tavares Rosa MARCANCINI & Marcos COSTA (2002, p. 70) identificam que a *"lei modelo, em 1996, para contar com a aprovação dos EUA, jamais poderia falar em criptografia, cuja exportação era proibida, e ainda se tentava impor restrições para seu uso interno"*.

Angela Bittencourt BRASIL (2004) ressalta que a Lei Modelo da UNCITRAL *"já volta os seus olhos para essa questão de segurança nas relações cibernéticas e reconhece os certificados emitidos por uma entidade certificadora de outro Estado membro da União Européia, se este possuir grau de segurança equivalente a dos países membros da ONU"*. Nota-se que a Lei Modelo UNCITRAL buscou a uniformização da legislação no âmbito internacional. Porém, mais especificamente quanto a assinatura digital, ela não fixa técnicas para aplicação, o que permite uma certa liberdade e traz uma amplitude inadequada quanto à sua aplicação frente àevolução tecnológica sem sua alteração[111]. A Lei Modelo UNCITRAL acabou servindo como um paradigma para vários países, que buscam leis mais específicas visando garantir segurança e viabilidade dos seus negócios eletrônicos.

Pautado na Lei Modelo UNCITRAL o Senado Federal apresentou seu primeiro **Projeto de Lei, sob o número 672 de 1999**. Em concordância com a Lei Modelo UNCITRAL confirmou a possibilidade de substituição da assinatura manual por métodos seguros de identificação, destacando em seu artigo 4° que

> *Artigo 4º - Questões relativas a matérias regidas por esta lei que nela não estejam expressamente disciplinadas serão solucionadas em conformidade, dentre outras, com os seguintes princípios gerais na qual ela se inspira:*
> *I- Facilitar o comércio eletrônico externo e interno*
> *II- Convalidar operações efetuadas por meio das novas tecnologias da informação...*

[110] Mas, em nenhum momento trata sobre a criptografia em seu sentido técnico ou método.
[111] Observa-se que esta Lei foi editada antes da real expansão da Internet como instrumento das relações jurídicas eletrônicas.

Ainda por estar baseado na Lei Modelo da UNCITRAL, em seu artigo 7° o PL n° 672/99 apresenta

> *Artigo 7° - No caso de a lei exigir a assinatura de uma pessoa, este requisito considerar-se-á preenchido por uma mensagem eletrônica, desde que seja utilizado algum método para identificar a pessoa e indicar sua aprovação para a informação contida na mensagem.*
>
> *Parágrafo único. O método utilizado deverá ser confiável e apropriado para os propósitos para os quais a mensagem for gerada ou comunicada, levando-se em consideração todas as circunstâncias do caso, inclusive qualquer acordo das partes a respeito.*

O que denota a idéia da eficácia probatória aplicada às técnicas de autenticação, fato perigoso, pois abre a possibilidade de monopólios, uma vez que estas técnicas são consideradas segredos industriais[112].

É dispositivo legal que possui a mesma intenção de que o método de identificação seja acordado pelas partes. Porém, há um risco neste acordo, qual seja, a possibilidade das partes não *"possuírem conhecimentos técnicos suficiente"*[113] para proceder à escolha adequada. É fato que torna as partes vulneráveis à fraude entre elas, bem como de terceiros. Assim, pode ser considerada uma falha do legislador, a falta de imposição de limites ao alcance da tecnologia. Uma sugestão seria a criação de uma entidade responsável pela regulamentação do comércio eletrônico. Por isso, há a necessidade do responsável ter conhecimento a respeito da matéria, para pode legislar de forma adequada[114].

Porém, não se pode deixar de lado o fato de que, apoiado[115] na Lei Modelo UNCITRAL, carregou também seus resquícios, ou seja, a falta de tratamento e indicação sobre a criptografia, de forma direta, como indicam Augusto Tavares Rosa MARCACINI & Marcos COSTA (2004, p.70)

---

[112] REZENDE. P. A. D.. **Entidades certificadoras, assinaturas eletrônicas e projetos de lei.** Disponível em : <http://www.cic.unb.br/docentes/pedro/_trabs/debate_oab1.htm>. Acesso em 26 jan. 2005.
[113] VOLPI, M.M., 2001, op. cit., p. 49-50.
[114] Ibid., p.49 – 50.
[115] Na verdade trata-se de uma forma de tradução da Lei Modelo UNCITRAL.

> *[...] pode ser considerada um paradigma da 'neutralidade tecnológica'. Em, 1996, o acesso público e irrestrito à Internet ainda engatinhava, e a criptografia era conhecida por uns poucos 'micreiros' que freqüentavam o underground da rede; além, é claro, dos organismos militares e de inteligência, usuários originais deste tipo de conhecimento.*

Frente a esta situação acabou por receber as mesmas críticas dirigidas a Lei Modelo UNCITRAL, pela omissão sobre a criptografia assimétrica, pois, a criptografia tornou-se, nos últimos anos, uma necessidade frente a realidade tecnológica e sua regulamentação beneficiaria e geraria segurança aos cidadãos, usuários desta tecnologia. Porém há a defesa de que em se omitindo sobre a criptografia assimétrica, uma nova técnica que por ventura seja lançada, não levará a queda desta lei.

Ainda em busca do aperfeiçoamento legislativo foi apresentado o **Projeto de Lei n° 1.483 de 1999**[116], da Câmara dos Deputados, que traz aspectos sobre a fatura eletrônica e a assinatura digital, recomendando a certificação por órgão público. Este projeto é composto por dois artigos, que têm por objetivo dar validade à assinatura digital como meio seguro para transações comerciais.

Definiu, ainda, que o reconhecimento da assinatura digital será conferido por órgão público e ainda definiu para este órgão a competência para fiscalização, avaliação e cadastro, mas deixou em aberto qual será o modo de operação deste órgão e a que Ministério estará vinculado.

Conforme o artigo 2º[117] do referido projeto, o legislador buscou deixar nas mãos do Estado o poder fiscalizador e certificador dos documentos eletrônicos, bem como a responsabilidade pelo registro das assinaturas digitais. Porém, deixa em aberto a definição de documento eletrônico, o que possibilita uma brecha na legislação. Tal lacuna fica evidente na distinção de documento eletrônico, pois para a área da tecnologia da informação é o material utilizado para

---

[116] INTERNETLEGAL. **Compêndio da Legislação Brasileira sobre Informática, Internet, Telecomunicações e conexos.** Disponível em: <http://www.internetlegal.com.br/legis/>. Acesso em 11 set 2003.

[117] Artigo 2º - "*A assinatura digital terá sua autenticação e reconhecimento certificado por órgão público que será regulamentado para este fim*".

confecção e manutenção da tecnologia e para a jurídica tem sua compreensão específica já observada no item 3.2. Outra idéia seria a de documento no sentido de registro de documento público, ligando o Estado ao aspecto material dos documentos.

Na verdade, este projeto foi apresentado sob a forma de regulamentação sobre a assinatura digital quanto a sua existência e transferindo a competência para normatizar e controlar mais especificamente a um órgão estatal. Mesmo em sua simplicidade, este Projeto de Lei, guarda grande valia por ser o precursor no Brasil a tratar sobre as assinaturas digitais, passando a provocar o Legislativo para a necessidade jurídica que existe sobre o assunto.

Ainda, em 1999, foi elaborado o **Projeto de Lei n° 1.589**, da Câmara dos Deputados que trata do comércio eletrônico, da validade jurídica do documento eletrônico e da assinatura digital. Sua elaboração partiu das contribuições vindas do anteprojeto da Comissão de Informática Jurídica da OAB[118]/SP. Esse projeto trouxe a previsão de criação da atividade cartorial eletrônica, realizando todas suas atividades via Internet, pautada num sistema de autenticação documental, sob a responsabilidade de tabeliães certificados[119]. Augusto Tavares Rosa MARCACINI & Marcos COSTA (2004, p.65) destacam

> *Curiosamente, desde que o Anteprojeto foi entregue à Câmara pela OAB/SP, que o redigiu, apareceram críticas aqui e ali no sentido de que tal dispositivo iria 'engessar a tecnologia', ou que o projeto não seria "tecnologicamente neutro", ao "optar" pela criptografia assimétrica como único meio de produzir assinaturas digitais, em detrimento de outras 'novas tecnologias', ainda inexistentes, mas que poderiam vir a serem criadas.*

[118] OAB- Ordem dos Advogados do Brasil.

[119] IPB BRASIL. **Projeto de Lei cria atividade cartorial eletrônica.** Disponível em: <http://www. Ibpbrasil.com.br/news/inf04.htm>. Acesso em 26 mar 2004.

Os autores ainda apontam que tais críticas não apresentam a mínima fundamentação sob o aspecto *"técnico, jurídico, econômico ou político"*, apenas visavam denegrir e enfraquecer a imagem de tal proposta[120]. Bem como, garantem que o Projeto 1.589/99 não engessaria a tecnologia, pois possibilita a utilização de outras formas de criptografia assimétrica, desde que estas comprovem segurança e eficiência.

Outro ponto relevante é que esse Projeto de Lei estabelece, em seu artigo 14[121] a equiparação do documento eletrônico com o documento tradicional, desde que haja a assinatura realizada por criptografia de chave pública, ou seja, pela criptografia assimétrica.

Há a necessidade de destacar a importância deste projeto no sentido de permitir aos certificados eletrônicos, por meio da autenticidade das chaves, o reconhecimento de firma, emanados por entidades privadas (art. 24)[122], como, por exemplo, por tabeliões (art. 25)[123]. Assim, seus efeitos práticos terão diferenciações, uma vez que apenas a certificação realizada por tabelião terá a presunção de autenticidade e veracidade, enquanto a realização por particulares ainda carregará a insegurança.

O mesmo Projeto de Lei 1589/99 apontou a questão da data do documento, pois, só seria válido se a assinatura não estivesse revogada ou expirada. Neste sentido, salienta Marlon Marcelo VOLPI (2001, p.53)

> *Com a existência deste aspecto de expiração da assinatura, surge uma nova importância sobre a data do documento eletrônico. Um documento eletrônico só pode ser considerado válido se a assinatura não estiver revogada ou expirada. Pelo projeto, pode ser considerada como a data do documento eletrônico: a data em que foi registrado, a data da sua*

---

[120] MARCACINI, A. T. R. & COSTA, M., 2004, op. cit., p. 65.

[121] Artigo 14 – "*Considera-se original o documento eletrônico assinado pelo seu autor mediante sistema criptográfico de chave pública*".

[122] Artigo 24 – "*Os serviços prestados por entidades certificadas privadas são de caráter comercial, essencialmente privados e não se confundem em seus efeitos com a atividade de certificação eletrônica por tabelião, prevista no Capitulo II deste Titulo*".

[123] Artigo 25 – "*O tabelião certificará a autenticidade de chaves públicas entregues pessoalmente pelo seu titular, devidamente identificado; o pedido de certificação será efetuado pelo requerente em ficha própria, em papel, por ele subscrita, onde constarão dados suficientes para identificação da chave pública, a ser arquivada em cartório*".

> *apresentação em repartição pública ou em juízo, ou, ainda, a data do ato ou fato que estabeleça, de modo certo, a anterioridade da formação do documento e respectivas assinaturas.*

Algumas críticas foram realizadas a este Projeto de Lei, dentre elas destaca-se a firmada por Guilherme Magalhães MARTINS (2003, p.118)

> *Em primeiro lugar, em matéria de autoridades de certificação, suas provisões incorrem num indesejável formalismo, curvando-se ao ainda arcaico sistema de notários públicos existente no Brasil, aos quais é conferido, com exclusividade, o privilégio de certificar a autenticidade das chaves públicas*.

Assim, no que tange à indicação da criptografia assimétrica, reservada à certificação para os notários, respaldada no artigo 236 da CF/88[124] determina o Projeto de Lei que a certificação da chave pública deve ser feita pelos tabeliães que assim, confeririam presunção de autenticidade, entende, ainda que a certificação realizada por entidades particulares não tem a presunção de autenticidade assegurada, porém deixa em aberto a possibilidade de certificação por outros agentes sociais[125] que seriam indicados em uma outra norma.

Muito importante foi o **Decreto n° 3.587 de 2000, do Governo Federal,** que teve por objetivo a normatização da Assinatura Digital, criando uma Infra-Estrutura de Chaves Públicas pelo Poder Executivo Federal. Esse Decreto possibilita a utilização do sistema de criptografia assimétrica (assinatura digital) na Administração Pública. Nota-se que o Estado buscou aplicar nele mesmo em

---

[124] Este artigo determina para certa categoria de agentes (tabeliães ou notários) a reserva de algumas atividades, o que poderia levar a entender que a certificação digital também poderia caber a estes. Porém, entende-se que ao tabelião cabe as atividades apontadas pelo § 1° do artigo 236 da CF/88, revelando-se à possibilidade da lei conferir a outro agente o poder de Autoridade Certificadora.

[125] CASTRO, A. A. **O Documento Eletrônico e a Assinatura Digital.** Uma visão geral. Disponível em: < http://www.aldemario.adv.br/doceleassdig.htm>. Acesso em 27 jan 2002.

primeiro lugar, visando a regulamentação da aplicação da assinatura digital no mercado privado, o que estimula a aceitação e aprovação dos demais projetos.

Ao analisar este Decreto há a possibilidade de se destacar alguns pontos importantes, como a criação da Infra-estrutura de Chaves Públicas do Poder Executivo Federal (ICP-Gov), que contém toda a estrutura funcional e operacional de um sistema de certificação[126], destacando-se a adoção da criptografia assimétrica.

Ou seja, é norma que possibilitou a instituição de uma Autoridade Certificadora Raiz (AC Raiz), que será *"responsável pela emissão e manutenção dos certificados das AC de órgãos e entidades da Administração Pública Federal e das AC privadas credenciadas, bem como o gerenciamento da Lista de Certificados Revogados (LCR)"* indicado por Marlon Marcelo VOLPI (2001, p.47). O citado autor complementa a aplicação do Decreto afirmando que em conformidade com o artigo 9º, *"As AC podem receber seu credenciamento em níveis diferenciados, de acordo com a finalidade em que forem atuar"*. Trata-se de processo de credenciamento que deve seguir as estipulações da Autoridade de

---

[126] Regida pela Autoridade de Gerência de Políticas (AGP). O sistema a ser aplicado segue o artigo 6º do Decreto 3.587/00 *"À Autoridade de Gerência de Políticas - AGP, integrante da ICP-Gov, compete:*
I - propor a criação da Autoridade Certificadora Raiz - AC Raiz;
II - estabelecer e administrar as políticas a serem seguidas pelas AC;
III - aprovar acordo de certificação cruzada e mapeamento de políticas entre a ICP-Gov e outras ICP externas;
IV - estabelecer critérios para credenciamento das AC e das Autoridades de Registro - AR;
V - definir a periodicidade de auditoria nas AC e AR e as sanções pelo descumprimento de normas por ela estabelecidas;
VI - definir regras operacionais e normas relativas a:
a) Autoridade Certificadora - AC;
b) Autoridade de Registro - AR;
c) assinatura digital;
d) segurança criptográfica;
e) repositório de certificados;
f) revogação de certificados;
g) cópia de segurança e recuperação de chaves;
h) atualização automática de chaves;
i) histórico de chaves;
j) certificação cruzada;
l) suporte a sistema para garantia de irretratabilidade de transações ou de operações eletrônicas;
m) período de validade de certificado;
n) aplicações cliente;
VII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Gov, em especial da Política de Certificados - PC e das Práticas e Regras de Operação da Autoridade Certificadora, de modo a garantir:
a) atendimento às necessidades dos órgãos e das entidades da Administração Pública Federal;
b) conformidade com as políticas de segurança definidas pelo órgão executor da ICP-Gov; e
c) atualização tecnológica".

Gerência de Políticas (AGP)[127], bem como os padrões internacionais no país aceitos.

O Decreto 3.587 de 2000, cria ainda a figura da Autoridade de Registro (AR) que nas palavras de Marlon Marcelo VOLPI (2001, p.47) será

> *Responsável por receber as requisições de certificação ou revogação de certificado dos usuários, confirmar a identidade desses usuários e a validade de sua requisição, além de encaminhar esses documentos à AC responsável. Cabe ainda à AR entregar os certificados assinados pela AC aos seus respectivos solicitantes.*

Assim, ao analisar o artigo 15[128] do Decreto 3587/00, destaca-se a finalidade buscada pelo governo, pautada na utilização da certificação digital para: conferir autenticidade, proceder cifragens, gerar segurança e sigilo em informações, entre outras.

Nota-se que esse Decreto acabou por valorizar as empresas privadas de certificação digital, uma vez que reconhece as Autoridades Certificadoras e adota como legal os documentos e transações por elas certificadas. Mas, não se pode deixar de destacar que o alcance e o objetivo deste Decreto é a normatização da Assinatura Digital, voltada aos órgãos e atividades governamentais.

Visando a melhoria e adequação aos projetos propostos e antes referidos, a partir de 1999, foi elaborado o **Substitutivo aos Projetos de Lei n° 1.483 e 1.589 de junho de 2001**. Trata-se de instrumento legal que convalidou o sistema baseado na criptografia assimétrica, mas, deu possibilidade à aplicação de outras formas de assinatura digital. Esse substitutivo determina, ainda, um modelo de certificação em que podem participar autoridades públicas e privadas, independente da autorização estatal. Ressaltou o projeto que a certificação

---

[127] Sobre a competência da AGP o artigo 16 traz : "*À AGP compete tomar as providências necessárias para que os documentos, dados e registros armazenados e transmitidos por meio eletrônico, óptico, magnético ou similar passem a ter a mesma validade, reconhecimento e autenticidade que se dá a seus equivalentes originais em papel*".

[128] Artigo 15 – "*Serão definidos tipos de certificados, no âmbito da ICP-Gov, que atendam às necessidades gerais da maioria das aplicações, de forma a viabilizar a interoperabilidade entre ambientes computacionais distintos, dentro da Administração Pública Federal*".

fornecida por autoridade do Poder Público é a que presume autenticidade e segurança.

Ainda em busca da segurança e do reconhecimento das assinaturas digitais, em 2001, foi apresentado o **Projeto de Lei nº 4.906 de 2001** o qual tratou do valor probante dos documentos eletrônicos, bem como da assinatura digital. Em seu conteúdo trata da certificação digital, estabelecendo normas que visam a segurança no comércio eletrônico. Esse projeto traz conceituações e definições como as de assinatura digital, documento eletrônico, criptografia assimétrica, etc., visando a necessidade de uniformidade no tratamento de tais conceitos. Basicamente foi criado baseado na Lei Modelo da UNCITRAL. Muito relevante foi a contribuição contida em seu artigo 3º[129] o qual reconhece a validade e eficácia aos documentos eletrônicos. Na realidade somou muitos pontos positivos de outros Projetos de Lei anteriormente citados como o 672/99 e o 1.483/99, culminando em uma nova proposta legislativa.

Deve-se destacar aqui que os Projetos de Lei 1.483/99 e 1.589/99 da Câmara do Deputados, seus Substitutivos, e o Projeto de Lei 672/99 do Senado Federal, já aprovado no mesmo e que se encontra na Câmara dos Deputados tem por objetivo a regulamentação da mesma matéria contida na Medida Provisória 2200/01, que será analisada a seguir. Estes três projetos foram focos centrais de muitos debates na sociedade, por meio de palestras, seminários e congressos, bem como, foi motivação para várias Audiências Públicas no Congresso Nacional[130]. Porém, considerando-se a importância do tema, e a necessidade da urgente regulamentação, o legislador acabou deixando de lado estes três Projetos de Lei, substituindo-os pela Medida Provisória 2200/01 que foi redigida e editada desconsiderando tais propostas, bem como, as manifestações públicas da sociedade brasileira.

Um dos maiores avanços legislativos sobre a assinatura digital, foi a **Medida Provisória 2200 de 29 de junho de 2001**[131] que instituiu a ICP-Brasil[132] como garantidor da autenticidade e da integridade de documentos eletrônicos por

---

[129] Artigo 3º- "*Não serão negados efeitos jurídicos, validade e eficácia ao documento eletrônico, pelo simples fato de apresentar-se em forma eletrônica*".

[130] Sem contar com o interesse presente na imprensa que divulgou as mais variadas opiniões, de diversos setores envolvidos no assunto.

[131] CÂMARA DOS DEPUTADOS. Disponível em: <www.camara.gov.br/internet/integras/outras.asp>. Acesso em 18 mar 2003.

[132] ICP-Brasil - Infra-Estrutura de Chaves Públicas Brasileiras.

meio da criptografia assimétrica. Tal objetivo fica claro no artigo 1° da MP 2200/01 ao apontar que visa *"garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras"*.

Para analisar a MP 2200/01 cabe a identificação do momento histórico e a maneira como foi promulgada. Pedro Antonio Dourado REZENDE (2004) destaca

> *A ICP-Brasil surgiu de uma canetada do presidente FHC, em 28 de junho de 2001, na Medida Provisória 2200. Esta medida estendeu uma iniciativa que até então vinha sendo internamente debatida, para se regulamentar uma infra-estrutura de chaves públicas para o governo federal. Esse debate foi suspenso e a regulamentação abruptamente extrapolada a toda a sociedade, atropelando anos de debate e vários projetos de lei que tramitavam no legislativo federal.*

Assim, a pretensão dessa Medida Provisória foi de resguardar a questão da *"validade jurídica de documentos em forma eletrônica"*. Assim, sua intenção, claramente superou a questão da força probante dos documentos, atingindo também a questão da validade do ato jurídico praticado no ambiente digital.

Outro aspecto guardado pela MP 2.200/01 foi a preocupação sobre a eficácia da certificação, devido ao fato de que esta não pressupõe apenas a tecnologia, mas também procedimento e conteúdo adequados[133].

Observa-se que a MP não se refere apenas aos documentos da administração federal, mas sim, à todos os documentos emitidos sob a formação e

[133] Procedimento no sentido de ter a possibilidade da confirmação de que a chave pública é de titularidade de certa pessoa, a capacidade de conhecê-la, identificá-la, e ter a chance de criar provas físicas de reconhecimento de que a propriedade da chave é desta pessoa. E conteúdo, no sentido de que algumas certificações apenas garantem que não há outra chave idêntica, mas o intuito aqui é identificar a quem pertence tal chave pública.

formatação eletrônica, fato facilmente comprovado pela leitura do artigo 12 determina que *"consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória"*.

O mesmo artigo 12 ainda revela grande importância quando define que os documentos eletrônicos deverão ser compatíveis com a ICP-Brasil, devendo assim, terem sido assinados por chaves certificadas por agente certificador credenciado.

Com isso a Medida Provisória, ainda descreve a criação da ICP-Brasil, composta por um Comitê Gestor, a Autoridade Certificadora Raiz (Instituto Nacional de Tecnologia da Informação ITI), Autoridades Certificadoras (AC) e Autoridades de Registro (AR), e cuja sua organização será regulamentada em lei específica[134].

O gerenciamento desse sistema foi delegado ao Comitê Gestor, que tem por obrigações: a implantação, imposição de critérios, diretrizes, regras operacionais e normas de licenciamento das Autoridades Certificadoras e de Registro, permitir a emissão de certificados, a negociação e aprovação de acordos de certificação bilateral, estipulando regras de cooperação. Ao analisar o sistema de certificação digital, que passou a regulamentar a ICP-Brasil, trouxe significativos avanços referentes aos negócios eletrônicos proporcionando autenticidade e veracidade a documentos eletrônicos.

Aldemiro Araújo CASTRO (2002), esclarece precisamente esse sistema

> *À AC Raiz, primeira autoridade da cadeia de certificação, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC (de nível*

[134] Observa-se que apenas nomeou um Comitê Gestor da ICP-Brasil, constituído por agentes do Poder Executivo Federal, a quem competirá expedir toda a regulamentação dos mais variados aspectos, destacando-se (artigo 5º): adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil (inciso I); estabelecer a política, os critérios e as normas para licenciamento ds AC, das AR e dos demais prestadores de serviços de suporte à ICP-Brasil (inciso II); estabelecer a política de certificação e as regras operacionais da AC Raiz (inciso III); estabelecer diretrizes e normas para a formulação de políticas de certificados (inciso V); aprovar políticas de certificados e regras operacionais, licenciar e autorizar o funcionamento das AC e das AR (inciso VI); atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança (inciso VIII).

imediatamente subseqüente ao seu), sendo vedado emitir certificados para o usuário final. Às AC, órgãos ou entidades públicas e pessoas jurídicas de direito privado, compete emitir, expedir, distribuir, revogar e gerenciar os certificados de usuários finais. Às AR, entidades operacionalmente vinculadas a determina AC, compete identificar e cadastrar usuários, na presença destes, e encaminhar solicitações de certificados às AC.

Porém o fato de deixar a regulamentação para lei específica, possibilitou uma lacuna perigosa, por não determinar como serão os certificados, qual será o procedimento para certificação, quais os requisitos que devem ser preenchidos, quem atuará como entidade certificadora e ainda qual a responsabilidade destas entidades. Esta medida provisória, em virtude do apontado, sofreu várias críticas por parte da Ordem dos Advogados do Brasil seccional do Estado de São Paulo, da CERTSIGN (Certificadora Digital Ltda.), da Sociedade Brasileira de Computação, entre outras entidades[135].

---

[135] Algumas críticas podem ser assim identificadas: **1)** da CertSign. Disponível em: <http://www.certisign.com.br/imprensa_mix.html>. Acesso em 26 jan 2002.; **2)** de Marcos da Costa e Augusto Tavares da Comissão de Informática Jurídica da OAB de São Paulo. Disponível em: <http://www.cbeji.com.br/artigos/artmarcosaugusto05072001.htm>. Acesso em 26 jan 2002; **3)** da Sociedade Brasileira de Computação. A SBC - Sociedade Brasileira de Computação manifesta publicamente seu desconforto com a edição da Medida Provisória 2.200, que trata de aspectos essenciais para a cidadania inscritos em nossa Constituição, e muito especialmente o direito à privacidade, com conseqüências específicas sobre a autenticidade, o sigilo e a inviolabilidade de documentos. Outros países estão discutindo estas questões há muitos anos, sem terem chegado ainda a soluções satisfatórias que sejam aceitáveis para suas sociedades. Não é, portanto, admissível, que o Brasil decida regular assuntos de tal relevância e complexidade técnica e jurídica sem amplo debate prévio com a sociedade, debate este que deveria tomar o tempo que a sociedade julgasse necessário para amadurecer sua posição. É igualmente inadmissível que a regulamentação da matéria venha através de norma a ser estabelecida pelo Comitê Gestor da ICP-Brasil após uma simples consulta pública que estabelece o prazo exíguo de 20 dias para estudo de uma documentação extensa e complexa. A sociedade brasileira não irá aceitar nenhuma regulamentação sobre a questão que venha a ser estabelecida desta forma açodada, imposta sem diálogo efetivo, especialmente considerando que ela pode ferir (ou deixar margem para que sejam feridos) direitos constitucionais básicos da cidadania. Face à complexidade, amplitude e potenciais impactos das matérias tratadas pela MP 2.200 e das ações dela derivadas, a SBC apela ao Governo Federal para que promova uma análise ampla, serena e transparente das mesmas, com a eventual revisão da atual proposta para criação da ICP Brasil e para a regulamentação das questões técnicas associadas. Para isto, a SBC se põe desde já à disposição do Governo e da sociedade brasileira, em tudo aquilo que sua competência e a de seus associados puder se fazer necessária. Disponível em: <http://www.sbc.org.br/novidades/cartaab.htm>. Acesso em 10 set 2005 e **4)**da OAB (logo adiante). A **primeira nota** da OAB*: "A Ordem dos Advogados do Brasil vem a público manifestar o seu repúdio à nova Medida Provisória nº 2.200, de 29/06/2001, que trata da segurança no comércio eletrônico no País. A MP, editada às vésperas do recesso dos Poderes Legislativo e Judiciário, desprezou os debates que vêm sendo realizados há mais de um ano no Congresso*

E em seguida foi proposta e aprovada a **Medida Provisória nº 2.200-2 de 24 de agosto de 2001** que ofereceu subsídios complementares à Medida anterior. Seu principal objetivo foi elaborar regras básicas para o credenciamento das Autoridades Certificadoras, que irão emitir os certificados e conferir autenticidade à assinatura digital, componente fundamental, nos documentos eletrônicos, como demonstra Felipe Costa FONTES & Rodrigo Guimarães COLARES (2002) que "g*ozam, dessa forma, de presunção relativa ou* ***juris tantum*** *de autenticidade, as assinaturas digitais contidas no documento certificado eletronicamente por uma Autoridade Certificadora que atende aos requisitos estabelecidos pelo Comitê Gestor da ICP-Brasil (CG da ICP-Brasil*)".

Ao analisar essa Medida Provisória 2.200-2 pode-se observar sua compatibilidade com o contido no Código Civil Brasileiro de 2002, artigo 219[136]. Assim, assegura-se que as declarações constantes nos documentos eletrônicos,

---

Nacional sobre três projetos a esse respeito, um dos quais oferecido pela OAB-SP. Ao estabelecer exigência de certificações para validade dos documentos eletrônicos públicos e privados, a MP não apenas burocratiza e onera o comércio eletrônico, como distancia o Brasil das legislações promulgadas em todo o mundo. Pior: ao outorgar poderes a um Comitê Gestor, nomeado internamente pelo Executivo e assessorado por órgão ligado ao serviço de segurança nacional, o governo subtrai a participação direta da sociedade civil na definição de normas jurídicas inerentes ao conteúdo, procedimentos e responsabilidades daquelas certificações.Tudo isso é motivo de extrema preocupação no que tange à preservação do sigilo de comunicação eletrônica e da privacidade dos cidadãos, num momento em que grampos telefônicos têm se proliferado país afora, afrontando, inclusive, o livre exercício da advocacia. Brasília, 03 de julho de 2001. Rubens Approbato Machado. Presidente nacional da OAB". A **segunda nota** da OAB*: "A Ordem dos Advogados do Brasil reconhece a sensibilidade do Governo Federal em acolher as críticas e sugestões manifestadas na primeira edição da Medida Provisória nº 2.200, alterando-a substancialmente em pontos fundamentais, a saber: 1) determina que o par de chaves criptográficas seja gerado sempre pelo próprio titular e sua chave privada de assinatura seja de seu exclusivo controle uso e conhecimento (§ único do art. 8º); 2) eleva o número de representantes da sociedade civil no Comitê Gestor (art. 3º); 3) limita os poderes daquele Comitê à adoção de normas de caráter técnico (incisos II e IV do Art. 5º e caput do art. 6º), bem como lhe determina a observância de tratados e acordos internacionais no que se refere ao acolhimento de certificações externas (inciso VII do art. 5º); 4) estabelece que a identificação do titular da chave pública seja presencial (art. 9º); 5) limita os efeitos legais da certificação ao próprio signatário (§ 1º do art. 12º); e 6) utiliza outros meios de prova da autenticidade dos documentos eletrônicos, afastando, assim, a obrigação do uso nos documentos particulares de certificações da ICP-Brasil (§ 2 º do art. 12º). Entende a OAB que tais disposições são fundamentais para o restabelecimento de um ambiente que assegure a privacidade, segurança e liberdade nas manifestações de vontade dos cidadãos realizadas por meio eletrônico. Independente desses verdadeiros avanços, a OAB continua certa de a disciplina do documento eletrônico, da assinatura digital e das certificações eletrônicas deva nascer de um amplo debate social, estabelecido em sede própria, qual seja, o Congresso Nacional, razão pela qual manifesta sua confiança em que a nova redação da MP não representará prejuízo ao andamento regular dos projetos de lei que tramitam atualmente em nosso Parlamento."* Sites acessados em janeiro de 2002.

[136] Na época da edição da MP 2002-2 tratava-se do art. 131 do Código Civil Brasileiro de 1916, porém tal artigo encontra sua referência no artigo 219 do atual Código Civil com a seguinte transcrição: *"As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários"*.

produzidos com a utilização de processos de certificação, presumem-se verdadeiras em relação aos signatários, trazendo por esta inovação a possibilidade do preenchimento da lacuna legislativa existente. Com isso equiparam-se os documentos eletrônicos a documentos públicos ou particulares desde que aplicado o processo de certificação, sendo admitido pelas partes como válido ou aceito o documento. Esta aplicação trará inúmeras discussões e questionamentos por se tratar de novas tecnologias e evolução, exigindo do Direito constante aperfeiçoamento e adaptações.

João Agnaldo Donizete GANDINI, Daiana Paola da Silva SALOMÃO & Cristiane JACOB (2004) apontam que a reedição da MP 2.200 teve por objetivo a alteração seguindo as críticas e sugestões indicadas pela OAB-SP. Assim, possibilitou a inclusão de mais um participante representante da iniciativa privada no Comitê Gestor da ICP-Brasil, afirmou que a privacidade do usuário certificado será garantida, previu a presunção de veracidade aos documentos eletrônicos com a possibilidade de aplicação de modalidades probatórias assegurando a sua autoria e integridade[137].

Face a todo esse desenvolvimento legislativo brasileiro, pode-se identificar a necessidade de mudança nas leis e nos projetos. Mas, também, de uma mudança na forma do processo, pois, a morosidade, a utilização de leis voltadas a interesses de alguns, prejudicam a vida e utilização da tecnologia por muitos, conforme afirma Marco Antonio Machado Ferreira MELO (2000, p.32)

> *Esta nova era digital exige um processo legislativo ágil, capaz de acompanhar a evolução tecnológica e suas conseqüência sociais. Se é verdade que a solução jurídica precede a solução tecnológica, estamos literalmente desprotegidos. A solução jurídica para as questões das novas tecnologias que evoluem rapidamente, não pode depender do processo legislativo arcaico, moroso por natureza, concebido num outro tipo de sociedade, não estando mais atendendo às necessidades legais para a sociedade pós-moderna. Há a necessidade de adequação de nossa legislação para este novo momento. O Direito e a Ciência do Direito*

[137] GANDINI, J. A. D.; SALOMÃO D.P. S.; JACOB C. **A validade jurídica dos documentos digitais.** Disponível em: <http://www.mct.gov.br/legis/Consultoria_Juridica/artigos/validade_juridica_docs_digitais.htm>. Acesso em 06 mar. 2004.

estarão em permanente crise, decorrente da velocidade das transformações sociais, culturais, políticas e tecnológica.

O Brasil tem se desenvolvido rapidamente quanto à utilização dos meios digitais de negócios jurídicos, acendendo a preocupação sobre a adequação legislativa. A necessidade de regulamentação é importante, pois visa a superação de questionamentos e situações jurídicas problemáticas, superando uma eventual resistência ao desenvolvimento tecnológico.

A possibilidade de segurança determinada pela assinatura digital passou a ser reconhecida em diversas das legislações o que confirma a sua importância e a força de validade jurídica que transmite aos contratos eletrônicos. Fato este que leva à maior utilização do meio eletrônico para suas relações jurídicas, nos mais variados locais, uma vez que nem todos os cidadãos têm a possibilidade de ter um computador próprio.

4
INCLUSÃO DIGITAL

"Não há amanhã sem projeto, sem sonho, sem utopia, sem esperança, sem o trabalho de criação e desenvolvimento de possibilidade que viabilizem a sua concretização".

Paulo Freire [138]

4.1
Revolução Tecnológica

Ao investigar a contribuição da Revolução Tecnológica na sociedade pode-se destacar três fases distintas e interconectadas. A primeira fase surge com a evolução da imprensa, possibilitando a formação da opinião pública, pela transmissão e difusão de idéias e ideais, fundamentais para a evolução da sociedade, que constantemente se atualiza e aperfeiçoa[139].

O avanço da sociedade levou à segunda fase que pode ser identificada pela utilização da energia elétrica e dos combustíveis, em especial o petróleo. Essa fase da evolução permitiu impingir ao mundo a oportunidade de uma modificação maior. A utilização dos combustíveis possibilitou melhorias como a diminuição das distâncias, o auxílio no aumento da produção agrícola e industrial e a melhoria do comércio e da economia. A inclusão da energia elétrica na sociedade aliou-se à evolução da imprensa[140].

A energia elétrica desenvolveu a possibilidade da transmissão do som e da imagem por ondas eletromagnéticas. Destaca-se aqui a criação e a evolução do rádio e da televisão, que passaram a ser um grande marco no desenvolvimento

---

[138] FREIRE, P.; FREIRE, A. M. (org.). **Pedagogia dos sonhos possíveis.** São Paulo: UNESP, 2001, p. 85.
[139] SILVEIRA, S.A., 2001, op. cit., p. 07.
[140] SILVEIRA, S.A., 2001, op. cit., p. 07-08.

e na mudança da sociedade, pelo seu poder de informação e de sistemas de idéias. Seu poder e sua importância podem ser observados pela disputa entre grupos políticos e econômicos pelo domínio e utilização dos meios de telecomunicação. Destacam-se outras possibilidades e melhorias trazidas pela evolução da energia elétrica, como na área da medicina, da educação, do transporte, da indústria, etc.. Porém, a maior contribuição da energia elétrica foi a melhoria da qualidade de vida de uma parte da população mundial[141].

Uma terceira fase, o ponto central da Revolução Tecnológica, iniciou com a criação dos computadores, que passou a ser um dos principais meios de comunicação, de comércio, de economia e de movimentação do poder[142]. Como indica Sérgio Amadeu da SILVEIRA (2001, p.8) a partir do momento em que passou, a *"transformar toda a produção simbólica em um conjunto de dígitos, de bytes e bits, de 0 e 1"*, possibilitou-se a criação deste meio de difusão, comunicação e disseminação de informações. Nesse sentido, o mesmo autor destaca *"a comunicação fundamental da nossa sociedade já é a comunicação mediada por computador"*[143].

Como foi apresentado no histórico do desenvolvimento dos computadores (Capítulo 2.), da Internet e da criptografia, nota-se que a tecnologia adentrou a sociedade, modificando as vidas em todos os níveis. Os avanços da Revolução Tecnológica levam Sérgio Amadeu da SILVEIRA (2001, p.15) a afirmar

> *Porque o computador, ícone da nova revolução, ligado a rede está alterando a relação das pessoas com o tempo e com o espaço. O computador ressuscitou a escrita após a supremacia das mídias audiovisuais, principalmente após o império da comunicação televisiva. As redes informacionais permitem ampliar a capacidade de pensar de modo inimaginável.*

[141] Cabe ressaltar que no início do século XXI, ainda, significativa camada popular não tem acesso a esse recurso.
[142] SILVEIRA, S. A., 2001, op. cit., p.8.
[143] Ibid, p.8.

O desenvolvimento tecnológico permitiu aumentar capacidade de armazenamento, a análise e o processamento de informações, proporcionando, inúmeros modos de relações pautados em dados. Este aumento, proveniente da revolução trouxe, também, o aumento da produção do conhecimento, criando novos meios de ensinar e aprender desenvolvendo múltiplas inteligências e determinando a revisão de velhos paradigmas.

O avanço da revolução tecnológica na sociedade do conhecimento[144] [145] aponta para a preocupação de Sérgio Amadeu da SILVEIRA (2001, p.16) quando alerta

> *Eis o maior perigo de se chegar atrasado a ela. Essa revolução, exatamente por fundar-se nas tecnologias da inteligência, amplia exponencialmente as diferenças na capacidade de tratar informações e transformá-las em conhecimento. Por isso essa revolução não apenas pode consolidar desigualdades sociais como também elevá-las, pois aprofunda o distanciamento cognitivo entre aqueles que já convivem com ela e os que dela estão apartados.*

Porém, não se pode afirmar que há uma total e segura certeza quanto ao futuro da revolução tecnológica, principalmente, pelas possibilidades dos avanços e a necessidade de mudança de pensamentos, comportamentos e de paradigmas nas Ciências e na sociedade. E apresenta uma especial preocupação com a necessidade de programas de inclusão digital buscando a igualdade social e tecnológica.

---

[144] A sociedade do conhecimento pode ser representada pelo "*conjunto de uma série de modificações, inovações sociais, institucionais, tecnológicas, organizacionais, econômicas e políticas, a partir das quais a informação e o conhecimento passaram a desempenhar um novo e estratégico papel. Tais inovações constituem-se em elementos de ruptura (para alguns), ou de forte diferenciação (para outros), em relação ao padrão pertencente, ainda que resultantes, em grande medida, de tendências e vetores que não são propriamente novos ou recentes*". LASTRES, H. M. M.; ALBAGLI, S. (org.). **Informação e globalização na era do conhecimento.** Rio de Janeiro: Campus, 1999, p. 8.

[145] Nesta sociedade há a configuração, a preocupação e a exigência de novos modelos, instrumentos institucionais, normativos, reguladores baseados em políticas tecnológicas de inovação e de busca do conhecimento, que visam responder aos anseios de uma nova realidade, a sócio-tecnológica.

4.2
Paradigmas

Nas últimas décadas do Século XX e no início do Século XXI, a Ciência tem contribuído para mudança de paradigmas ocasionado, especialmente, pela Revolução Tecnológica e informacional. Frente a esse novo panorama do desenvolvimento da sociedade Marcos Antonio Machado Ferreira de MELO (2000, p.21), aponta que

> *O mundo, a sociedade, tem por meta natural o desenvolvimento e sempre esteve envolto por constantes transformações, mudanças que são fomentadas por uma contínua evolução tecnológica. As revoluções tecnológicas foram e são marcadas por inúmeros desdobramentos no mundo social, institucional e jurídico. São quebras de modelos, de paradigmas.*

Assim, entende-se como paradigma uma caracterização histórica que atende um determinado modelo em uma determinada época. Para definir paradigma torna-se apropriado tomar a referência de Thomas KHUN, filósofo e historiador da ciência, que em sua obra "*As estruturas das revoluções científicas*" tem a preocupação em esclarecer o termo. Segundo Thomas KHUN (1996, p.225), um paradigma constitui-se de uma "*constelação de crenças, valores e técnicas partilhadas pelos membros de uma comunidade científica*". Ao referendar um modelo, a força de um paradigma está constituída no consenso de determinada comunidade científica durante uma certa época.

A contribuição de Maria Cândida MORAES (1997, p.31) torna-se significativa para o entendimento do que Thomas KHUN propõe em sua obra, quando indica que o "*paradigma, na ótica de Kuhn, é uma realização científica de grande envergadura, com base teórica e metodológica convincente e sedutora, e que passa a ser aceita pela maioria dos cientistas integrantes de uma comunidade*".

No sentido de aprimorar o conceito, Fritjof CAPRA (1996, p.25) se apropria da definição que Thomas KHUN e propõe o paradigma científico definindo-o como paradigma social, sendo "*uma constelação de concepções, valores, de percepções e de práticas compartilhadas por uma comunidade científica, que dá forma a uma visão particular da realidade, a qual constitui a base da maneira como a comunidade se organiza*".

Ao entender paradigma como um conjunto de crenças e valores que determina o modo de pensar e agir do homem em uma determinada época, Clodoaldo Meneguello CARDOSO (1995, p.17) referenda Thomas KHUN e propõe que "*o conceito de paradigma é entendido por mim como um modelo de pensar e ser capaz de engendrar determinadas teorias e linhas de pensamento dando certa homogeneidade a um modo de o homem ser no mundo, nos diversos momentos históricos*".

Com a contribuição destes autores para o entendimento do termo paradigma, esclarece-se que a superação de um paradigma científico não o invalida, não o torna errado ou nulo, mas evidencia que seus pressupostos e determinantes não correspondem mais às novas exigências históricas e sociais. A passagem para um novo paradigma não é abrupta e nem radical. É um processo que vai crescendo, se construindo e se legitimando. Na realidade, o novo paradigma incorpora alguns referenciais significativos do velho paradigma e que ainda atende aos anseios históricos de determinada época. Nesse processo de transição, os cientistas passam a desafiar os pressupostos do velho paradigma, embora ao anunciar um mundo novo ainda se assentem em bases mais utópicas do que concretas, como afirma Clodoaldo Meneguello CARDOSO (1995, p.17) "*a formação de um novo paradigma ocorre nas entranhas do anterior. E este, por sua vez, nunca desaparecerá totalmente*".

A crise e a resistência fazem parte deste processo de transposição: por um lado provocam um mal-estar na comunidade científica, derrubando alguns pilares de sustentação dos pensamentos, conceitos e ações, e por outro, instiga cientistas e intelectuais para reverem suas teorias e buscarem uma profunda renovação de suas concepções. Manuel CASTELLS (1999, p.77) apropriadamente aproxima as definições de paradigma à concepção da tecnologia quando conceitua

> *Um paradigma econômico e tecnológico é um agrupamento de inovações tecnológicas, organizacionais e administrativas inter-relacionadas cujas vantagens devem ser descobertas não apenas em uma nova gama de produtos e sistemas, mas também e sobretudo na dinâmica da estrutura dos custos relativos de todos os possíveis insumos para a produção*.

Observa-se a importância do desenvolvimento e da criação de um novo paradigma, propiciando a inclusão na construção do conhecimento de novas tecnologias que resultam na mudança da sociedade. Estas mudanças formam novas questões sociais e políticas como, por exemplo, o enfrentamento da exclusão digital.

4.3
A mudança paradigmática

A pesquisa dos paradigmas da Ciência e a influência na tecnologia acompanharam os momentos históricos e a evolução da produção do conhecimento. Nas últimas décadas do século XX, o paradigma inovador tinha forte tendência de ser denominado como paradigma emergente ou sistêmico, denominação utilizada por autores como Fritjof CAPRA (1996)[146] e Boaventura de Sousa SANTOS (2000)[147].

No entanto, na entrada do século XXI, Fritjof CAPRA (2002, p.13) no prefácio da sua obra *"As conexões ocultas. Ciências para vida sustentável"* modifica a denominação de paradigma emergente para denominação de

[146] CAPRA, F. **A teia da vida.** Uma nova compreensão cientifica dos sistemas vivos. São Paulo: Cultrix, 1996.
[147] SANTOS, B. S. **A crítica da razão indolente.** Contra o desperdício da experiência. Para um novo senso comum: a ciência, o direito e a política na transição paradigmática. São Paulo: Cortez, 2000, v. 1, p. 74.

Complexidade[148] envolvendo uma nova compreensão e concepção da vida. Para tanto, defende *"uma estrutura conceitual que integra as dimensões biológica, cognitiva e social da vida, da mente e da sociedade*" e, inclui o desenvolvimento de *"uma maneira coerente e sistêmica de encarar algumas das questões mais críticas da nossa época"*. Essa proposição necessita de alteração da visão de mundo, de sociedade e de homem. Nessa obra, Fritjof CAPRA (2002, p.14) afirma que ao escrever o *Ponto de Mutação* em 1982, previa a necessidade que "o *paradigma da física tinha que ser substituído por uma estrutura conceitual mais ampla, uma visão da realidade cujo centro fosse ocupado pela própria vida"* e complementa *"a nova visão da realidade que haveria enfim de substituir em diversas disciplinas a visão de mundo mecanicista e cartesiana ainda não estava de maneira alguma, plenamente desenvolvida e estruturada*".

Mas, o movimento que iniciou nos anos oitenta cresceu, como Fritjof CAPRA (2002, p.16) alerta

> ***Depois disso, cientistas e matemáticos deram um passo gigantesco rumo à formulação de uma teoria dos sistemas vivos: desenvolveram uma nova teoria matemática - um conjunto e técnicas matemáticas - para escrever e analisar a complexidade dos sistemas vivos. Isso tem sido chamado de 'teoria da complexidade' ou 'ciência da complexidade' nos escritos de divulgação científica. Os cientistas e matemáticos, por sua vez, preferem chamá-la pelo nome mais prosaico de 'dinâmica não-linear'.***

A manifestação de Fritjof CAPRA (1996) na obra intitulada *"Teia da Vida"*[149] apresentou referenciais significativos para mudança paradigmática que acompanhou os profissionais de todas a áreas do conhecimento no final do século XX. Fritjof CAPRA (2002, p.16) se manifesta sobre o papel dessa obra referindo-se ao alerta proposto para a comunidade científica por meio de *"um resumo da teoria matemática da complexidade e apresentei uma síntese das atuais teorias*

---

[148] Concordando com Fritjof CAPRA (2002) e Edgar MORIN (2000) desse momento em diante, nessa obra, o paradigma emergente ou sistêmico passa a denominar-se paradigma da complexidade.

[149] CAPRA, F., 1997,op. cit.

não-lineares sobre os seres vivos. Essa síntese pode ser compreendida como uma manifestação organizada de uma nova compreensão científica da vida".

Os físicos quânticos tiveram um papel relevante nesse processo de transformação, mas, como afirma Fritjof CAPRA (2002, p.129) "o*s físicos quânticos levaram bastante tempo para superar a sua crise, mas, no fim, obtiveram uma grande recompensa. Do esforço intelectual e emocional deles nasceram profundas intuições sobre a natureza do espaço, do tempo e da matéria, e, com elas, as linhas-mestras de todo um novo paradigma científico*".

O grande papel da contribuição de Fritjof CAPRA prende-se a proposição da superação da teoria não-linear e da proposição da conexão entre o domínio material e do domínio social. O desafio intenso e as manifestações de acolhimento e de repúdio fazem Fritjof CAPRA (2002, p.17) em *"As Conexões Ocultas"* confirmar que haverá superação da dualidade entre estruturas materiais e de estruturas sociais, pois *"... o principal desafio deste novo século – para cientistas sociais, os cientistas da natureza e todas pessoas- será a construção de comunidades ecologicamente sustentável, organizadas de tal modo que suas tecnologias e instituições sociais- suas estruturas materiais e sociais- não prejudiquem a capacidade intrínseca da natureza de sustentar a vida*".

A busca de superação da visão que propunha a dualidade em todos os segmentos da sociedade envolve também a tecnologia e, por conseqüência, as ações dos profissionais de todas as áreas do conhecimento. Afinal, a mudança paradigmática atinge a lógica epistemológica de conceber o universo, que segundo Maria Cândido MORAES (2004, p.129)

> ***[...] implica em uma abertura epistemológica que leve em conta o papel da incerteza e do diálogo, o desafio construtivo implícito na desordem em relação a ordem, garantindo, assim, a indispensável e flexível abertura de nosso olhar epistemológico, do nosso pensamento relacional que traz consigo 'verdades' biodegradáveis e, a cada dia, mais reconhecidamente, falíveis.***

A ênfase paradigmática é desenvolver uma estrutura teórica unificada e sistêmica para compreensão dos fenômenos biológicos, tecnológicos e sociais. Assim, Fritjof CAPRA (2002, p.267) alerta a comunidade científica para

> ***A idéia central dessa concepção sistêmica e unificada da vida é a de que o seu padrão básico de organização é a rede. Em todos os níveis de vida - desde as redes metabólicas dentro da célula até as teias alimentares dos ecossistemas e as redes de comunicações da sociedade humana -, os componentes dos sistemas vivos se interligam sob a forma de rede.***

Outro autor que apresentou forte influência para renomear o paradigma inovador foi Edgar MORIN, que passa a utilizar a denominação *"Paradigma da Complexidade"*[150]. Em sua obra, propõe a leitura do universo com a visão do todo e a reaproximação das partes fragmentadas pelo paradigma conservador. A indicação do paradigma da complexidade busca a produção do conhecimento e a formação para resolução de problemas globais, ou seja, tomar por suporte os conhecimentos fundamentais, parciais e locais com a visão do todo.

Para tanto, Edgar MORIN (2000, p.14) defende a existência do desafio para a superação da visão mecanicista do universo, quando propõe "*a supremacia do conhecimento fragmentado de acordo com as disciplinas impede freqüentemente de operar o vínculo entre as partes e a totalidade, e deve ser substituída por um modo de conhecimento capaz de apreender os objetos em seu contexto, sua complexidade, seu conjunto*". E, acrescenta "*é necessário desenvolver a aptidão natural do espírito humano para situar todas essas informações em um contexto e um conjunto. É preciso ensinar os métodos que permitem estabelecer as relações mútuas e as influências recíprocas entre as partes e o todo em um mundo complexo*".

A humanidade, acostumada aos princípios reducionistas e as certezas absolutas e inquestionáveis propostas pelo pensamento newtoniano-cartesiano, precisa repensar a lógica epistemológica que regeu o universo nesses últimos

---

[150] MORIN, E. **Os sete saberes necessários a educação do futuro.** São Paulo: Cortez, Brasília: UNESCO, 2000.

séculos. Neste contexto, Edgar MORIN (2000, p.16) propõe que deve-se *"ensinar princípios de estratégia que permitiriam enfrentar os imprevistos, o inesperado e a incerteza, e modificar seu desenvolvimento, em virtude das informações adquiridas ao longo do tempo. É preciso aprender a navegar em um oceano de incertezas em meio a arquipélagos de certezas"*. Trata-se do abandono da visão determinista da história humana, tornando o homem um sujeito que constrói sua própria história, e por conseqüência, requer uma nova visão de mundo.

Nesse sentido, a contribuição da sociedade do conhecimento e da revolução tecnológica tem provocado inúmeras realidades diferenciadas que passam a desafiar a busca de possíveis soluções aos novos questionamentos em todas as áreas do conhecimento. O ambiente jurídico regido por uma forte influência conservadora, reducionista e positivista tem sido provocado pela revolução paradigmática. Nesse processo, o Direito, desafiado pela mudança paradigmática e tecnológica, precisa reconstruir velhos paradigmas e construir novos para atender as novas necessidades sociais.

No entanto, essas novidades e mudanças não têm atingido as comunidades como um todo, privilegiando os cidadãos de camadas abastadas, causando um posicionamento ético questionável. O paradigma das complexidades vem alertar a comunidade em geral para a necessária inclusão social na busca de convivência pacífica da humanidade na comunidade mundial, especialmente, na tentativa da superação de conflitos entre os povos, de neutralização de processos de violência e de supressão das atitudes de agressão à natureza e aos seres vivos. Nesse sentido, a proposição do conhecimento isolado em partes não oferece uma visão adequada do contexto em que se insere e nem uma visão global. O entendimento de global é defendido por Edgar MORIN (2000, p.37) como

> ***O global é mais que o contexto, é o conjunto das diversas partes ligadas a ele de modo inter-retroativo ou organizacional. Dessa maneira, uma sociedade é mais que um contexto: é o todo organizador de que fazemos parte... O todo tem qualidades ou propriedades que não são encontradas nas partes, se estas estiverem isoladas umas das outras, e certas qualidades ou propriedades das partes podem ser inibidas pelas restrições provenientes do todo [...] é preciso efetivamente recompor o todo para conhecer as partes.***

A proposição do global retrata o novo desafio para superar a visão disciplinar, mecânica e reducionista criada pelos cientistas a partir do século XVIII. O Direito tem papel essencial neste processo paradigmático transformador, pois, exige a visão global de homem, de sociedade e de mundo. A formação envolve a construção para a cidadania, para responsabilidade social e a intervenção consciente na sociedade.

O processo de transformação está ligado diretamente ao Direito nos diversos segmentos, especialmente, com a finalidade de formar cidadãos para atuar no século XXI. Neste contexto, os procedimentos tecnológicos aplicados ao Direito precisam ser compatíveis com a nova leitura de mundo advindo da visão sistêmica e complexa da sociedade. Boaventura de Sousa SANTOS (2000, p.185) indica que

> ***O direito moderno oferece uma vantagem estratégica para a apreciação sociológica da transição devido à sua estreita articulação com a ciência moderna em todo o processo de racionalização da vida social prometida pela modernidade. A tarefa de racionalização, concebida como um equilíbrio dinâmico e tenso entre regulamentação e emancipação, foi confiada à ciência. A solução dos problemas decorrentes da insuficiência do conhecimento cientifico, só superável a longo prazo, foi confiada ao direito. Como racionalizador de segunda ordem da vida social, o direito – na forma de direito estatal – entrou numa fase de crescimento ilimitado, semelhante ao pretendido para a ciência e para toda a transformação social.***

Assim, Boaventura de Sousa SANTOS (2000, p.160-164) ainda observando as exigências do novo paradigma (da complexidade), contribui quando indica que ao Direito cabe um repensar efetivo e radical sobre a ciência moderna e sobre o próprio Direito moderno. Esta idéia confirma a possibilidade de aplicação, avanço e adaptação do Direito, em seus mais variados ramos, à mudança paradigmática. O autor ainda defende que *"a discussão paradigmática do direito moderno, em conjunto com a da ciência moderna, irá esclarecer os termos e as direcções*(sic) *possíveis da transição para um novo paradigma societal*(sic)*"* (SANTOS, p.164).

Nota-se que o paradigma da complexidade absorve características fortemente enfocadas na visão de totalidade, de interconexão, de inter-relacionamento, e, especialmente, na superação da visão fragmentada da sociedade. Trata-se de buscar a reaproximação das partes para reconstituir o todo nas variadas áreas do conhecimento. O paradigma da complexidade contempla a inclusão de gênero, homens e mulheres, independente de raça, sexo, credo, cor e condição econômica. O enfrentamento da inclusão digital tornou-se um desafio a ser enfrentado por todas as áreas do conhecimento, em especial, pelo Direito.

4.4
A inclusão digital

Para analisar e buscar compreender a inclusão digital há a necessidade de observar a situação atual da utilização e das influências da tecnologia no cotidiano. A sociedade vem passando por inúmeras mudanças em todas as áreas, em especial, na social, econômica e comportamental, pois tem exigido novas maneiras de pensar e agir. Tais mudanças, foram o marco definitivo para a transformação, transposição e caracterização para a sociedade do conhecimento. Pautada no paradigma da complexidade, que tem buscado superar os comportamentos e procedimentos tradicionais, essa revolução gerou as mais diversas alterações como: o modo de trabalhar, de interagir com o próximo, mas, principalmente, o modo de viver da humanidade.

Face a evolução paradigmática, alguns conceitos e idéias foram modificados ou revistos. Pode-se afirmar que não existem mais verdades absolutas, muitas certezas são temporárias e provisórias, criando um ar de incerteza, inquietação e constantes questionamentos. Essa situação advém do desenvolvimento da sociedade do conhecimento, de suas descobertas e processos de superação, gerando um ambiente instável em face de problemas e situações de

imprevisibilidade e na necessidade da busca de soluções rápidas e eficazes por certo tempo histórico.

Outro aspecto predominante, neste panorama da evolução paradigmática tecnológica, foi a impressão da competitividade como marca da sociedade. Esta marca é representada pelas disputas, nas quais apenas os melhores vencem, bem como, os mais ágeis, criativos, críticos e preparados. Principalmente, porque o acesso ao conhecimento escrito, abstrato e distante da realidade não é suficiente, é necessário que ele esteja atrelado ao fazer, à utilização e ao desenvolvimento de habilidades e competências que, somados, resultem na solução de problemas sociais, econômicos e tecnológicos.

A velocidade da evolução de transformação tecnológica é cada vez maior e resulta, também, num distanciamento maior dos que não têm acesso a essa nova realidade. Exemplifica Sérgio Amadeu da SILVEIRA (2001, p.17)

> *Para acessar a Internet, a rede mundial de computadores, é preciso pagar mensalmente um provedor de acesso e o gasto com a conta telefônica. Além disso, é preciso ter um computador que custa mais de 1.000 reais. Em um país com quase um terço da sociedade abaixo da linha da pobreza, gastar algo em torno de 40 reais por mês pelo uso mínimo de conexão e conta telefônica é impossível para a maioria da população.*

Portanto, frutos dessa nova realidade, nasceram os "excluídos digitais". Ou seja, enquanto indivíduos de classes sociais mais altas, passam seus dias interagindo, informando-se e criticando situações e conteúdos de *sites*[151], os indivíduos de classes mais pobres estão, muitas vezes, longe desta realidade informática e informacional. Para os ativos na rede, os denominados incluídos, a Internet é a possibilidade de conhecer o mundo. Nesse sentido, destaca Sérgio Amadeu da SILVEIRA (2001, p.17)

[151] Nos dias de hoje, são milhões de sites distribuídos pela rede, sobre os mais diversos temas.

> *Quem está desconectado desconhece o oceano informacional, ficando impossibilitado de encontrar uma informação básica, descobrir novos temas, de despertar para novos interesses.*
> *[...] não conseguem se comunicar com a velocidade dos incluídos pela comunicação mediada por computador.*

Frente a esta realidade de desconhecimento e e rapidez na evolução ponde ser apontados os seguintes dados do Instituto Brasileiro de Geografia e Estatística (IBGE), porém referentes a 2002, no Brasil, somente 16,3% dos domicílios possuem computador, sendo que apenas 12% com acesso à Internet[152].

Assim, alguns poucos podem acessar o conhecimento informacional, enquanto, grande parte da população do país não tem condições mínimas de acessibilidade. A tecnologia está presente nos bancos, nas empresas, nos hospitais, nas escolas entre outros ambientes. Mesmo usufruindo desses recursos indiretamente[153], a população tem dificuldade em se conectar à rede de conhecimentos via eletrônica. Segundo Sérgio Amadeu da SILVEIRA (2001, p.18) a falta de acesso pode agravar-se pois

> *Além de ser um veto cognitivo e um rompimento com a mais liberal das idéias de igualdade formal e de direito de oportunidade, a exclusão digital impede que se reduza a exclusão social, uma vez que as principais atividades econômicas, governamentais e boa parte da produção cultural da sociedade vão migrando para a rede, sendo praticadas e divulgadas por meio da comunicação informacional. Estar fora dos principais fluxos de informação. Desconhecer seus fluxos de informação. Desconhecer seus procedimentos básicos é amargar a nova ignorância.*

Face a essa realidade optou-se por desenvolver esse estudo pela visão da temática da inclusão digital, especialmente, por entender que a exclusão social possibilita apontar erros e problemas, mas muitas vezes, não apresenta possíveis caminhos de superação. Conforme a nova proposta paradigmática, deve-se

---

[152] Disponível em https://gestao.idbrasil.gov.br/noticias/News_Item.2004-05-31.1051/view Acesso em 10 set 2005.
[153] Pois, a tecnologia está em ambientes que exigem sua utilização, como em bancos, porém não interage diretamente com computadores ou com a Internet.

apontar dentro da inclusão digital a possibilidade de envolver as pessoas em novas economias, e em novas formas de sociedade, além de fornecer mecanismos de conhecimento de seus direitos, aumentando a cidadania e melhorando as condições de vida.

Assim, visa-se uma releitura de mundo, pautada na justiça, na democracia, na solidariedade, no acesso, nas condições de vida, na saúde, na tecnologia, na educação. Paulo FREIRE & Ana Maria FREIRE (2001, p.99) ao aplicar a releitura de mundo à educação destacam que

> ***A educação para os direitos humanos, na perspectiva da justiça, é exatamente aquela educação que desperta os dominados para a necessidade da briga, da organização, da mobilização crítica, justa, democrática, séria, rigorosa, disciplinada, sem manipulações, com vistas à reinvenção do mundo, à reinvenção do poder.***

A inclusão digital, inicialmente, foi confundida com a inclusão social, assim, considerada como um esforço em busca de implantação de ações de acesso[154] na sociedade do conhecimento. Face à realidade social atual o conhecer, a informação e a aprendizagem passam a ter enorme relevância. Nesse contexto, pode-se apontar diversos impactos sociais gerados por esta nova forma de sociedade, na qual a inclusão busca amenizar e democratizar o acesso ao conhecimento à todos os cidadãos que hoje encontram-se fora deste processo.

Porém, não há como separar a inclusão digital da inclusão social, pois a sociedade da informação tem como um de seus objetivos primordiais à segurança e possibilidade de alcance da cidadania. Sobre a proposta de inclusão, Paulo FREIRE e Ana Maria FREIRE (2001, p.99) defenderam que *"sem dúvida alguma, é possível crer que com a maciça inclusão das pessoas na sociedade da informação teremos uma explosão das possibilidades da cidadania. E quanto mais cidadãs forem as pessoas, mais conscientes serão das necessidades de*

[154] Este acesso visa permitir, além do conhecimento puro, a possibilidade de ampliar horizontes amparando os cidadãos na sociedade atual, competitiva, criando redes de solidariedade, de democracia e de defesa dos direitos de cidadania.

reinvenção da dinâmica social excludente e desigual"[155]. A inclusão social não deve ser apartada da digital, também pelos motivos apontados por Luiz GUSHIKEN (2004, p.58) em entrevista à Revista ISTOÉ Dinheiro

> *É difícil fazer uma hierarquia rígida entre atender as demandas mais importantes do País como a questão da fome e depois outros níveis de necessidades da população como a inclusão digital. O esforço é estruturar esses movimentos em paralelo. Oferecer aos nossos jovens acesso à banda larga e à Internet é uma questão de estratégia da qual o governo terá de cumprir. Nenhum povo conseguirá um salto rápido de qualidade se não acessar esse conhecimento que está fora do circuito tradicional das escolas, universidades e centros de pesquisa. Hoje o conhecimento se espalha por vários meios e mecanismos. Devemos melhorar a estrutura no circuito formal que são as escolas e ao mesmo tempo criar um modelo de inclusão digital para que todos os brasileiros tenham acesso.*

Mas, a inclusão digital, enquanto conceito, engloba novas tecnologias de informação, comunicação, educação, levando à construção da cidadania com características criativas, empreendedora e democrática. Com isso, torna-se também um meio de gerar e disseminar a melhoria da qualidade de vida, sendo um fator relevante para a liberdade social, a geração de conhecimento e a troca de informações. Como identificou Gilberto DIMENSTEIN (2004, p.57), da Fundação do Aprendiz, no Fórum Dinheiro, *"a demanda pelo conhecimento na rede está cada vez maior*".

Não se pode deixar de lado que, reconhecidas as condições econômicas, culturas políticas, históricas, há a apresentação de "*novos requisitos metodológicos e táticos, de modo que é sempre necessário pesquisar a atualização da substantividade de idéias com qualquer nova situação*"[156].

Na verdade, observando a informática enquanto área de acesso à produção do conhecimento, qualquer indivíduo depara-se com uma linguagem específica, de difícil compreensão e com necessidade de muito estudo e

[155] FREIRE, P.; FREIRE, A. M. (org.), 2001,op. cit., p. 99.
[156] FREIRE, P.; FREIRE, A. M.(org.), 2001, op. cit., p. 80.

conhecimento. Frente a este mundo informatizado a Inclusão Digital vem com o objetivo de promover o relacionamento do cidadão com o computador, com suas possibilidades e potencialidades, porém, tendo como foco principal os excluídos sociais[157]. Com isso, passa a fornecer conhecimento por meio de equipamentos e lições básicas das operações de uso socialmente estabelecido[158], promove-se a alfabetização digital[159] e a utilização de programas e recursos comumente utilizados no mundo digital. Bem como, busca-se o barateamento de máquinas básicas, utilizando-se, por exemplo, da promoção de projetos e linhas de financiamentos de fácil acesso voltadas à aquisição e melhoria da qualidade de vida.

Ao analisar a inclusão digital, pode-se indicar que ela propicia um conjunto de possibilidades, tais como: a necessidade de criação de políticas públicas visando a organização e a defesa do direito do cidadão; a capacitação do cidadão proporcionando a oportunidade de busca de informações e da transformação da realidade, introduzindo-o em espaços democráticos já existentes e tornando-o capaz de criar novos espaços para o desenvolvimento e aplicação da justiça, da paz, da igualdade e da democracia; disponibilizar equipamentos e acesso à informações digitais para todos sem distinção.

No processo de inclusão digital podem ser identificados vários agentes envolvidos, como o governo, os parceiros e os usuários. A relação governo e parcerias podem ser analisadas sobre o prisma da necessidade de informações, iniciativas e incentivos para a busca da inclusão digital como indica Luiz GUSHIKEN (2004, p.60) ao falar pelo governo

---

[157] Entende-se por excluídos sociais:as camadas pobres da população, os idosos, os deficientes, os segregados em hospitais, prisões, entre outros. *"Na maioria das vezes são os integrantes das camadas mais pobres que estão à margem dessa revolução tecnológica, grupo que pode ser definido como excluídos digitais*" FORUM DINHEIRO. FORUM DINHEIRO. O desfio na rede. Seminário Três Editorial. REVISTA: ISTOÉ Dinheiro., nº 284, p. 55-70, 8 de dezembro de 2004, p.56.

[158] Podem ser consideradas operações de uso socialmente estabelecido a utilização de banco, o preenchimento de certos formulários, questões sobre impostos, o acompanhamento da política pública, entre outros.

[159] A alfabetização digital refere-se ao alcance da linguagem digital, por meio do domínio das ferramentas, programas, sistema, organização de informações e equipamentos.

Devemos nos posicionar como um grande articulador de políticas públicas e buscar parcerias externas. Existem vários setores da sociedade já investindo na área social e muitas dessas iniciativas são de inclusão digital. O que falta é um foco preciso da sociedade em relação ao conceito. O governo pode ser o estimulador desse movimento. Pode criar esse foco, uma base mínima para a integração entre as políticas do governo e da sociedade no mesmo espaço.

A sociedade contemporânea está passando por um processo de mudança no modelo dominante, ou seja, está se desenvolvendo um modelo que inclui os modelos informacionais, revestidos por uma nova roupagem tecnológica, econômica, política, organizacional e de gestão coletiva. Em virtude desta mudança a Internet, não pode ser considerada apenas uma nova tecnologia da informação, mas sim, como um meio que pode auxiliar na organização econômica e social como um todo, sob a forma de capacitador e possibilitador da produção do conhecimento.

Ao analisar a conjuntura do setor empresarial, pode-se identificar o seu desenvolvimento e aprendizado dentro deste novo paradigma e modelo de sociedade. Tal aspecto pode ser reconhecido pelas ações que vêm sendo utilizadas como: o comércio eletrônico, as relações externas, os processos de organização interna e a busca da melhoria da qualidade de serviços. As empresas estão face a face com um ambiente altamente competitivo, em virtude dessa realidade. A inclusão digital busca uma forma de melhoria, de acesso, também, às empresas, visando adequação, compatibilização e promoção de sua interação e integração no mundo digital.

As mudanças tecnológicas, quase diárias, necessitam também de uma regulamentação, devendo observar aspectos éticos, pautada em princípios como a solidariedade, o humanismo, a democracia, a igualdade, entre outros, visando um avanço para a sociedade e para a economia. Deve-se levar em conta que a possibilidade de inclusão de um maior número de cidadãos, resulta num aumento da produtividade, e com esta melhoria será facilitado o desenvolvimento de um Estado baseado no *"bem-estar social"*[160].

---

[160] **GOVERNO ELETRÔNICO**. Disponível em <http://www.governoeletronico.gov.br/governoeletronico/index.htm>. Acesso em 06 fev. 2005.

A necessidade de uma regulamentação adequada, em busca da inclusão digital, provoca o estudioso e o aplicador do Direito a preparar-se para as novas realidades, bem como, preocupar-se com os acontecimentos e inovações sociais e tecnológicas, assim como indica Marco Antonio Machado Ferreira de MELO (2000, p.32-33)

> *A Informática Jurídica e o Direito da informática assumem papel preponderante neste início de novo milênio, caracterizado pelo avanço da tecnologia eletrônica, concentrada nas mãos de uma pequena fração que detém o domínio tecnológico. Quem tem mais tecnologia, tem mais riqueza. É visível que esta riqueza está cada vez mais concentrada no mundo. Sua conseqüência é a exclusão social. Seus reflexos são perniciosos para as sociedades menos desenvolvidas. Nem todos têm acesso às novas tecnologias, mas muitos poderão, de certa forma e indiretamente, ser por elas atingidos.*

Neste contexto, analisando as diferenças de possibilidades, as discriminações e seus resultados, em busca de uma sociedade democrática Paulo FREIRE & Ana Maria FREIRE (2001, p.79) manifestam-se, afirmando que

> *Respeito pelo outro implica, necessariamente, minha recusa em aceitar todo tipo de discriminação, minha oposição radical à discriminação racial, à discriminação de gênero, discriminação de classe, e discriminação cultural, fora das quais eu não seria capaz de me entender. Outra substantividade de minhas idéias é minha compreensão da historia como possibilidade, minha rejeição de qualquer compreensão fatalista ou visão determinista da história.*

Não é necessário aceitar a realidade como fatalista, pode-se transformá-la, isto depende dos juristas, dos tecnólogos, dos sociólogos, dos educadores, entre outros. Nesse contexto, Paulo FREIRE e Ana Maria FREIRE (2001, p.80) complementam

> *Outro aspecto de minha substantividade é o amor incondicional pela liberdade e minha certeza de que podemos nos tornar seres transformativos e não adaptativos, que podemos nos tornar seres dialógicos, eu podemos também nos tornar seres com capacidade para tomar decisões e que podemos também desenvolver a capacidade para a ruptura. Logo, por isso combato e luto contra qualquer sistema – social, econômico, político – que me proíba de ser, de perguntar, de discutir, de intervir, de ser um ser humano descente.*

Assim, ao Direito cabe, não apenas a tarefa da regulamentação, mas, a participação na formação de uma consciência e na vivência do processo de inclusão social, apoiando projetos, formulando propostas e até mesmo analisando os aspectos evolutivos e práticos dos avanços e necessidades tecnológicas.

4.5
Projetos governamentais para aumento da participação dos cidadãos no mundo digital

Muitas áreas jurídicas e governamentais estão preocupadas com a questão da inclusão digital como a Fiesp e a Câmara-e.net que, em busca da diminuição das desigualdades e da exclusão digital e a melhoria no desenvolvimento para a área empresarial, elaboraram e enviaram aos candidatos à eleições em 2002, a seguinte lista

> ***1. A digitalização é inexorável: a Internet, como mídia da sociedade do conhecimento, permeia todas as atividades econômicas, quebrando paradigmas históricos da sociedade industrial; 2. O setor privado deve liderar: a sociedade civil deve pautar e liderar o processo de formulação de políticas públicas e regulatórias sobre a economia digital; 3. Menos legislação: garantir um ambiente regulatório flexível à evolução das tecnologias, evitando o formalismo da cultura jurídica brasileira, por meio da valorização da jurisprudência, da arbitragem, da auto-regulação e***

auto-regulamentação; 4. Menos barreiras internacionais: facilitar o comércio exterior por meio da harmonização das legislações, da racionalização dos critérios tributários e do incentivo aos negócios on-line; 5. Governo mais eletrônico: e-Gov significa modernizar o Estado, democratizar os mecanismos de compras públicas, aumentar a transparência e disponibilizar mais canais de exercício da cidadania. As iniciativas dos governos federal, estadual e municipal devem ser integradas; 6. Inclusão empresarial é o caminho: conectar o micro, pequeno e médio empresários significa modernizá-los, desenvolvê-los e transformá-los em principais agentes de promoção da inclusão digital do cidadão; 7. Mais educação: inclusão digital não é 'um micro para cada cidadão', mas evitar que a digitalização de processos marginalize ainda mais os 'desconectados' do mercado de trabalho e das relações de consumo; 8. Não descuidar da infra-estrutura: garantir, sempre, tecnologia de vanguarda, por meio de estímulo à pesquisa, fortalecimento da indústria nacional e conseqüente barateamento de equipamentos, programas e serviços; 9. Proteção à privacidade: informações confidenciais de usuários devem ser utilizadas só para seus fins específicos; 10. Segurança é fundamental: é obrigação do Estado e das empresas zelar pela inviolabilidade dos dados que trafeguem em seus sistemas[161].

Este rol de propostas pode ser considerado, um alerta sobre certas preocupações e anseios de vários setores não só econômicos, mas também setores como o social, o educacional, o jurídico, entre outros.

Nesse item pretende-se destacar os principais projetos governamentais, havendo preocupação em não apresentar exaustivamente todos, mas identificar seus principais objetivos e metas, entre eles destaca-se os TELECENTROS, o @lis, o Paraná Digital e o Governo Eletrônico.

4.5.1
TELECENTROS

[161] TORQUATO, C.. Por uma política nacional de tecnologia da informação e comércio eletrônico. In: Revista **B2B MAGAZINE**. Ano 2, nº23, Out, 2002, p. 70.

Este projeto iniciou-se como uma proposta e hoje é uma realidade nacional, pela implantação dos **TELECENTROS**. *"Nas comunidades mais carentes, a porta de entrada para o mundo digital são espaços comunitários nos quais há computadores com acesso à Internet e instrutores que orientam os usuários em suas necessidades dentro desse novo mundo"*[162].

Os TELECENTROS se traduzem em espaços compostos por computadores conectados à Internet, pelo sistema de banda larga, sendo cada unidade formada por um grupo de 10 a 20 microcomputadores em funcionamento. A meta fundamental é proporcionar à população, que compõe certa comunidade, a liberdade de utilização dos equipamentos, cursos de informática básica, bem como, oficinas especiais na área da tecnologia.

Destacam-se como objetivos o

> *uso intensivo da tecnologia da informação para ampliar a cidadania e combater a pobreza, visando garantir a privacidade e segurança digital do cidadão, sua inserção na sociedade da informação e o fortalecimento do desenvolvimento local"*, mas seu principal objetivo é *"organizar uma rede de unidades de múltiplas funções que permita às pessoas adquirirem autonomia tecnológica básica e privacidade a partir do software livre*[163].

Nota-se que a inclusão digital é o foco central dos TELECENTROS, como explica o IDBRASIL[164] ao apontar que

> *Trata-se de uma iniciativa fundamental para capacitar a população brasileira e inseri-la na sociedade da informação, para assegurar a preservação de nossa cultura com a construção de sites de língua portuguesa e de temáticas vinculadas ao nosso cotidiano, qualificar profissionalmente nossos trabalhadores, incentivar a criação de postos de trabalho de maior qualidade, afirmar os direitos das mulheres e crianças, para um desenvolvimento tecnológico sustentável e ambientalmente correto,*

---

[162] FORUM DINHEIRO., 2004, op. cit., p. 61.

[163] IDBRASIL. Disponível em: <http://www.idbrasil.gov.br/docs_telecentro/docs_telecentro/o_que_e>. Acesso em 06 fev. 2005.

[164] O IDBRASIL - Inclusão Digital Brasil - é um portal oficial do Ministério da Comunicação que tem por objetivo a promoção da inclusão digital a todo país, traz definições, objetivos, regulamentação e funcionamento dos TELECENTROS. Porém ainda trata de outros assuntos ligados à inclusão digital como o software livre, tv digital, fome zero, FUST, links de acesso à outros Ministérios, bem como possibilita o acesso ao GESAC – Governo Eletrônico - Serviço de Atendimento ao Cidadão, entre outros.

aprimorar a relação entre o cidadão e o poder público, enfim, para a construção da cidadania digital e ativa[165].

Sua idéia fundamental gira em torno da modificação de postura e da capacidade da sociedade, pautada na cultura, na profissionalização, no aumento de trabalhadores capacitados, e, o mais importante, o direito à tecnologia ao alcance do cidadão. Assim como, propõe a criação de estruturas em busca de condições para parcerias com a iniciativa privada, buscando a redução nos custos, gerando a possibilidade da criação de outros TELECENTROS. Os Estados com maior destaque nesse tipo de projeto são: São Paulo, Rio de Janeiro, Paraná, Santa Catarina e Distrito Federal. Outras propostas são desenvolvidas com a mesma função e estão espalhados por todo país, porém cada uma leva um nome diferenciado, como, por exemplo, os FARÓIS DO SABER em Curitiba-PR.

Ao analisar os projetos de TELECENTROS, depara-se com a realidade de que a evolução tecnológica é muito intensa, e, representa iniciativa de importância, na atualidade, da comunicação via Internet, principalmente ao possibilitar a interação do cidadão com o poder público. A partir do momento que um TELECENTRO está conectado à Internet passa a proporcionar à comunidade interessada a possibilidade de estudos, pesquisas, comunicações, desenvolvimento de conhecimento, oportunidades de trabalho[166] e de vida[167], entre outros.

Podem ser destacadas duas modalidades de TELECENTROS, os diretos que estão instalados em prédios ou terrenos das prefeituras, e os conveniados instalados em espaços cedidos por entidades ou associações conveniadas com as prefeituras. Porém, nos dois modelos as prefeituras são responsáveis pela implantação dos equipamentos, pelos funcionários e, principalmente, pela manutenção e garantia do funcionamento.

Para a administração, gestão e fiscalização do TELECENTROS, um grupo de componentes da comunidade local forma um Conselho Gestor, que fica

---

[165] IDBRASIL., 2005, op. cit.

[166] Pois os usuários podem confeccionar e enviar seus currículos, bem como realizar cursos à distância.

[167] Conhecer a respeito de saúde, educação, interagir com outras pessoas e trocar idéias e interesses.

responsável pela manutenção do local e dos funcionários[168]. Assim, a comunidade ao receber o novo projeto se reúne, em uma primeira plenária visando a preparação para a eleição do conselho, bem como, discutem o estatuto, o regimento e as tarefas que serão assumidas por seus envolvidos, como cada um participará com o intuito de oferecer serviços com qualidade. Ainda, devem discutir e traçar o Plano Local de Inclusão Digital.

O funcionamento dos TELECENTROS, tem por premissa a qualidade, e deverá, entre suas atividades, incluir

- *Criação do site da própria comunidade com hospedagem assegurada em um Portal;*
- *Manutenção e atualização do site do telecentro;*
- *Publicação de dados, notícias e informações;*
- *Criação e formulação de experiências de economia solidária;*
- *Criação de oficinas e incubadoras de empreendimentos culturais e de negócios que utilizem as redes informacionais como elemento importante;*
- *Ser canal de expressão social e cultural da comunidade para a própria comunidade e desta para o mundo;*
- *Estímulo às práticas educacionais formais e não-formais definidas pela comunidade;*
- *Estímulo à criação de fóruns eletrônicos e mecanismos democráticos de tomada de decisão;*
- *Estímulo ao controle dos governos;*
- *Estímulo às práticas de esclarecimento dos direitos básicos da cidadania;*
- *Incentivo para a comunidade participar de uma teia de comunicação autônoma de todos os telecentros do país*[169].

Na plenária seguinte é eleito o Conselho Gestor, que trabalha sob a forma voluntária e segue as indicações[170] das atividades citadas. Por serem representantes do povo, são os cidadãos que exigem a manutenção da qualidade dos TELECENTROS, assim mantém estrito contato com as prefeituras. Por outro lado, também prezam pelo funcionamento adequado em relação aos seus usuários. Além deste aspecto de fiscalização e vigilância, ainda, estimulam a criação de

[168] PREFEITURA DE SÃO PAULO. Disponível em: <http://portal.prefeitura.sp.gov.br/cidadania/coordenadoria_governo_eletronico/pid/0001>. Acesso em 06 fev. de 2005.
[169] IDBRASIL., 2005, op. cit.
[170] Estas são fornecidas pelo IDBRASIL.

novidades e iniciativas comunitárias em prol do bairro e das pequenas empresas que compõe a comunidade atendida. Com isso, "*além de ser um ponto de presença do governo, é um ponto de referência da comunidade, portanto, o trabalho de recepção e atendimento ao cidadão é fundamental*"[171]. Isto possibilita a proximidade e o reconhecimento dos aspectos sociais, tecnológicos e metodológicos da região em que foi implantado o TELECENTRO.

Ao analisar a proposição da criação de um Plano de Inclusão Digital, deve-se levar em consideração os seguintes pressupostos, como indica o IDBRASIL

> ***Primeiro**: é o reconhecimento que a exclusão digital amplia a miséria e dificulta o desenvolvimento humano local e nacional. A exclusão digital não se trata de uma mera conseqüência da pobreza crônica, mas torna-se fator de congelamento da condição de miséria e de grande distanciamento das sociedades ricas. **Segundo**: é a constatação de que o mercado não irá incluir na era da informação os extratos pobres e desprovidos de dinheiro. A própria alfabetização e escolarização da população não seria massiva se não fosse pela transformação da educação em política pública e gratuita. A alfabetização digital e a formação básica para viver na cibercultura também dependerão da ação do Estado para serem amplas ou universalistas. **Terceiro**: a velocidade da inclusão é decisiva para que a sociedade tenha sujeitos e quadros em número suficiente para aproveitar as brechas de desenvolvimento no contexto da mundialização de trocas desiguais e, também, para adquirir capacidade de gerar inovações. **Quarto**: é a aceitação de que a liberdade de expressão e o direito de se comunicar seriam falácias se fossem apenas para a minoria que tem acesso à comunicação em rede*[172].

Face à consolidação destes pressupostos deve-se levar em conta que, a comunicação passou a ser um sinônimo de troca de informações por computadores, e assim, passou também a ser um direito. Com isso, tornou-se uma questão de cidadania, passando a inclusão digital a ser também uma questão de política pública.

Além do envolvimento da comunidade, outras parcerias foram realizadas com organizações especializadas, como, por exemplo, a Rede de Informações para

---

[171] IDBRASIL., 2005, op. cit.
[172] IDBRASIL., 2005, op. cit.

o Terceiro Setor (RITS)[173] que auxiliam no recrutamento e preparo dos funcionários na própria comunidade que será beneficiada pelos TELECENTROS.

Nos projetos dos TELECENTROS, que viraram realidade, o Poder Público unido à comunidade e aos seus parceiros, produziu significativos resultados, como, por exemplo, o incentivo a criação e ao desenvolvimento de empresas locais que atua na área tecnológica. Destaca-se que a ligação com a comunidade na criação e aplicação de um Plano de Inclusão Digital levou ao aperfeiçoamento e evolução constante dos TELECENTROS, garantindo seu funcionamento, estabilidade e permanência.

4.5.2
@lis – Aliança para Sociedade da Informação[174]

A Aliança para Sociedade da Informação foi criada em 1999, porém sua implantação ocorreu por volta de 2001, tendo por objetivo principal a busca de um diálogo a respeito da inclusão digital entre a União Européia e a América Latina, com isso visa a redução da exclusão digital e a extensão das vantagens na Sociedade do Conhecimento à todos os cidadãos.

A introdução da América Latina na sociedade do conhecimento, pela cooperação com a União Européia, se deu por meio da aplicação de práticas inovadoras em correspondência às necessidades das regiões beneficiadas, resultando numa maior interconexão. Por meio da aplicação de novas tecnologias, busca a criação de oportunidades para a população, possibilitando o surgimento de novas ocupações e competências, bem como colaboração para empresas e para o

---

[173] Para mais informações sobre a Rede de informações para o terceiro setor, projetos, apoios, objetivos, e demais esclarecimentos, pesquisar em http://www.rits.org.br/

[174] COORDENADORIA DO GOVERNO ELETRÔNICO. Disponível em: <http://portal.prefeitura.sp.gov.br/cidadania/coordenadoria_governo_eletronico/internet_cidada/0001>. Acesso em 06 fev. 2005.

desenvolvimento do país. Isto se dá pela divulgação de projetos de capacitação e aprimoramento tecnológico dos cidadãos.

Em busca da promoção da inclusão digital, ofereceu-se não só o acesso mais amplo às novas tecnologias, mas também se propiciou a apresentação de um maior conteúdo, com qualidade e desenvolvimento tecnológicos, visando à capacitação digital. Aos envolvidos dá-se o nome de Cibernárium, também chamado de sócio, o qual tem por objetivo aproveitar dos conteúdos e metodologias disponibilizados às equipes resultando no desenvolvimento de diferentes capacidades digitais, que oportunizarão maior crescimento pessoal e comunitário. A princípio as atribuições dos sócios eram coordenar o projeto e o processo de produção dos materiais e o desenvolvimento de suas atuações. As atividades passaram a ficar mais definidas[175]

> *- Barcelona: espaço web e coordenação do projeto*
> *- Bruxelas: simulador TIC (Tecnologia de Informação e Comunicação) para alfabetização digital básica, 6 materiais de divulgação para auto formação de TIC e 6 profissionalizantes e 1 curso de formação on line para Agentes de Divulgação Digital*
> *- San Sebastian: software de gestão do projeto, software de navegação e metodologia de informática para assessoria tecnológica-Contact Center*
> *- Tampere: formação online*
> *- São Paulo, David, Maule, Quito, Porto Alegre e Lua Multimedia: 10 programas de TV para exibição nos sócios e 1 programa de TV com 1 hora de duração*
> *Todos os sócios são encarregados de desenvolver 10 vídeos com enfoque local e 10 com enfoque nacional, um CiberEspaço e conteúdo para alimentar o CiberWeb.*

Este projeto utilizou os seguintes meio para a aplicação: espaços de referência, programas de televisão e a *Web.* Inicialmente, os envolvidos seriam beneficiados com a conscientização da importância da utilização do Ciberespaço. Outra metodologia seria a aplicação da *"Ciber TV"*, por meio da apresentação de

[175] COORDENADORIA DO GOVERNO ELETRÔNICO., 2005, op. cit.

dez programas de televisão com conteúdos que divulguem as oportunidades oferecidas pela sociedade do conhecimento.

Estes programas compreendem temas que envolvem aspectos como despertar o interesse pela sociedade do conhecimento, criar e aprimorar a cultura de inclusão digital, bem como visa ampliar o impacto das campanhas de divulgação digital.

4.5.3
Paraná Digital

O programa Paraná Digital, busca a inclusão digital, voltada ao Estado do Paraná. É um projeto desenvolvido pela Federação das Associações Comerciais e Empresariais do Paraná (FACIAP), porém sua área de atuação não se limitou a algumas comunidades, mas sim, aos vários setores. Este programa expandiu e contou com a colaboração do governo do Paraná. Inicialmente contou com parceiros como o Banco do Brasil, Sebrae, Intel, Microsoft e DtCom.

Os primeiros beneficiados, em janeiro de 2003, foram os comerciantes paranaenses, por meio de um programa de informatização empresarial. Esse projeto possibilitou a aquisição de computadores pagando em parcelas com juros mais baixos do que os disponíveis no mercado, os equipamentos proporcionarão acesso à Internet e a softwares de gestão empresarial. Este projeto voltado ao comércio tem a previsão da comercialização de 53 mil computadores e 6 mil servidores. O primeiro passo foi a informatização das associações comerciais ligadas a FACIAP, pois das 282 existentes apenas 135 estão tecnologicamente preparadas. Atenta-se para que, em janeiro de 2003, a realidade era que, de 400 mil empresas do Estado, quase metade não tinha computador, e entre as que tinham, apenas, 30% apresentam conexão à Internet[176].

[176] REVISTA AMANHÃ. Disponível em <http://amanha.terra.com.br/notas_quentes/notas_index.asp?cod=591>. Acesso em 18 mar. 2003.

No final do ano de 2004 e início de 2005 o Governo do Estado do Paraná firmou um convênio com a Copel criando a inclusão digital de alunos e professores de escolas públicas para acessar a Internet com alta velocidade. Para a concretização deste projeto envolvendo 2.100 escolas estaduais [177], será utilizada a rede de fibra ótica implantada pela Copel. Na verdade, a utilização desta rede foi apresentada há 2 anos e hoje está sendo consolidada por meio do programa Paraná Digital. O projeto é composto por um quadro de parcerias, da Secretaria da Educação, da Copel, com a participação da Celepar.

A busca pela integração de todas as escolas públicas do Paraná à Internet, possibilita maior inclusão digital e cria possibilidades de atuar de maneira tecnologicamente moderna. As escolas terão acesso com velocidade dez vezes maior que a Internet turbo. A área de alcance do Projeto será determinada pela disponibilidade da rede de fibras ópticas, que atualmente conta com 4.500 quilômetros instalados, dando cobertura a 146 cidades, sob uma concentração de 87% da população do Estado [178].

4.5.4
Governo Eletrônico

Não se pode negar que o Governo Eletrônico, também pode ser considerado um projeto de inclusão digital. Inicialmente, mais precisamente em 2000, foram lançadas bases visando à criação de uma sociedade digital, para isto foi criado o Grupo de Trabalho Interministerial, que, a princípio, buscava traçar as primeiras diretrizes e normas. Passo seguinte, formou-se um Grupo de Trabalho em Tecnologia da Informação, que apontou linhas de ação para direcionar seus

[177] CELEPAR - Disponível em : <http://celepar7cta.pr.gov.br/CELEPAR/SiteCel.nsf//b0de5906b9f72e8783256f950046c33a?Open>. Acesso em 06 fev. 2005.
[178] Ibid., 2005.

projetos. Dentre as sete linhas destacam-se três: a universalização de serviços, o governo ao alcance de todos e infra-estruturas avançadas.

A princípio foi proposta uma política de interação eletrônica entre a sociedade e o Governo, e ainda, foi implantado o Comitê Executivo de Governo Eletrônico (CEGE), com o compromisso de possibilitar a evolução e a informação aos cidadãos. Na realidade, o CEGE tem a responsabilidade de formular políticas, coordenar e articular ações de implantação, bem como determinar diretrizes, com base no Plano de Metas[179] do Governo estabelecido em 20/09/2000[180].

Nos anos seguintes o trabalho continuou, e, em 2003, mais precisamente em 29 de novembro, o Presidente da República criou oito Comitês Técnicos de Governo Eletrônico, cada um com objetivos pré-definidos: implementação do Software Livre; Inclusão Digital; Integração de Sistemas; Sistemas Legados e Licenças de Software; Gestão de Sítios e Serviços On-Line; Infra-Estrutura de Rede; Governo para Governo – G2G; Gestão de Conhecimentos e Informação Estratégica[181]. As linhas de ação determinadas pelo Poder Executivo, tem basicamente o objetivo de promover a universalização do acesso, a transparência em ações, a integração das redes e um desempenho significativo dos seus sistemas.

O Governo Eletrônico traz a compreensão de universalização dos serviços como proporcionar o acesso à Internet, sob várias formas, individual, coletiva, comunitária ou pública, visando propiciar a todos o contato com o governo, aumentando a participação dos cidadãos. Com isso, o governo está trabalhando na interação com o cidadão, a melhoria efetiva em sua gestão interna e a possibilidade de integrar parceiros e fornecedores.

Para a implementação e funcionamento adequado foram estabelecidas Diretrizes Gerais para o Governo Eletrônico, com o objetivo de estruturar as estratégias de intervenção, adotadas sob a forma de orientação para as ações, bem como para a gestão do conhecimento da Tecnologia da Informação no Governo Federal. Foram propostas como estratégias[182]:

---

[179] Também chamado de Política de Governo Eletrônico.
[180] GOVERNO ELETRÔNICO., 2005, op. cit.
[181] GOVERNO ELETRÔNICO., 2005, op. cit.
[182] GOVERNO ELETRÔNICO., 2005, op. cit.

1- A prioridade do Governo Eletrônico é a promoção da cidadania: fazendo referência aos direitos coletivos e a visão de cidadania, promovendo a participação e o controle social. Realiza a ligação entre os princípios da universalidade, da igualdade perante a lei e da eqüidade na oferta de serviços e informações.

2- A Inclusão Digital é indissociável do Governo Eletrônico: passou a ser o elemento central da política de Governo Eletrônico, com o objetivo de concretizar uma política universal. A inclusão digital é regida como direito de cidadania e a sua promoção é o foco das políticas públicas. Ainda estabelece

> *Entretanto, a articulação à política de governo eletrônico não pode levar a uma visão instrumental da inclusão digital. Esta deve ser vista como estratégia para construção e afirmação de novos direitos e consolidação de outros pela facilitação de acesso a eles. Não se trata, portanto, de contar com iniciativas de inclusão digital somente como recurso para ampliar a base de usuários (e, portanto, justificar os investimentos em governo eletrônico), nem reduzida a elemento de aumento da empregabilidade de indivíduos ou de formação de consumidores para novos tipos ou canais de distribuição de bens e serviços. Além disso, enquanto a inclusão digital concentra-se apenas em indivíduos, ela cria benefícios individuais mas não transforma as práticas políticas. Não é possível falar destas sem que se fale também da utilização da tecnologia da informação pelas organizações da sociedade civil em suas interações com os governos, o que evidencia o papel relevante da transformação dessas mesmas organizações pelo uso de recursos tecnológicos* [183].

Assim, a proposta de inclusão digital vem acompanhada da ampliação da utilização de tecnologias de informação alcançando os cidadãos brasileiros, por meio da facilitação e do alcance da universalização e da democratização do acesso aos serviços em ambientes públicos ou comunitários.

3- O Software Livre[184] é um recurso estratégico para a implementação do Governo Eletrônico: é tido como uma opção tecnológica. Propõe o desenvolvimento de soluções, programas e serviços, utilizando adequadamente

---

[183] GOVERNO ELETRÔNICO., 2005, op. cit.

[184] Já por Software Comercial é aquele que se encontra no comércio, sua utilização legal só é possível mediante a compra.

recursos e investimentos voltados à tecnologia da informação. A opção pela utilização do software livre baseia-se na facilidade de produção e circulação do conhecimento, proporcionando o alcance de novas tecnologias, propiciando sua aplicação em ambientes colaborativos, bem como, garantindo o direito ao acesso de serviços públicos, sem a utilização de plataformas específicas.

4 - A gestão do conhecimento é um instrumento estratégico de articulação e gestão das políticas públicas do Governo Eletrônico: é aplicada como *"um conjunto de processos sistematizados, articulados e intencionais, capazes de assegurar a habilidade de criar, coletar, organizar, transferir e compartilhar conhecimentos estratégicos que podem servir para a tomada de decisões, para a gestão de políticas públicas e para inclusão do cidadão como produtor de conhecimento coletivo*"[185].

5 - O Governo Eletrônico deve racionalizar o uso de recursos: com o objetivo de reduzir custos unitários e o uso de certos recursos, propõe a parceria na utilização de recursos entre órgãos públicos, podendo ser efetivado como, por exemplo, no compartilhamento de equipamentos e recursos humanos.

6- O Governo Eletrônico deve contar com um arcabouço integrado de políticas, sistemas, padrões e normas com a finalidade de apoiar e ampliar as implantações e projetos do Governo Eletrônico, evitando erros e lacunas.

7- Integração das ações de Governo Eletrônico com outros níveis de governo e outros poderes: trata-se da busca de unidade, excluindo atitudes isoladas, mas utilizando-se da integração de ações e informações. Ao Governo Federal cabe o papel de garantidor e promotor do conjunto de políticas, padrões e iniciativas, propiciando a integração das ações dos governos e dos poderes[186].

Visando o alcance dessas propostas ao cidadão, desenvolveram-se alguns sites na Internet, com a finalidade de proporcionar informações, atender às necessidades, melhorar a prestação de serviços, desenvolver sistemas informáticos, entre outros. Assim, possibilitam diferentes formas de relacionamento, tanto com o Governo, quanto com os cidadãos e empresas, por meio de variadas transações eletrônicas. O processo de inclusão digital, como ponto central, pode vir por meio da redução de custos, maior qualidade e presteza

[185] GOVERNO ELETRÔNICO., 2005, op. cit.
[186] GOVERNO ELETRÔNICO., 2005, op, cit.

na gestão de serviços públicos, na transparência e na facilitação do alcance de processos.

Porém para a realização destas metas são necessárias várias atitudes coletivas como a conscientização da possibilidade de informação como estratégia para a formação da base cultural e comportamental da sociedade do futuro e da nova gestão pública. Ainda há a necessidade de integração, cooperação, responsabilização, independência e respeito, aos cidadãos, aos sistemas, ao governo e às novas propostas.

O Governo Eletrônico vem sendo reconhecido como a real iniciativa de transformação, nas quais as informações passaram a ser um fator estratégico, Florência FERRES & Paula SANTOS (2004, p.XVIII-XIX) apropriadamente apontam cinco níveis de classificação evolutiva do Governo Eletrônico.

O primeiro nível é o **Institucional,** no qual o governo participa como promotor de conhecimento, serviços e informações aos cidadãos, por meio da utilização de tecnologia e comunicação, possibilitando o alcance de serviços. Destacam as autoras

> *Há a disseminação seletiva de informações ou o acesso a serviços para o cidadão como notícias, informações, publicações, download de documentos, formulários e links. Exemplos no Brasil de informações ao cidadão são sites que oferecem, por exemplo, o saldo do FGTS, as contribuições feitas no Pis/Pasep, a requisição de uma segunda via da carteira de identidade, do CPF e do título de eleitor. A maior parte dos governos eletrônicos pelo mundo se encontra nesse estágio. No Brasil, o governo federal e alguns Estados (por exemplo, São Paulo, Paraná e Minas Gerais) já estão em estágios de transacional ao colaborativo*[187].

O segundo nível é o **Transacional** referente aos serviços que proporcionam uma transação financeira (ou processo transacional), oferecidos pelo governo. As autoras anteriormente citadas destacam como exemplos do nível transacional

---

[187] FERRES, F.; SANTOS, P. **E-government. O governo eletrônico no Brasil**. São Paulo: Saraiva, 2004, p. XVIII.

> *A declaração do imposto de renda e seu pagamento eletrônico, assim como os pregões eletrônicos, pelos quais o governo faz suas aquisições materiais. No Brasil, portais de compras como ComprasNet (R$ 4 bilhões de reais, 4.000 compradores e 167 fornecedores), bem como a Bolsa Eletrônica de Compras do Estado de São Paulo.*

O terceiro nível é o **Colaborativo**, que tem como finalidade dar alcance pela Internet a todos os serviços prestados pelo Governo. No Brasil, destacam-se

> *O Projeto Interlegis, ou mesmo o acesso ao Infojus (Internet do Judiciário). Ambos os projetos ainda estão em construção, mas oferecem informações que permitem ao cidadão utilizar vários serviços compartilhados, como fazer uma procura em todos os cartórios do país por certidões negativas, fazer o pagamento eletrônico on-line dos impostos devidos e de imediato poder participar de pregões eletrônicos. Cada um desses passos é uma fase de integração com um sistema estruturador diferente e em organizações distintas. O governo eletrônico no Brasil encontra-se entre o transacional e o colaborativo*[188].

O quarto nível é a **Integração entre todos os níveis**, ou seja, é a interligação de todas as bases de dados governamentais, possibilitando transações e desenvolvimento legislativos, sendo aplicados de forma adequada e simultânea. Mas para sua concretização seria necessário

> *Ampliar e capilarizar a infra-estrutura de redes, prever uma nova geração de serviços genéricos de redes, conceber esquemas de difusão ativa de informações em regime de atacado de todas as atividades de governo, gerar*

[188] FERRES, F.; SANTOS, P., 2004, op. cit., p. XVIII.

> *padrões técnicos para aplicações governamentais. O governo eletrônico do Brasil ainda não possui esse nível de sofisticação*[189].

O quinto nível trata da **Personalização Total,** refletida no momento em que o cidadão participa diretamente, ou seja

> *Interage com o governo de forma customizada e personalizada. Para ter sucesso nesse nível é necessário integrar e otimizar as infra-estruturas de rede para as três esferas do governo, atribuir um endereço eletrônico autenticado a cada cidadão brasileiro habilitado, criando, assim, a figura de domicílio oficial eletrônico, criar um diretório eletrônico nacional para todas as informações do governo e implantar programas de capacitação em gestão estratégica de tecnologias*[190].

Neste momento o Governo estaria participando do cotidiano do cidadão, proporcionando informações de interesse especifico para a comunidade. O Governo procuraria e informaria cada cidadão de forma personalizada e individual, como, por exemplo, quando informaria a necessidade da renovação de alvarás para as empresas, a data do pagamento do IPVA, entre outras possibilidades.

Os projetos aqui apontados demonstraram vários pontos em comum como a busca por uma moderna infra-estrutura de tecnologia, de comunicação, de acesso à equipamentos e dispositivos; a implantação de novas formas de organização com a participação da sociedade; a inserção em redes dinâmicas proporcionando a informação, o conhecimento, a inovação, a produção e a comercialização; entre outros. Mas todos estes fatores identificados e estes projetos apresentados têm por objetivo maior, a inclusão digital visando a transposição de barreiras técnicas, culturais e sociais.

---

[189] FERRES, F.; SANTOS, P., 2004, op. cit., p. XIX.
[190] FERRES, F.; SANTOS, P., 2004, op. cit., p. XVIII.

4.6
Perspectivas futuras de aplicações da inclusão digital no Brasil

Face aos níveis de classificação (conforme item 4.5) e as necessidades de evolução, observa-se que a inclusão digital é um tema muito relevante. Com o interesse da melhoria e da busca de um maior campo de atuação, o Brasil está em constante reformulação com projetos que já vem sendo desenvolvido e com propostas a serem concretizadas.

Existem iniciativas dispersas, ou seja, variados projetos implantados ou em implantação, o governo federal propôs a união de todos, denominando-os como **Casa Brasil**[191]**.** Seu objetivo inicial é reunir num só *"local serviços de acesso à internet, governo eletrônico, cidadania, eventos culturais e até Internet banking para quem não tem acesso de casa ao mundo virtual. A Casa Brasil será um ambiente multimídia e multicultural"*[192]. Este projeto visa implantar mil unidades em 2005, visando o atendimento a quatro milhões de cidadãos.

Na realidade este projeto aproveitará os 3.200 TELECENTROS já em funcionamento nas grandes cidades, que disponibilizam o acesso à Internet, e que com o projeto **Casa Brasil** receberão uma gama maior de serviços públicos e privados. O **Casa Brasil**, além de aproveitar os TELECENTROS[193] existentes, buscará outros locais de atuação como: "*igrejas, sindicatos e associações de moradores*", tendo como meta atender todo o país, e não apenas as grandes cidades.

A idéia do projeto **Casa Brasil** é unificar as iniciativas de inclusão digital dos diferentes Ministérios, mas com o cuidado de preservar suas características. Num mesmo local, ter-se-ia um TELECENTRO voltado para difusão cultural, ensino à distância, cidadania digital e empreendedorismo[194].

---

[191] FORUM DINHEIRO., 2004, op. cit., p. 64.
[192] Ibid., p. 64.
[193] "*Nesses locais já existem 22 mil PCs conectados à rede que servem para atender 390 mil pessoa por dia".* FORUM DINHEIRO., 2004, op. cit., p. 65.
[194] Assim, parte das mil unidades planejadas para 2005 terão estúdios multimídia e auditórios.

Sobre este assunto tratou Paulo LUSTOSA (2004, p.284), Secretário Executivo do Ministério das Comunicações, em entrevista para a ISTOÉ Dinheiro quando apresentou a inclusão digital como prioridade do governo e as estratégias para enfrentar esta realidade

> *É um tema complexo e abrangente. Estamos diante de uma questão realmente nova, fruto da mudança de paradigmas tecnológicos que perpassem todos os setores produtivos e organizações sociais [..] Devemos considerar quatro pontos fundamentais. Em relação aos recursos físicos é necessário prover equipamentos e preços acessíveis para as camadas de baixa renda. Precisamos nos preocupar com a formação de mão-de-obra capaz de entender os desafios desse novo mundo. Também é nosso dever oferecer suporte para que as estruturas sociais subam nesta onda e, por último, definir com a sociedade uma estratégia de produção de conteúdos on-line em linguagem adequada para as classes mais pobres.*

Ainda no início do ano de 2005, mais uma atitude em busca da inclusão digital foi tomada pelo governo com a universalização do PC com Internet. O objetivo inicial é possibilitar o alcance dos equipamentos às pessoas de baixa renda e às pequenas empresas do país. O nome deste programa é **PC conectado**, nome escolhido em virtude da possibilidade de acesso à Internet disponibilizada nesses computadores.

Com referência a este projeto, José RAMOS (2005) em matéria para o *link.Estadão,* apresentou as metas a serem alcançadas

> *De acordo com informações do Ministério das Comunicações, o objetivo do programa é que famílias da classe C que tenham telefone fixo em casa possam comprar computadores por R$ 1.400,00. O governo pagará um subsídio de aproximadamente R$ 250,00, o que baixará o valor para R$ 1.150,00. O produto poderá ser comprado em 24 prestações e já virá com uma dezena de programas de software livre instalados. Pelo projeto, o comprador do PC Popular receberá um contrato que lhe permitirá utilizar a rede telefônica para navegar 15 horas mensais na Internet, pagando R$ 7,50 (R$ 5,00 mais taxas), por um prazo de dois anos. Embora o valor seja baixo, companhias telefônicas como a Telefônica, a Telemar e a Brasil Telecom*

estão inclinadas a oferecer esse pacote, numa estratégia de atrair clientes cujo poder aquisitivo tende a crescer no futuro.

Inicialmente, o Ministério das Comunicações está fazendo contatos com parceiros e providenciando a fixação dos detalhes técnicos, para então passar a credenciar as empresas interessadas em participar na fabricação do produto. O subsídio para a realização desse projeto já está disponível, porém deverá ser analisada a forma de repasse[195].

A princípio este projeto visa aumentar a inclusão digital de forma mais rápida, assim, levando a sociedade do conhecimento a um maior número de cidadãos, como indica Luiz GUSHKEN (2004, p.60) em entrevista, ao afirmar que *"é uma boa idéia. Há uma equipe dentro do governo estudando essa questão porque precisamos responder algumas questões, como a existência de uma capacidade de produção local, para atender essa demanda"*, ainda complementa que se deve observar *"a definição de valor adequado a ser cobrado para quem adquirir uma máquina com essas características. Essa equação esta sendo discutida"*.

Outra proposta ou projeto a ser desenvolvido é a criação do **Observatório Nacional de Inclusão Digital (ONID)**[196], apresentado no início de janeiro de 2005. Trata-se de uma das ações que fazem parte do Programa Brasileiro de Inclusão Digital. Inicialmente, realizou-se um levantamento de acontecimentos e projetos já realizados no Brasil. Esse levantamento foi realizado a partir do cadastro dos TELECENTROS já existente e em funcionamento, que mantém parceria com o Banco do Brasil.

O **ONID**, nesta fase inicial, é composto e conservado por iniciativas de inclusão digital das mais variadas esferas da sociedade, formando uma espécie de rede, envolvendo órgãos da Administração Pública, algumas entidades e os cidadãos brasileiros.

---

[195] RAMOS, J. Governo prepara universalização do PC com Internet. Disponível em: <http://www.link.estadao.com.br/index.cfm?id_conteudo=2529>. Acesso em 26 jan. 2005.
[196] GOVERNO ELETRÔNICO., 2005, op. cit.

Inicialmente, o **ONID** tem por escopo a troca de informações e o intercâmbio de experiências em projetos existentes. Nesse sentido, busca apoio na formação de parcerias entre instituições particulares e o Governo Federal, com a finalidade de realizar a implantação e a manutenção de um banco de dados com informações, documentos, e iniciativas a respeito de projetos e atividades que atendam a inclusão digital, possibilitando a consulta pública à todos os interessados.

Outro objetivo do **ONID** envolve a criação de uma forma válida e criteriosa de avaliação de projetos e iniciativas de inclusão digital, que permitirá no futuro estudos e compatibilizações com as necessidades e a realidade brasileira. Para a realização dos objetivos o ONID desenvolverá um sítio na Internet, possibilitando o cadastro dos TELECENTROS, por meio de uma senha[197].

Inseridas nestes projetos estão as pequenas e médias empresas, que também devem ser beneficiadas com o leque de políticas de apoio, por meio dos projetos de difusão de tecnologias e de capacitação como indica Renata Lèbre La ROVERE (1997, p.161)

> *A articulação entre empresas, associações patronais, comerciais e de classe, centros de ensino e pesquisa, instituições financeiras e órgãos de política que caracteriza um sistema de inovações varia de acordo com a região considerada, o que coloca limites a políticas baseadas em experiências de sucesso de outros países ou regiões. Nesse sentido, o conceito de redes de firmas pode se tornar um instrumento útil para a compreensão das especialidades locais.*

Assim, não basta apenas investir e incentivar cidadãos e empresas, deve-se promover a capacitação e a construção do conhecimento. Com isso, há a necessidade de realizarem-se mudanças baseadas nas novas tecnologias, com processos de geração, acesso, fluxo, disseminação e uso de informações e conhecimento, bem como, que regulem novas práticas e relações estabelecidas em torno das atividades tecnológicas.

---

[197] Além da avaliação busca-se também a facilitação na troca de informações e experiências.

E, sem dúvida, quanto maiores forem os conhecimentos tecnológicos, maiores serão as seguranças dadas nos negócios jurídicos, como a possibilidade de utilização da assinatura digital como meio de assegurar as relações virtuais.

A investigação sobre a inclusão digital permite avançar no sentido de aprofundar a temática sobre os procedimentos jurídicos necessários para beneficiar e proteger a população que usufrui e que poderá vir a utilizar os recursos eletrônicos. O amparo jurídico é fundamental nas transações via rede eletrônica, tanto nos contratos como nas múltiplas relações que envolvem a sociedade informatizada.

5
Considerações Finais

O advento da Sociedade do Conhecimento, no final do século XX, trouxe para a sociedade o grande encontro da Era Oral, da Era Escrita e da Era Digital. Dessas Eras, sem dúvida a que ocasionou maior impacto, é a Digital, que afeta todas as áreas do conhecimento, em especial, os ramos econômicos, sociais, jurídicos e de saúde. Todos os segmentos da sociedade estão sendo provocados no sentido de atualizarem, questionarem e adaptarem seus conhecimentos, suas atividades, seus conceitos e paradigmas. Como não poderia ser diferente o Direito também foi afetado diretamente pelo advento das novas tecnologias. O Direito, em parceria com a Informática tem buscado as melhores formas de criar um ambiente seguro para comunicações, relações jurídicas e tecnológicas.

As inovações tecnológicas trazem outro problema por não estarem sendo disponibilizadas para a população em geral. Este fato tem ocasionado movimentos em busca de políticas públicas de inclusão que criem possibilidade de acesso de maneira igualitária para todos os cidadãos.

A Informática, enquanto responsável por criações e novidades tecnológicas, mantém-se continuamente em desenvolvimento. Desde a criação dos computadores (década de 40), sua utilização vem se realizando de múltiplas maneiras, com diversas utilidades e com os mais variados objetivos. Inicialmente, os computadores tinham funções semelhantes às máquinas de calcular, mas com o desenvolvimento tecnológico, passou a ter cada vez maior potencial, sendo possível finalmente armazenar e trocar dados com segurança, bem como criar um meio próprio de comunicação, em especial, a Internet.

O poder tecnológico sempre foi cobiçado por muitos países, em especial, quanto ao domínio de meios de comunicação e de desenvolvimento. A criação da Internet contribuiu de maneira definitiva para mudança na realidade mundial, pois se tornou um sistema que torna possível a troca de dados ou arquivos de uma máquina à outra, em qualquer localidade, desde que conectadas à rede. Tal fato proporcionou a agilidade e rapidez no intercâmbio de informações nunca imaginadas pelos criadores dos primeiros computadores.

Porém, esta evolução não cessou apenas nas formas de trocar informações, mas alcançou a criação de novos meios para a realização de relações comerciais, econômicas, sociais, e ainda, nas mais variadas formas de negócios jurídicos. Junto às novidades, facilidades e rápidas mudanças, foram também identificados os aspectos negativos, em especial, os ocasionados pela geração de atividades que decorrem em função da insegurança no uso do sistema. Esta dificuldade instigou os estudiosos da Informática e do Direito no sentido de procurarem soluções, visando a transparência, segurança, confiança e certeza dos negócios jurídicos realizados por meios eletrônicos. Em se tratando da garantia de segurança dos negócios jurídicos, mais especialmente, os contratos eletrônicos, passou-se a utilizar um método milenar, denominado criptografia, que foi adaptado e desenvolvido para o ambiente digital, sob a forma de programas especializados, que continuam em constante evolução.

Ao tratar de criptografia, conhecida como a arte de cifrar ou codificar, tornando possível o conhecimento da mensagem apenas pelo possuidor do código de acesso, destaca-se que o método mesmo desenvolvido e adaptado à digitalização não perdeu suas raízes históricas. O primeiro método, conhecido como simétrico ou convencional, também foi utilizado na busca de atribuir segurança para informações. Seu funcionamento consiste em uma chave que tem por finalidade codificar certa informação ou mensagem, que será enviada a outra pessoa, este destinatário receberá esta chave para decifrar e possibilitar a leitura. Porém, este método não se mostrou suficientemente seguro, pois, se outra pessoa possuir a chave secreta poderá tomar conhecimento da mensagem. Detectada a insegurança do método simétrico, reconheceu-se a fragilidade da autenticidade de documentos enviados com a utilização desse método criptográfico.

Para suprir as deficiências do método simétrico foi desenvolvida a criptografia pelo método assimétrico. Este método consiste na encriptacão de um documento, pelo seu emissor, com a utilização de uma chave privada, sob esta forma (encriptada) é enviado ao destinatário que recebe e utiliza uma chave pública, que possibilita a leitura do documento, mas não a modificação de seu conteúdo. Assim, podem ser identificadas diferentes funções das chaves, sendo que a privada permite encriptar e modificar e a pública, apenas desencriptar (decodificar). A principal vantagem deste método é o controle do envio das

mensagens, uma vez que o emissor necessita apenas de uma chave (privada) para tornar seguro seu documento, e poder liberar a chave pública que proporciona apenas a leitura aos mais variados receptores.

Uma vez que a criação das chaves se dá por meio de programas e possui alto grau de complexidade, tem-se assegurado a impossibilidade de duplicação ou clonagem dessas chaves. É o método que, portanto, traz consigo a segurança quanto a autenticidade, pois promove a certeza da identidade do emissor da mensagem e a integridade dos dados transmitidos. Assim, ao analisar os métodos criptográficos, pode-se afirmar que o assimétrico é considerado o mais seguro. Entre suas mais diversas utilidades, a principal, em virtude da segurança, é sua aplicação nas chamadas assinaturas digitais.

A assinatura digital traz para o meio eletrônico conceitos básicos que têm sido aplicados por muitos anos em meios escritos (físicos). A assinatura digital contém as mesmas características das assinaturas manuscritas, pois propicia a identificação o autor do documento, este passa a assumir sua confecção, e garante que é o indivíduo, realmente, responsável pela firma aplicada no documento. Torna-se o meio garantidor da integridade do documento, pois se modificado torna inválida a assinatura e, ainda, carrega a possibilidade de gerar a autenticidade válida para assegurar a manifestação da vontade, que geram a segurança e a confiança desejada para a realização de negócios jurídicos. Para que a assinatura digital goze de confiabilidade é necessário que uma Autoridade Certificadora a endosse, essa informa e garante que determinada pessoa é possuidora de um par de chaves, gerando a identificação do emissor da chave pública por meio de um certificado.

A Autoridade Certificadora deve ser instituída por lei (MP 2.200/01), tem por função a concepção das chaves, a possibilidade de consulta dos certificados já emitidos, bem como, a divulgação de uma lista contendo os certificados que foram revogados. Estes aspectos positivos apresentados pela assinatura digital apontam seus reflexos ao âmbito jurídico, ao certificar e assegurar a autenticidade, a autoria e a integridade do documento no qual foi aplicado, tornando o negócio jurídico e a declaração de vontade seguros.

A relevância dada à utilização da assinatura digital, para o Direito, possibilitou a ocorrência de várias formas de negócios jurídicos eletrônicos, que

têm por finalidade negocial modificar, transmitir, extinguir e transferir direito. Assim, pode-se identificar a possibilidade de sua realização e efetivação em ambiente eletrônico, que utilizando a assinatura digital o tornará um documento eletrônico. Essa passa a ser um elemento garantidor da manifestação da vontade nos documentos eletrônicos, pela impossibilidade de modificação, violação ou acesso por outra pessoa que não seu emissor.

Ao se tratar de documentos, destacou-se que sua função primordial é a manutenção, sob qualquer forma, da segurança e confiança de um negócio jurídico. Mas, em se tratando de ambientes digitais e da evolução tecnológica, a idéia e o conceito da expressão documento tem que ser revista e aperfeiçoada. Assim, ao observar os documentos eletrônicos, esses têm as mesmas características que o documento em papel, como, por exemplo, a possibilidade de leitura e releitura, de armazenamento, de segurança e de cópia e de reprodução sem alteração do original. Isto é aplicado por meio da implantação da assinatura digital, gerando a validade, confiança e segurança, resultando no reconhecimento pelo meio jurídico, em especial na Internet.

Os contratos eletrônicos são os meios em que mais se utiliza a aplicação da assinatura digital. Podem ocorrer sob qualquer uma de suas formas de contratação: intersistêmica, interpessoal e interativa. Assim, pode-se definir contrato eletrônico como aqueles negócios jurídicos que utilizam o computador para sua formação e registro em meio digital. Traz os mesmos elementos exigidos dos contratos em meio físico, ou seja, a manifestação multilateral do objeto convencionado, a obediência ao acordo firmado, bem como outros aspectos como a lealdade, a honestidade, a boa-fé, a confiança. São características que se coadunam com princípios contratuais como o da boa-fé objetiva, da autonomia da vontade, da autonomia privada, da equivalência funcional, da função social do contrato e da aplicação das normas jurídicas existentes aos contratos eletrônicos.

Os avanços e entendimentos jurídicos sobre a validade dos contratos eletrônicos não vieram sozinhos. Não apenas a doutrina confirmou a assinatura digital como requisito de validade dos negócios jurídicos, que se fez acompanhar da legislação própria. Como no momento em que se reconheceu a Lei Modelo UNCITRAL que regulamenta o comércio eletrônico, indica a necessidade de identificação e aplicação de um método confiável, aponta a necessidade de

garantia da originalidade dos documentos que pode ser concretizada por meio da utilização da assinatura eletrônica e pela emissão do certificado da Autoridade Certificadora.

Apoiada na Lei UNCITRAL, foi proposto no Senado o Projeto de Lei 672/99, que no decorrer dos tempos foi acompanhado de outras propostas que foram apresentadas sob a forma de novos Projetos de Lei. Mas, em junho de 2001 tais projetos foram substituídos pela MP 2200, que instituiu a ICP –Brasil como a autoridade garantidora da autenticidade e da integridade de documentos eletrônicos, por meio da criptografia assimétrica, bem como, indicou as providências a serem realizadas, as obrigações e definições e passou a reconhecer a assinatura digital como meio de segurança e validade dos negócios jurídicos praticados em ambiente digital. Em complemento a essa foi aprovada a MP 2200-2 em agosto de 2001, que trouxe entre outras providências regras para o credenciamento das Autoridades Certificadoras. O reconhecimento da segurança devido à aplicação da assinatura digital pelas mais diversas formas legislativas e doutrinárias certificam e asseguram a relevância e a validade jurídica aos contratos eletrônicos.

Em paralelo ao desenvolvimento tecnológico e legislativo houve e, ainda há, a necessidade de se reconhecer outros avanços, como a mudança paradigmática na Ciência e suas influências na sociedade e em todas as áreas do conhecimento. Esta mudança pode ser representada pelo paradigma emergente ou da complexidade que propõe a superação da visão reducionista e equivocada da fragmentação dos fenômenos do universo em busca da visão da totalidade. A produção do conhecimento que atenda à visão do todo precisa considerar a formação para a resolução de problemas da realidade advindos das necessidades da comunidade local e global.

As mudanças paradigmáticas afetam a sociedade e o universo como um todo, e nessa caminhada começam a aparecer movimentos em defesa das classes menos favorecidas e das dificuldades de acesso a grande camada da população brasileira e mundial ao desenvolvimento tecnológico. É nesse sentido que se passa a alertar para a necessidade da inclusão social em busca de uma convivência mais pacífica, buscando como resultado a superação de conflitos e a diminuição de agressões à dignidade da pessoa humana e ao meio ambiente. Em

especial, alerta ao meio jurídico para a necessidade da formação de cidadãos aptos a acompanhar as inovações tecnológicas. Ao Direito, nesse contexto, cabe a aplicação de uma visão sistêmica e complexa de mundo e de sociedade, garantindo a observação de direitos fundamentais individuais e coletivos.

Diante desse panorama de grandes mudanças paradigmáticas e conceituais, a sociedade deixou de se satisfazer apenas com o conhecimento escrito, abstrato e distante da realidade, requerendo um desenvolvimento de habilidades e competências visando à solução de problemas tecnológicos, econômicos e sociais. Em virtude disso, surgiram os "excluídos digitais", ou seja, os que se encontram longe da realidade informática e informacional. Mesmo tendo um acesso indireto à tecnologia (bancos, empresas), isto não é suficiente para serem considerados conectados à rede de conhecimento via eletrônica.

Face ao paradigma da complexidade, a inclusão digital, segue o liâme de que as pessoas devem ter a possibilidade de conhecer novas realidades, criar e possibilitar o acesso a todos os seres humanos indiferente de ração, religião, sexo ou cor, em especial, a ter acesso aos seus direitos, visando o aumento da cidadania e da qualidade de vida. A inclusão digital, para o alcance destes resultados passa a englobar o acesso a novas tecnologias na área da informática, educação, comunicação, desenvolvendo uma cidadania democrática, empreendedora e capacitada.

O aceso à produção do conhecimento traz algumas dificuldades que devem ser superadas como: a linguagem específica, a distância, o material, a falta de recursos econômicos e de apoio social. Mas, na busca da superação destas problemáticas estão sendo desenvolvidos vários projetos que têm por objetivo a alfabetização digital, a utilização de programas e recursos tecnológicos e o desenvolvimento de capacidades e competências para atuar na Sociedade do Conhecimento. Assim, introduzindo os cidadãos em espaços existentes, tornando-os disponíveis, auxiliando-os na criação de novas frentes que possibilitem o alcance da justiça, da democracia, da igualdade e da paz. Engajados nesses processos e nos projetos estão vários agentes dos mais variados setores como o governo, os profissionais de diversas áreas de conhecimento, os usuários da rede digital e parceiros.

O Direito e a Informática precisam aliar-se para oferecer à população recursos e processos que oportunizem à sociedade o acesso ao desenvolvimento tecnológico, ao desenvolvimento de uma regulamentação, e com ênfase, a formação da consciência e da cidadania, da participação da população e da necessidade de criação de processo de inclusão. E, sem dúvidas, quanto maior for o desenvolvimento e a disseminação do conhecimento tecnológico entre a população, mais segurança será exigida da rede eletrônica e, com isso, maior será o aproveitamento dos métodos e equipamentos já existentes, tanto do acesso à tecnologia, como da assinatura digital e das possíveis criações de novas possibilidades jurídicas e sociais.

6
Referências Bibliográficas

1. ALBERTIN, L. A. **Comércio eletrônico**. São Paulo: Ed. Atlas, 1999.
2. ALMEIDA, A. A. L. C. A Internet e o direito. **Revista Consulex**, Brasília, n. 24, p. 52-53, dez. 1998, 1 v.
3. AMARAL, F. **Direito civil:** introdução. Rio de Janeiro: Renovar. 5 ed, 2003, 1 v.
4. ARRUDA JÚNIOR, I. Documentos eletrônicos, Autoridades Certificadoras e legislação aplicável. **Revista Consulex**, Brasília, ano V, nº 111, p. 52/53, 2001.
5. AZEVEDO, A. J. **Negócio Jurídico** - Existência, Validade e Eficácia. São Paulo: Saraiva, 2ª ed., 1986.
6. BARBAGALO, E. B. **Contratos eletrônicos**: contratos formados por meio de redes de computadores: peculiaridades jurídicas da formação do vínculo. São Paulo: Ed. Saraiva, 2001.
7. BARCELLOS, A. P. **A eficácia jurídica dos princípios constitucionais** – O princípio da dignidade da pessoa humana. Rio de Janeiro: Renovar, 2002.
8. BIEWAGEN, M. Y. **Novo Código Civil**: princípios e regras de interpretação dos contratos. São Paulo: Saraiva, 2003.
9. BRASIL, A. B. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=1782>. Acesso em 17 mar. 2004.
10. BRUNO, G.M. **As relações do "business to consumer" (b2c) no âmbito do " e-commerce**. Disponível em: <http://www.direitonaweb.adv.br/doutrina/dinfo/Gilberto_M_Bruno_(DINFO_0009).htm>. Acesso em 15 mai. 2003.
11. BUCHMANN, J.A. **Introdução a criptografia.** Rio de Janeiro**:** Berkeley Brasil, 2002.
12. CÂMARA DOS DEPUTADOS. Disponível em: <www.camara.gov.br/internet/integras/outras.asp>. Acesso em 18 mar. 2003.
13. CAPRA, F. **A teia da vida**. Uma nova compreensão cientifica dos sistemas vivos. São Paulo: Cultrix, 1996.
14. _____. **As conexões ocultas**. Ciência para uma vida sustentável. São Paulo: Cultrix, 2002.
15. CARDOSO, C. M. **A canção da inteireza**. Uma visão holística da educação. São Paulo: Summus, 1995.
16. CARNELUTTI, F. **A prova civil**. Campinas: Booskseller, 2002.
17. CARVALHO, R. B. **Internet: o direito na era virtual.** Luiz Eduardo Shoueri, org. Rio de Janeiro. Forense, 2001.
18. CASTELLS, M. **A sociedade em rede: a era da informação: economia, sociedade e cultura.** Trad. Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999, 1 v.
19. CASTRO, A. A. **O Documento Eletrônico e a Assinatura Digital. Uma visão geral**. Disponível em: <http://www.aldemario.adv.br/doceleassdig.htm>. Acesso em 27 jan. 2002.

20. CELEPAR - Disponível em <http://celepar7cta.pr.gov.br/CELEPAR/SiteCel.nsf/0/b0de5906b9f72e8783256f950046c33a?Open>. Acesso em 06 fev. 2005.
21. CERTSIGN CERTIFICADORA DIGITAL LTDA. **Críticas**. Disponível em: <http://www.certisign.com.br/imprensa_mix.html>. Acesso em 27 jan. 2002.
22. CERTISIGN Certificadora Digital Ltda. Disponível em: <http://www.certisign.com.br>. Acesso em 26 mar. 2004.
23. CHIOVENDA, G. **Instituições de Direito Processual** Civil. Trad. J. Guimarães Menegale. São Paulo: Saraiva, 1994, v. III.
24. COORDENADORIA DO GOVERNO ELETRÔNICO. Disponível em: <http://portal.prefeitura.sp.gov.br/cidadania/coordenadoria_governo_eletronico/internet_cidada/0001>. Acesso em 06 fev. 2005.
25. CORRÊA, G.T. **Aspectos jurídicos da Internet.** São Paulo: Saraiva, 2ª ed, 2002.
26. COSTA, M.; TAVARES, A. Comissão de Informática Jurídica da OAB de São Paulo. Disponível em: <http://www.cbeji.com.br/artigos/artmarcosaugusto05072001.htm>. Acesso em 27 jan. 2002.
27. **CRIPTOGRAFIA clássica**. Disponível em: <http://members.fortunecity.es/ criptografia/criptografiaclasica.html>. Acesso em 17 mar. 2004.
28. **CULTURA**. Disponível em: http://www.culturatura.com.br/termos/internet/1.htm. Acesso em 10 set 2005.
29. DE LUCCA, N. Títulos e contratos eletrônico: o advento da informática e seu impacto no mundo jurídico. In: DE LUCCA, N. ; SIMÃO FILHO, A. (coord.). **Direito e Internet – aspectos jurídicos relevantes**, 1ª reimp. Bauru: SP: Edipro, 2001, p. 274-281.
30. DEVEGILI, A.; SANTOS, A. S. S. Conceitos de criptografia e sua relação com o direito. In: KAMINSKI, Omar (coord.). **Internet legal: o direito na tecnologia da informação**. Curitiba: Juruá. 1 ed, 2ª tiragem. 2004, pp. 203-208.
31. DIAS, J. C. **O direito contratual no ambiente virtual**. Curitiba: Juruá, 1 ed, 2ª tiragem, 2002.
32. DIMENSTEIN, G. Fórum inclusão digital: tecnologia ao alcance de todas debate como a internet pode promover justiça social . In: FORUM DINHEIRO. O desfio na rede. Seminário Três Editorial. REVISTA: **ISTOÉ Dinheiro**. 8 de dezembro de 2004, nº 284, p. 56-57.
33. EFING, A. C. **Direito das relações contratuais**. Curitiba: Juruá, 2002.
34. **_____ . Direito das relações contratuais.** Curitiba: Juruá, 2005, 2 v.
35. ELIAS, P. S. O documento eletrônico, a criptografia e o Direito. In: KAMINSKI, O. (coord.). **Internet legal: o direito na tecnologia da informação**. Curitiba: Juruá. 1 ed, 2ª tiragem. 2004, pp. 47-50.
36. E-GOV. Disponível em:<http://www.e.gov.br/>. Acesso em 24 jul. 2003.
37. FERRES, F.; SANTOS, P. (org.). **E-government. O governo eletrônico no Brasi**l. São Paulo: Saraiva, 2004.
38. FIGUEIREDO, A. M. S. **Revisão de contrato**. Curitiba: Juruá, 2004.
39. FREIRE, P.; FREIRE, A. M.(org.). **Pedagogia dos sonhos possíveis**. São Paulo: UNESP, 2001.

40. FONTES, F. C.; COLARES, R. G.. **Assinatura digital**: Sua importância nos negócios eletrônicos. Disponível em: <http://conjur.uol.com.br/ view.cfm?id=12833&ad=c>. Acesso em 10 nov. 2002.
41. FORUM DINHEIRO. O desfio na rede. Seminário Três Editorial. REVISTA: **ISTOÉ Dinheiro**., nº 284, p. 55-70, 8 de dezembro de 2004.
42. FROOMKIN, M. **The essential role of trusted third parties in electronic commerce**. Oregon Law Review, Vol 75, 1996, p. 49-115.
43. GANDINI, J. A. D.; SALOMÃO D.P. S.; JACOB C. **A validade jurídica dos documentos digitais**. Disponível em: <http://www.mct.gov.br/legis/ Consultoria_Juridica/artigos/validade_juridica_docs_digitais.htm>. Acesso em 06 mar. 2004.
44. GLANZ, S. **Internet e contrato eletrônico**. Em Revista dos Tribunais n. 757.
São Paulo:Revista dos Tribunais, 1998.
45. GOVERNO ELETRÔNICO. Disponível em: <http://www.governoeletronico.gov.br/ governoeletronico/index.htm>. Acesso em 06 fev. 2005.
46. GRECO, M. A. **Internet e Direito**. São Paulo: Dialética, 2000.
47. GUSHIKEN, L. "Parcerias são fundamentais". In: FORUM DINHEIRO. O desfio na rede. Seminário Três Editorial. REVISTA: **ISTOÉ Dinheiro**. 8 de dezembro de 2004, nº 284, p. 58-60.
48. ICP-BRASIL**.** Disponível em: <http://www.icpbrasil.gov.br/Portaria_1.htm>. Acesso em 20 abr. 2003.
49. IDBRASIL. Disponível em: <http://www.idbrasil.gov.br/docs_telecentro/ docs_telecentro/o_que_e>. Acesso em 06 fev. 2005.
50. INTERNETLEGAL. **Compêndio da Legislação Brasileira sobre informática, Internet, telecomunicações e conexos.** Disponível em: <http://www.internetlegal.com.br/legis/>. Acesso em 12 set. 2003.
51. IPB BRASIL. **Projeto de Lei cria atividade cartorial eletrônica.** Disponível em: <http://www.ibpbrasil.com.br/news/inf04.htm>. Acesso em 26 mar. 2004.
52. ISAGUIRRE, K. R. **Internet: Responsabilidade das empresas que desenvolvem os sites para web-com.** Curitiba: Juruá, 2002.
53. KAMINSKI, O. (coord.). **Internet legal: o direito na tecnologia da informação**. Curiitba: Juruá. 1 ed, 2ª tiragem. 2004.
54. KHUN, T. **As estruturas das relações científicas**. 4 ed. São Paulo: Perspectiva, 1996.
55. LAQUEY, T.; RYER, J. C. **O manual da Internet**: **um guia introdutório para acesso às redes globais.** Rio de Janeiro: Campus, 1994.
56. LASTRES, Helena M. M.; ALBAGLI, Sarita (org.). **Informação e globalização na era do conhecimento**. Rio de Janeiro: Campus, 1999.
57. LAWAND, J. J. **Teoria geral dos contratos eletrônicos.** São Paulo: Ed. Juarez de Oliveira, 2003.
58. LEAL, S.R.C.S. Validade jurídica dos contratos eletrônicos via Internet. Curitiba: **Dissertação de Mestrado**, PUC/PR, 2003.
59. LÉVY, P. **Cibercultura**. Trad: Carlos Irineu Costa. São Paulo: Ed. 34, 1999.
60. LOPEZ, M. J. L. **Criptografia y Seguridade em Computadores**. Disponível em: <http://www.kriptopolis.com>. Acesso em 03 ago. 2003.

61. LORENZONI, A.P. Aspectos relevantes sobre os documentos eletrônicos. In: EFING, A. C. **Direito das relações contratuais.** Curitiba: Juruá, 2005, 2 v., p.139-150.
62. LOZZI, F. Sottoscrizione e documento elettronico: um problema che richiede algiurista uma mentalitá nuova (não paginado). Apud. ZOCCOLI, D. Autenticidade e integridade dos documentos eletrônicos: a firma eletrônica. In: ROVER, A.J. (org.). **Direito, Sociedade e Informática: limites e perspectivas da vida digital**. Florianópolis: Fundação Boiteux. 2000, p.178.
63. LUCCA, N.; SIMÃO FILHO, A. **Direito e Intemet Aspectos Jurídicos Relevantes**. São Paulo: Edipro, 2000.
64. LUNA FILHO, E. P. Internet no Brasil e o direito no ciberespaço. **Revista Forense**, Rio de Janeiro, n. 353, p. 437-445, jan./fev. 2001, 97 v.
65. LUSTOSA, P. Novo mundo In: FORUM DINHEIRO. O desfio na rede. Seminário Três Editorial. REVISTA: **ISTOÉ Dinheiro**., nº 284, p. 65, 8 de dezembro de 2004.
66. MARCACINI, A. T. R. **Direito e informática : Uma abordagem jurídica sobre criptografia**. Rio de Janeiro: Forense, 2002.
67. MARCACINI, A. T. R. **O documento eletrônico como meio de prova**. Disponível em: <www.advogado.com/internet/zip/tavares.htm>. Acesso em 03 ago. 2003.
68. MARCACINI, A. T. R., COSTA, M.; REZENDE, P.A.D. Segurança, Bits & Cia . **Jornal do Commercio** . Publicado em 13, 20, 27/02/03.Não paginado.
69. MARCACINI, A.T.R.; COSTA, M. Criptografia Assimétrica, Assinaturas digitais e a falácia da 'neutralidade tencológica'. IN: KAMINSKI, Omar (coord.). **Internet legal: o direito na tecnologia da informação**. Curiitba: Juruá. 1 ed, 2ª tiragem. 2004, pp. 65-70.
70. MARQUES, C. L. **Contratos no Código de Defesa do Consumidor**: o novo regime das relações contratuais. São Paulo: RT, 2 ed, 1995.
71. MARQUES, Jose Frederico. **Manual de processo civil**. Campinas: Bookseller, 1997, 2 v.
72. MARTINS, G. M. **Formação dos contratos eletrônicos de consumo via Internet.** Rio de Janeiro: Forense, 2003.
73. MARTINS, G. M. Contratos eletrônicos via internet: problemas relativos à sua formação e execução. São Paulo: **Revista dos Tribunais**, p.92-106, jun. 2000, 776 v.
74. MATTE, M. **Internet – Comércio eletrônico. Aplicabilidade do Código de Defesa do Consumidor nos contratos de e-commerce**. LTr: São Paulo, 2001.
75. MELO, M. A. M. F. A tecnologia, direito e a solidariedade. In: ROVER, Aires José (org.). **Direito, Sociedade e Informática: limites e perspectivas da vida digital**. Florianópolis: Fundação Boiteux. 2000, pp. 21-34.
76. MICROSOFT PRESS. **Dicionário de informática inglês-português e português-inglês/Microsotf Press.** Tradutor: Fernando B. Ximenes. Rio de Janeiro: Campus, 1993.
77. MORAES, M. C. **O paradigma educacional emergente**. Campinas: Papirus, 1997.
78. _____. **Pensamento eco-sistêmico**. Educação, aprendizagem e cidadania no século XXI. Rio de Janeiro: Vozes, 2004.

79. MORIN, E. **Os sete saberes necessários à educação do futuro**. São Paulo: Cortez, Brasília: UNESCO, 2000.
80. NALIN, P. **Do contrato: conceito pós-moderno em busca de sua formulação na perspectiva civil-constitucional.** Curitiba: Juruá, 2000.
81. NALIN, P (org.). **Contrato & Sociedade. Princípio de Direito Contratual**. Curitiba: Juruá, 2004.
82. OLIVEIRA, W. J. **Segurança da informação - técnicas e soluções.** Santa Catarina: Visual Books, 2001.
83. OPICE BLUM, R..; GONÇALVES, S.R.M. As assinaturas eletrônicas e o direito brasileiro. In: SILVA JUNIOR, R. L. e WAISBERG, I. (org.) **Comércio eletrônico**. São Paulo: RT, 2001, p. 295-382.
84. PAESANI, L. M. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil.** São Paulo. Atlas, 2000.
85. PAULA, L. A problemática da aplicação do princípio da autonomia privada nas relações contratuais contemporâneas. In: NALIN, P (org.). **Contrato & Sociedade. Princípio de Direito Contratual**. Curitiba: Juruá, 2004, p.82-93.
86. PEREIRA, C.M.S. **Instituições de Direito Civil.** Introdução ao Direito Civil. Teoria Geral de Direito Civil. 20ª ed., Rio de Janeiro: Forense, 2004, 1 v.
87. PREFEITURA DE SÃO PAULO. Disponível em: <http://portal.prefeitura.sp.gov.br/cidadania/coordenadoria_governo_eletronico/pid/0001>. Acesso em 06 fev. 2005.
88. RAMOS, J. **Governo prepara universalização do PC com Internet**. Disponível em: <http://www.link.estadao.com.br/index.cfm?id_conteudo=2529>. Acesso em 26 jan. 2005.
89. **REVISTA AMANHÃ**. Disponível em: <http://amanha.terra.com.br/ notas_quentes/ notas_index.asp?cod=591>. Acesso em 18 mar. 2003.
90. REZENDE, P. A. D. **Entidades Certificadoras, Assinaturas Eletrônicas e Projetos de Lei.** Disponível em : <http://www.cic.unb.br/docentes/pedro/trabs/debate_oab1.htm>. Acesso em 26 mar. 2004
91. _____. **Relatório sobre o tema "Privacidade e Responsabilidades na Infra-estrutura de Chaves Públicas ICP-BR".** I Fórum sobre Segurança, Privacidade e Certificação Digital - ITI -Casa Civil da Presidência da República. Disponível em: <http://www.cic.unb.br/docentes/pedro/segdadtop.htm>. Acesso em 26 mar. 2004.
92. ROVER, A. J. (org.). **Direito, Sociedade e Informática: limites e perspectivas da vida digital**. Florianópolis: Fundação Boiteux. 2000.
93. ROVERE, R. L.. As pequenas e médias empresas na economia do conhecimento. In: LASTRES, H. M. M.; ALBAGLI, S. (org.). **Informação e globalização na era do conhecimento**. Rio de Janeiro: Campus, 1999, p. 145-163.
94. SANTOS, A. O. **Procurando o rumo.** Rio de Janeiro: CNC, 2002.
95. SANTOS, B. S. **A crítica da razão indolente.** Contra o desperdício da experiência. Para um novo senso comum: a ciência, o direito e a política na transição paradigmática. São Paulo: Cortez, 2000, 1 v.

96. SANTOS, M. A. **Primeiras linhas de direito processual civil**. 18. ed. São Paulo: Saraiva, 1997, 2 v.
97. SANTOS, M.J.P. Contratos eletrônicos. In: ROVER, A. J. (org.). **Direito, Sociedade e Informática: limites e perspectivas da vida digital**. Florianópolis: Fundação Boiteux. 2000.
98. SANTOS, M. J. P. & ROSSI, M D. Aspectos legais do comércio eletrônico – contratos de adesão. **Revista de Direito do Consumidor**, São Paulo, ano 09, nº 36, pp. 105-109, out.-dez. 2000.
99. SCHAEFFER, F. Princípio da confiança e procediemntos medicos realizados à distância. In: NALIN, P (org.). **Contrato & Sociedade. Princípio de Direito Contratual**. Curitiba: Juruá, 2004, 1 v., p. 39-61.
100. SILVA, M. A. 2005. **Títulos e documentos: Eficácia probante em face da revolução informática**. Disponível em: <http://www.cbeji.com.br/artigos/ artmarcussilva28102001.htm >. Acesso em 06 fev. 2005.
101. SILVA JÚNIOR, R. L. & WAISBERG, I. (Org.) **Comércio eletrônico**. São Paulo: Ed. Revista dos Tribunais, 2001.
102. SILVEIRA, S. A. & CASSIANO, J. (orgs.). **Software livre e inclusão digital.** São Paulo: Conrad, 2003.
103. SILVEIRA, S. A. **Exclusão Digital**: A miséria na era da informação. São Paulo: Fundação Perseu Abramo. 2001.
104. SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. Disponível em: <http://www.sbc.org.br/novidades/cartaab.htm>. Acesso em 10 set 2005STUBER, W. D. & FRANCO, A. C. P. A Internet sob a ótica jurídica. **Revista dos Tribunais**, São Paulo, ano 87, mar.1998, 749 v, pp. 60-81.
105. THEODORO JUNIOR, H. **Curso de direito processual civil.** 35 ed. São Paulo: Saraiva, 2001, 1 v.
106. TORQUATO, C. **Por uma política nacional de tecnologia da informação e comércio eletrônico**. In: Revista B2B MAGAZINE. Ano 2, nº23, Out, 2002, p.70.
107. ULHOA COELHO, F. **Curso de Direito Civil**. São Paulo: Saraiva, 2003, 1 v.
108. VOLPI, M. M. **Assinatura digital: aspectos técnicos, práticos e legais.** Rio de Janeiro: Axcel Books , 2001.
109. VOLPI NETO, A. **Comércio eletrônico: direito e segurança.** Curitiba: Juruá, 2002.
110. ZOCCOLI, D. Autenticidade e integridade dos documentos eletrônicos: a firma eletrônica. In: ROVER. Aires José (org.). **Direito, Sociedade e Informática: limites e perspectivas da vida digital**. Florianópolis: Fundação Boiteux. 2000, pp. 177-192.