

**O DIREITO ELETRÔNICO NO BRASIL.  
Os instrumentos que conferem validade e  
segurança aos contratos formados  
digitalmente: chaves de segurança pública,  
assinatura digital e a criptografia.**

Luciana Ferreira de Mello<sup>1</sup>

*“O direito não é mero pensamento, mas sim força viva.”<sup>2</sup>*

Rudolf Von Ihering

**RESUMO:** O objetivo do presente estudo é analisar as relações travadas digitalmente, bem como apresentar os instrumentos cuja finalidade é conferir validade e segurança aos contratos e relações travadas digitalmente. Serão analisados três dos principais instrumentos que, atualmente, conferem segurança aos documentos digitais: a chave de segurança pública, a assinatura digital e a criptografia.

**PALAVRAS CHAVE:** Direito eletrônico, regulamentação, criptografia, segurança pública, assinatura digital.

---

<sup>1</sup> UNIBRASIL. E-mail: luciana\_mello84@hotmail.com

<sup>2</sup> IHERING, Rudolf Von. **A luta pelo direito**. 6. ed. São Paulo: Revista dos Tribunais, 2010, p. 35.

**SUMÁRIO:** Introdução; 1. Relato histórico sobre o direito digital no Brasil 2. Documento eletrônico digital e sua regulamentação; 3. Criptografia 4. Assinatura digital; Conclusão; Referências.

## INTRODUÇÃO

No fim do século XX e início do século XXI, houve um forte e crescente desenvolvimento das tecnologias digitais no mundo globalizado, sendo que a sociedade mundial já não mais consegue se imaginar no presente, desvinculada de sua utilização cotidiana. O uso de ferramentas tecnológicas na vida do cidadão comum tornou-se algo primordial, uma vez que a utilização otimiza as relações jurídicas.

A tecnologia digital acabou com a necessidade de despendar tempo em filas para realizar transações bancárias, como pagamentos, transferências, empréstimos, e demais contratações financeiras. Ainda, o comércio eletrônico atualmente é o responsável por grande parte das vendas, principalmente no setor de equipamentos eletrônicos e informática, pois sua comodidade convida os usuários para contratar virtualmente, além da confiança em que os mesmos depositam nas lojas virtuais.

Vale ressaltar o grande número de sites de compras coletivas que surgiram na presente década, o que fato ocasionou um verdadeiro chamariz para realização de compras pela internet, aumentando cada vez a confiança dos usuários nos serviços utilizados.

Certamente não se pode ignorar o fato de que a evolução e aumento do uso da internet para inúmeras práticas comuns do cotidiano facilita a vida de grande parte dos usuários, porém, em contrapartida, também se depara com o crescimento de fraudes por meio da utilização da rede mundial de computadores, o que

ocasiona o investimento das empresas em sistemas de segurança digitais.

Também no âmbito jurídico importante mencionar a informatização do processo virtual, o que de fato vem sendo implantando em nosso país, e em menos de dez anos de utilização, pode-se perceber o grande passo dado em favor da celeridade processual, facilitação de acesso aos autos do processo em qualquer lugar que tenha acesso à internet, além da economia de papel, tinta, entre outros.

É certo que as tecnologias cada vez mais vêm avançando em termos de programação, criação de novas ferramentas e elementos de proteção, valendo citar a criação de desenvolvimento da certificação digital e da firma eletrônica, que vem tratar da questão do documento eletrônico, sua validade, autenticidade e eficácia como meio probatório.

O presente estudo visa abordar o histórico da utilização dos meios digitais no Brasil, bem como o desenvolvimento das ferramentas tecnológicas, em particular, o documento eletrônico e sua regulação, um breve estudo sobre segurança digital, abordando-se o tema criptografia, certificação digital e assinatura digital, demonstrando que o sistema adotado em nosso país baseou-se no modelo imposto pela Diretiva Européia n. 93/9993/99.

## **1. BREVE HISTÓRICO DO DIREITO DIGITAL NO BRASIL**

A internet não foi criada por interesse social, mas com objetivos estratégico-militares do Departamento de Defesa americano. A internet foi idealizada em 1969 como um sistema de comunicação de informações pela *Advanced Research Projects Agency*

(ARPA), que faz parte do Departamento de Defesa norte americano, sendo que os sites de pesquisa da *ARPA* passaram a compartilhar informação e dar acesso a computadores de qualquer lugar.<sup>3</sup>

Originalmente criada para servir como meio de comunicação nos tempos de crises nacionais e internacionais, além de apoiar pesquisas acadêmicas relativas á defesa nacional, foi crescendo e tornou-se uma rede verdadeiramente distribuída, sendo que protocolos de rede foram desenvolvidos para criar um ambiente de sistema aberto, permitindo rotear mensagens e informações por meio de plataformas de rede amplamente dispersas.<sup>4</sup>

No Brasil, nos últimos vinte anos, houve uma verdadeira revolução digital, em razão da utilização rotineira da navegação na internet, bem como da informatização de praticamente todos os setores da sociedade, em especial no campo das relações jurídicas, modificando e influenciando o cotidiano dos profissionais do direito, bem como da sociedade em geral.

O aumento do número de pessoas que, cada vez mais, passaram a aderir ao uso da internet também foi fundamental para a transformação e aprimoramentos dos sistemas e ferramentas digitais e tecnológicos. Contudo, cada vez mais se investe no meio digital como propagador da informação, meio de comunicação, contratação de bens ou serviços, entre outros, objetivando a otimização das atividades inerentes à sociedade. O conhecimento e a informação podem ser difundidos á distância, sem a necessidade da presença física do usuário.

No âmbito jurídico, a implantação e utilização das ferramentas virtuais é fundamental e funcional, porém, obviamente

---

<sup>3</sup> ALBERTIN, Alberto Luiz. Comercio Eletrônico: modelos, aspectos e contribuições de sua aplicação. São Paulo:Atlas,2010. p. 28.

<sup>4</sup> Idem.

está em contínua adaptação às necessidades dos usuários e eficácia dos serviços postos a utilização.

Fala-se muito atualmente em segurança virtual, como princípio fundamental para a eficácia dos serviços utilizados, o que ocasionou o surgimento das certificações digitais. A certificação visa a conferir segurança e autenticidade aos atos realizados no ambiente virtual, o que está em constante adaptação e criação.

Não obstante, verifica-se que a era da informação está presenciando um processo de reestruturação global do modelo de desenvolvimento dominante, migrando do modelo industrial para um modelo informacional que concilia uma nova arquitetura tecnológica, econômica, política, organizacional e gestão coletiva. O termo sociedade da informação é a denominação mais usual para indicar o conjunto de impactos e conseqüências sociais das novas tecnologias da informação e comunicação.<sup>5</sup>

Toda essa transformação ocasionada pelos sistemas digitais e tecnológicos, de forma inequívoca também implicou em inúmeras conseqüências, sejam elas positivas quanto negativas. Cita-se que em nosso país, as relações jurídicas advindas da utilização da rede mundial de computadores, ainda não teve a atenção necessária para emergir do setor secundário em que está, uma vez que tais relações ainda estão atreladas aos demais ramos do direito tradicional.

Portanto, para Lobato Paiva, direito digital “é a ciência que estuda a utilização dos elementos físicos, eletrônicos, como o computador, no Direito; isto é, a ajuda que este uso presta ao desenvolvimento e aplicação do Direito. Em outras palavras, é o instrumento necessário à utilização da informática no Direito”.<sup>6</sup>

Todavia, o direito digital não se ocupa apenas ao estudo do uso dos aparatos tecnológicos como meio de auxiliar o direito,

---

<sup>5</sup> Ibidem, p. 25.

<sup>6</sup>PAIVA, Mario Antônio Lobato de. Primeiras Linhas em Direito Eletrônico. Disponível em: <http://jus.com.br/revista/texto/3575/primeiras-linhas-em-direito-eletronico> Acesso em: 07 de jan. de 2013..

mas ao contrário, estuda o conjunto de normas e aplicações, processos, relações jurídicas que surgem como consequência da aplicação e desenvolvimento da informática perante a sociedade informatizada.

A interatividade de uma sociedade conectada em tempo real deve ser levada em consideração para que o Direito Digital progrida a partir desta perspectiva de acesso e agilidade na comunicação. O Direito Digital é a evolução do próprio direito, não se tratando de uma nova área, mas sim de todas as áreas já existentes que passam a estudar questões tecnológicas. Portanto o “Direito Eletrônico é um ramo autônomo atípico da ciência jurídica que congrega as mais variadas normas e instituições jurídicas que almejam regulamentar as relações jurídicas estabelecidas no ambiente virtual.”<sup>7</sup>

O Direito Digital possui uma relação com diversos ramos do direito. Em relação ao Direito Constitucional, pode-se dizer que a relação concerne ao direito à privacidade, inviolabilidade, intimidade, em relação ao envio e recebimento de e-mails sem que haja violação do conteúdo por terceiros, direito à honra e imagem, entre outros.

Já em relação ao Direito Penal, pode-se afirmar que muitas condutas delituosas têm sido perpetradas por meio da utilização das ferramentas digitais, sendo que há necessidade de regulamentação específica para conter os ilícitos penais praticados contra usuários da rede.

Também é importante destacar a relação do Direito Digital com a propriedade intelectual. O conteúdo disponibilizado na internet não é de domínio público, sendo que existe uma proteção legal por meio da Lei de Direitos Autorais<sup>8</sup>, pois pela

---

<sup>7</sup> PAIVA, Mario Antônio Lobato de. Processo Virtual. Revista Jurídica Consulex, ano VII, nº 154, abr. 2003.

<sup>8</sup> LEI Nº 9.610, DE 19 DE FEVEREIRO DE 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências e posteriores alterações.

grande facilidade de acesso à informações, os usuários da internet se utilizavam indevidamente do conteúdo, tais como imagens, músicas, vídeos, textos, etc. As implicações jurídicas decorrem da facilidade de reprodução e utilização da propriedade intelectual que pode ser violada por um simples toque de comando por intermédio de um computador.

Não menos importante e que está em patamares elevados, é o Direito Civil e Direito do Consumo em relação ao Direito Digital. Em relação ao Direito Civil, a prática cotidiana de contratar perante a internet já se tornou algo fluente. De tais práticas tem se visto o crescimento de inadimplementos contratuais e práticas abusivas, sendo que não há qualquer lei específica para regular essas relações, pelo que tem se aplicado o Código Civil e Código de Defesa do Consumidor.

Sob essa ótica, existem várias questões que devem ser levantadas e estudadas, tais como a validade jurídica dos contratos formalizados pela internet, competência territorial para solução de controvérsias, eis que os contratos também são celebrados em sites de inúmeros países, como regular a propaganda dissipada pela rede, geralmente não solicitada e não autorizada, dentre outros problemas.

## **2. DOCUMENTO ELETRÔNICO OU DIGITAL E SUA REGULAMENTAÇÃO**

É importante destacar o conceito de documento, que segundo CARNELUTTI:

“ é uma coisa capaz de representar um fato. É o resultado de uma obra humana que tenha por objetivo a fixação ou retratação material de algum acontecimento. Contrapõe-se ao testemunho, que é o registro de fatos gravados apenas na memória do homem. Em sentido lato, documento compreende não apenas os escritos, mas toda e qualquer coisa que transmita diretamente um registro físico a respeito de algum fato, como os desenhos, as fotografia, as gravações sonoras, filmes cinematográficos, etc. Mas, em sentido estrito, quando se fala da prova documental, cuida-se especificamente dos documentos escritos, que são aqueles em que o fato vem registrado através da palavra escrita, em papel ou outro material adequado.”<sup>9</sup>

E ainda, nas palavras de PAMPLONA FILHO “documento é toda coisa capaz de representar um fato. Pode constituir prova documental se for apta a indicar diretamente este fato ou prova documentada, quando a representação do fato se dê de forma indireta.”<sup>10</sup>

Nosso ordenamento jurídico reconhece os negócios realizados no meio eletrônico, uma vez que a validade das declarações de vontade independem de forma especial, conforme preceitua o art. 107 do Código Civil brasileiro. Porém, há uma preocupação dos usuários quanto a autenticidade e validade dos documentos produzidos de forma eletrônica.

Nos termos do art. 104 do Código Civil, os documentos são instrumentos produzidos, hábeis a se comprovar fatos, atos e negócios jurídicos realizados, para o fim de se analisar os requisitos

---

<sup>9</sup> MARINONI, Luiz Guilherme, ARENHART, Sérgio Cruz. Comentários ao Código de Processo Civil. São Paulo: Revista dos Tribunais, v. 5., t. 2., 2000. p. 19.

<sup>10</sup> GAGLIANO, Pablo Stolze, PAMPLONA FILHO, Rodolfo. Novo Curso de Direito Civil. São Paulo: Saraiva, 2004. v. 1. p. 259-261.



de validade: agente capaz, objeto lícito, possível, determinado ou determinável, consentimento das partes e forma não proibida em lei.

Há uma forte ligação entre o papel e o documento, sendo que não necessariamente o documento seja representado por um papel, pois sua representação pode ocorrer através de imagens, sons, mídias eletrônicas, CD, DVD, significando a fixação do conhecimento ou da informação para posterior acesso e comprovação, independentemente do suporte utilizado.<sup>11</sup>

Existe uma estreita relação entre o papel e a noção de documento, virtualmente é diferente, pois o documento é uma seqüência de bits, intangível que pode ser infinitamente reproduzida. No mundo digital não há cópias, mas sim vias registradas em diferentes suportes.<sup>12</sup>

Com a edição da Medida Provisória nº 2.200-2, em 24 de agosto de 2001, que instituiu a Infra-Estrutura de Chaves Públicas Brasileira, o ICP-Brasil, foram abordadas questões sobre documento eletrônico, entre outros temas de relevante importância:

"O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem

---

<sup>11</sup> OTTONI, Márcia Benedicto. Certificação digital. In: BLUM, Renato M. S. Opice (COORD.). Manual de Direito Eletrônico e Internet. São Paulo:Lex Editora, 2006. p. 244-245.

<sup>12</sup> Idem.

certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR."<sup>13</sup>

A referida medida provisória foi pioneira para a regulamentação jurídica do documento eletrônico no Brasil, sendo que ainda significa seu principal fundamento. Posteriormente surgiram leis para implementar a utilização do processo eletrônico em todo país, nas competências da justiça estadual, federal, trabalhista, etc.

Ocorre que tempos antes da referida MP ser editada, uma parte dos Doutrinadores já havia sinalizado sobre a importância de se regulamentar a matéria:

"Hoje, no Brasil, é grande a necessidade de novas leis regulamentadoras das relações humanas que ocorrem em meio virtual. Como já tivemos a oportunidade de ver, não só na área da privacidade on-line, como em outros aspectos do comércio eletrônico, o Brasil ainda carece de uma legislação específica."<sup>14</sup>

O objetivo da Medida Provisória nº 2.200-2 foi trazer ao ordenamento jurídico brasileiro às necessidades atuais do comércio

---

<sup>13</sup> ROHRMANN, Carlos Alberto. Notas acerca do Direito à Privacidade na Internet: A perspectiva comparativa. Revista da Faculdade de Direito Milton Campos. Belo Horizonte, v. 9, 2002. p. 33.

<sup>14</sup> DINIZ, Davi Monteiro. Documentos Eletrônicos, Assinaturas Digitais: Da qualificação jurídica dos arquivos digitais como documentos. São Paulo: LT, 1999. p. 122.

nacional e internacional, principalmente no que concerne o uso da internet para a prática de atos comerciais. O que se questiona é se a referida MP seria eficaz e adequada para atingir os objetivos a que se propõe.

Importante se faz demonstrar a funcionalidade do documento eletrônico em nosso país, a partir da MP nº 2.200-2, conforme abaixo transcrito:

“A Medida Provisória 2200-2, de 24 de agosto de 2001, permite o uso da certificação digital como ‘forma de garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica.’ A MP também regulamenta os órgãos governamentais e empresas privadas que atuam na certificação. Para isso, foi criada a Infra-estrutura de Chaves Públicas (ICP-Brasil), que é composta por um autoridade gestora de políticas e pela cadeia de autoridades certificadoras, que são a autoridade raiz (AR), as certificadoras (AC) e as de registro (AR).

A autoridade certificadora raiz é o Instituto Nacional de Tecnologia da Informação (ITI), que é responsável pela fiscalização e pode aplicar sanções e penalidades em forma de lei. É também a Ar que emite, expede, distribui, revoga e gerencia os certificados de uma AC. As autoridades certificadoras, por sua vez, emitem os certificados para as autoridades de registro (AR), que fazem o atendimento ao público em geral. Na prática, quer dizer que tudo é gerenciado pelo ICP e, conseqüentemente, pelo governo federal.”

Conforme preceitua o art. 62 da Constituição Federal de 1988, ditames constitucionais, as medidas provisórias que não fossem convertidas em lei no prazo de sessenta dias seriam prorrogáveis por no máximo mais um período, de igual prazo, senão vejamos o seu conteúdo:

"Art. 62. Em caso de relevância e urgência, o Presidente da República poderá adotar medidas provisórias, com força de lei, devendo submetê-las de imediato ao Congresso Nacional.

(...)

§ 3º. As medidas provisórias, ressalvado o disposto nos §§ 11 e 12 perderão sua eficácia, desde a edição, se não forem convertidas em lei no prazo de sessenta dias, prorrogável, nos termos do § 7º, uma vez por igual período, devendo o Congresso Nacional disciplinar, por decreto legislativo, as relações jurídicas delas decorrentes."

A referida Medida Provisória ainda continua em vigor, tendo em vista que o referido dispositivo constitucional passou a valor somente em setembro de 2001, ou seja, posterior à edição da MP 2.200-2, em agosto de 2001.

Assim, destaca-se que alguns artigos de conteúdo relevante, entre eles o artigo 10, o qual se passa a transcrever:

"Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil."

Esse artigo é importante para se entender o conceito de documento eletrônico, porém, relevante mencionar que o referido

dispositivo já nasceu desatualizado, em virtude de mencionar o código de 1916, revogado em 2003.

Petrônio Calmon entende que “Peca a lei por não considerar o documento eletrônico como original”.<sup>15</sup> O que ocorre é que o § 1º do art. 11 não considera o documento eletrônico como original, muito embora o caput o considere. Pode-se concluir que o documento gerado eletronicamente ou digitalizado pode ser considerado original, bastando que seja assinado eletronicamente, cuja a garantia da autenticidade pode ser constatada por meio da assinatura digital.

Tanto os documentos eletrônicos privados, quanto os documentos eletrônicos públicos, somente produzirão efeitos a terceiros se forem assinados digitalmente por meio de certificado digital da ICP-Brasil, incluindo o certificado digital AC-OAB.

É certo que mesmo existindo todos esses meios de certificar segurança aos documentos digitais e digitalizados, não se está livre da ocorrência de fraudes. Na hipótese de se constatar a adulteração de um documento antes ou durante o processo de digitalização consiste em alterar o próprio documento em papel, ensejando fraude. Não obstante, também há a possibilidade de se adulterar um documento após a digitalização, fato este que mesmo não tendo constado expressamente no corpo da referida lei, não deixa de implicar na existência de fraude.

Resta incontroverso que existem vários tipos de softwares de edição de imagens como ferramentas hábeis a alterar e até mesmo construir documentos, o que de fato é muito difícil de se fiscalizar, porém, nada impede que se regulamente essas hipóteses, a fim de responsabilizar e punir.<sup>16</sup>

Também resta importante destacar os artigos 8º e § 2º do artigo 10º da MP, a valer:

---

<sup>15</sup> CALMON, Petrônio. Comentários à Lei de Informatização do Processo Judicial. Rio de Janeiro: Forense, 2007. p. 108.

<sup>16</sup> KRUEL, Eduardo. Processo Judicial Eletrônico & Certificação digital na advocacia. Brasília: OAB, 2009. p. 248-249.

"Art. 8º. Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado."

"Art. 10. (...)

§ 2º. O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento."

Tais dispositivos são de suma importância, uma vez que destacam quem poderá realizar a certificação eletrônica perante o consumidor.

A autoridade de certificação (*certification authority* – CA) é um agente, público ou privado, que procura atender à necessidade de serviços confiáveis de terceiros no CE, emitindo certificados digitais que atestam para o mesmo para o mesmo fato sobre o assunto de certificado.<sup>17</sup>

Um certificado é uma declaração digitalmente assinada por uma CA que provê confirmação independente de um atributo reivindicado por uma pessoa que oferece uma assinatura digital, ou seja, um certificado é um registro baseado em computador que:

1. Identifica a CA que o forneceu;
2. Nomeia, identifica ou descreve um atributo de um subscritor;
3. Contém a chave-pública do subscritor;

---

<sup>17</sup> ALBERTIN, Alberto Luiz. Op. cit., p. 213.

4. é assinado digitalmente pela CA que o forneceu.<sup>18</sup>

O papel da CA na identificação e autenticação é particularmente importante para transações que tenham efeitos que se estendem no tempo. Nas transações básicas de consumo, em que alguma coisa é trocada por dinheiro, pode não haver necessidade de certificados, um cartão de crédito seria suficiente.

A situação muda consideravelmente quando a transação tem um efeito limitado no tempo, ou seja, se as comunicações são parte de um relacionamento em desenvolvimento, as partes têm muito interesse em se identificar e autenticar umas para as outras.

Desse modo, pode-se concluir que o Brasil já possui os pressupostos necessários para a plena utilização do documento eletrônico e transações virtuais, vez que a MP 2.200-2, indicou o suporte legal para a certificação digital, baseadas em técnicas de criptografia, objetivando garantir autenticidade e integridade às transações e arquivos eletrônicos. Essa norma faculta, inclusive, a utilização de padrões internacionais de criptográfica, já testados e aprovados em outros países.<sup>19</sup>

### 3. CRIPTOGRAFIA

Cabe aqui fazer uma breve análise sobre o aspecto geral da criptográfica para se entender sobre a segurança e autenticidade no âmbito digital.

Os aspectos e as características da realidade global atual que vivemos explicam porque a criptografia precisa ser uma parte integral da infraestrutura global de informação (*global information*

---

<sup>18</sup> Idem.

<sup>19</sup> LUGCA, Newton de, SIMÃO FILHO, Adalberto (Coord.). Direito e Internet: Aspectos Jurídicos Relevantes. Bauru: Edipro, 2001. p. 240.

*infrastructure* – GII), que visa proteger a propriedade intelectual e os ativos financeiros, e para promover uma base confiável para o comércio eletrônico e demais transações e atividades profissionais realizadas por meio digital.

Alguns dos aspectos e características citadas são: informação, conectividade global, comércio eletrônico, competição, espionagem econômica, crime organizado global, armas químicas, biológicas e nucleares, terrorismo, conflitos, instabilidade econômica e social, violação de privacidade e direitos humanos, erosão e confiança, etc.<sup>20</sup>

A ausência de segurança de dados e mensagens na internet tem se tornado um problema em razão do crescente número de empresas que estão tentando colocar seus negócios na rede global. As principais ameaças de segurança podem ser divididas em três categorias distintas, quais são elas:

- a. **Confidencialidade.** Preservar os dados utilizados por arquivos governamentais, cartão de créditos, números de documentos pessoais, registros de empregados, dados profissionais, entre outros. A confidencialidade impede o acesso, ou a liberação, de tais informações para usuários não autorizados.
- b. **Integridade.** A informação recebida deve ter o mesmo conteúdo da informação enviada. Enquanto a confidencialidade visa proteger a monitoria passiva de dados, os mecanismos para integridade tem de prevenir ataques ativos envolvendo a modificação de dados.

---

<sup>20</sup> ALBERTIN, Alberto Luiz. Op. cit., p. 213-214.



C. Autenticação/identificação. É necessária a verificação da identidade de uma entidade (usuário ou serviço), utilizando certas informações criptografadas transferidas do emissor para o destinatário.<sup>21</sup>

As informações de dados viajam por meio de canais públicos, tais como a internet, e necessitam de proteção por meio da criptografia. A criptografia é a mutação de informação em qualquer forma: texto, vídeo ou gráficos, sendo ilegível para quem não possua a chave criptográfica.<sup>22</sup>

A origem da palavra criptografia vem das palavras *kryptós* e *grafos*, que significam *escondido* e *oculto*, e *grafia* e *escrita*, respectivamente. A criptografia é definida como:

“A arte ou a ciência de escrever em cifra ou em código, ou, ainda, como o conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que somente o destinatário a decifre e a compreenda. Os algoritmos de criptografia americanos são mundialmente reconhecidos como os mais seguros e fortes. Porém a legislação dos EUA restringe seu uso, inclusive não permitindo sua exportação. Considera-se que para quebrar um algoritmo dessa qualidade seria necessário empregar um volume de *hardware* bastante elevado e, assim mesmo, o processo levaria alguns anos para ter sucesso.”<sup>23</sup>

---

<sup>21</sup> Ibidem. p. 216-217.

<sup>22</sup> Idem.

<sup>23</sup> Idem.

Existem dois métodos de criptografia: 1. Criptografia com chave secreta (*secret-key*). Refere-se ao uso de uma chave compartilhada para a criptografia pelo transmissor e de decifração pelo destinatário. 2. Criptografia com chave pública (*public-key*). É uma forma mais forte de criptografia que envolve o uso de um par de chaves, sendo uma pública e outra privada. A chave privada, usada para criptografar a informação transmitida pelo usuário, é mantida secreta. Já a chave pública é utilizada para decifrar no destinatário e não é mantida secreta. Uma vez que somente o autor de uma mensagem criptografada tem conhecimento da chave privada, uma decifração com sucesso utilizando a chave pública correspondente verifica a identidade do autor e assegura a integridade da mensagem.<sup>24</sup>

Pode-se dizer que a criptografia é utilizada para conferir maior segurança e autenticidade para os documentos produzidos em meio digital, porém, como já dito, nada é a prova de fraudes. Nesse sentido, cada vez mais se investe em tecnologia para a elaboração de novos meios de segurança, a fim de agregar aos já existentes, objetivando aprimorar a segurança no ambiente virtual.

Eduardo Krueel citada dados obtidos pela *Price WaterHouse Coopers* do ano de 2004, em relação à ataques tecnológicos a sistemas na internet, concluiu-se que “53% ocorreram através de código malicioso (vírus), 29% *Denial of Service* e 25% de acesso não autorizado. Destes, 66% foram realizados por *Hackers* e 28% por empregados. As desastrosas conseqüências foram 50% das redes se tornaram indisponíveis, bem como 44% dos e-mails de demais aplicações, sendo que disso tudo 37% dos arquivos sem *backup* se perderam!”<sup>25</sup>

Diante disso, constata-se que enquanto se investe em segurança, em contrapartida os *hackers* também se aprimoram em invasão de sistemas, sendo totalmente necessário o constante

---

<sup>24</sup> Ibidem. p. 219-220.

<sup>25</sup> KRUEEL, Eduardo. Op. cit., p. 256.

investimento em segurança e demais meios para se evitar invasões a sistemas, bem como fraudes virtuais.

#### 4. ASSINATURA DIGITAL

Segundo Ottoni, “as assinaturas são distintivos únicos e exclusivos de uma pessoa que permitem identificar o autor do documento. Graças a esta natureza de exclusividade de cada indivíduo, a assinatura manuscrita aposta sobre o papel atesta a autoria do documento.”<sup>26</sup>

Desse modo, a criptografia com chave pública pode ser utilizada para a autenticação de emissor, conhecida como assinatura digital, o qual permite que a assinatura digital seja manejada para autenticar documentos eletrônicos da mesma forma que as assinaturas manuscritas são usadas para autenticar documentos de papel.

Importante destacar que a assinatura manuscrita atesta a integridade do documento, sendo que está associada ao referido documento. Qualquer tentativa de reutilização do papel destruirá o original, ou seja, a assinatura manual está atrelada ao suporte físico, sendo que não mais poderá ser utilizada, copiada ou reaproveitada em outro documento.

Em nosso ordenamento pátrio, a assinatura manual apostada no papel está atrelada à obrigação, atesta a ciência do subscritor sobre o fato, serve como meio legal de prova, a fim de se comprovar uma obrigação, sendo forçado a cumpri-la, em razão

---

<sup>26</sup> OTTONI, Márcia Benedicto. Op. cit., p. 245.

do ato pessoal de assinatura. A assinatura manual, também autentica o documento, atestando a vontade do signatário.

Para que a assinatura digital alcance a mesma validade e funcionalidade da assinatura manual, o ato de assinar eletronicamente deve representar ao subscritor o mesmo significado de lançar uma assinatura de próprio punho, devendo representar uma consciência sobre o ato e suas implicações jurídicas.

Há um consenso jurídico de que as leis não devem contemplar tecnologias específicas, vez que as tecnologias se desenvolvem, sendo alteradas e superadas de forma mais rápida do que são aprovadas e modificadas as leis. As normatizações deveriam permanecer em regulamentos, sendo mais fáceis de serem atualizadas e acompanhar os avanços tecnológicos.<sup>27</sup>

Por outro lado, vale dizer sobre o advogado como terceiro de boa fé no ato de assinar digitalmente os documentos eletrônicos, pois no caso de ocorrer a juntada de um arquivo editado ou fraudulento, a responsabilidade recai sobre quem assinou digitalmente o arquivo, considerando que, uma vez assinado digitalmente um documento, seja ele gerado eletronicamente ou digitalizado, o não repúdio é uma das características da certificação digital.

Assim, quem assina um documento digitalmente, está atestando a autenticidade do referido documento, ou seja, que ele confere ao original e não sofreu qualquer tipo de modificação ou alteração. Portanto, enseja a responsabilidade do signatário, devendo o advogado agir como terceiro de boa fé, uma vez que ao assinar o documento, traz para si toda a responsabilidade pela autenticação.

Portanto, por cautela, cabe ao advogado exigir um termo de declarações ou algo similar ao seu cliente, a fim de que o mesmo ateste que lhe está repassando documentos originais,

---

<sup>27</sup>Ibidem. p. 248

autênticos, idôneos e íntegros, sem qualquer tipo de fraude, pois o risco do advogado que assinar digitalmente um documento falso é demasiadamente sério.<sup>28</sup>

Assim, a utilização da criptografia, como recurso matemático para identificação de usuários de meios eletrônicos, com a concessão de pares de chaves criptográficas associadas a pessoas, com a emissão de certificados digitais, vem sendo adotada legalmente em inúmeros países, tanto na União Européia como nas Américas.

Em relação ao direito comparado com o modelo Europeu, Ottoni menciona que

“ [...] a regulamentação brasileira adotou a nomenclatura da indústria americana de PKI baseada em criptografia assimétrica, utilizando termos como Autoridade Certificadora (AC) e Autoridade de Registro (AR), ao contrário do exemplo da Diretiva que, ao apresentar-se como lei tecnicamente, neutra substitui a utilização de termos como chave de assinatura por dados e dispositivos de geração de assinaturas de forma a descaracterizar que seja, legalizada de uma tecnologia específica, a assinatura pela técnica da criptografia assimétrica, do conceito de assinatura eletrônica; e os nomes Autoridade Certificadora – Autoridade de Registro pelos termos prestadores de serviços de certificação de órgãos de registro, mais condizentes, segundo a nomenclatura jurídica, com a natureza privada e comercial da atividade prestada.”<sup>29</sup>

A referida Diretiva determina o uso desses termos em substituição à nomenclatura da indústria, ampliando o conceito de

---

<sup>28</sup> KRUEL, Eduardo. Op. cit., p. 249.

<sup>29</sup> OTTONI, Márcia Benedicto. Op. cit., p. 248

certificação digital. O sistema brasileiro é baseado no modelo europeu em relação ao conteúdo e função, em razão da inspiração na Diretiva Européia. Assim, para se entender o sistema que foi adotado em nosso país, deve-se entender a influência internacional, em particular, os moldes ditados pela Diretiva Européia.<sup>30</sup>

A Comissão de Comércio da ONU tratou de assuntos relacionados à assinatura eletrônica e as Autoridades Certificadoras (AC), ou Prestadores de Serviço de Certificação. Foi publicada a *Uncitrdital Model Law on Eletronic Signatures* em 2001, qual seja, a lei modelo que regulamenta os requisitos para que a assinatura eletrônica tenha seus efeitos equiparados à assinatura manuscrita, nos mesmos parâmetros dos ditames estabelecidos pela comunidade européia.

A Diretiva Européia 93/9993/99<sup>31</sup>, de forma distinta das leis modelos da ONU, que tem apenas a função de orientar a comunidade e os legisladores de cada país, mas não são de adoção obrigatória, tem poder regulatório na comunidade européia.<sup>32</sup> Os respectivos países membros da comunidade tem dever e prazos para implantar as orientações das diretivas em seus ordenamentos jurídicos pátrios.

Em relação à assinatura digital, a Diretiva 93/1999 determinou que alguns países da União Européia revisassem suas leis sobre a assinatura digital, a fim de adaptar o conteúdo que contradizia o disposto na diretiva. Nas palavras de Ottoni:

---

<sup>30</sup> Ibidem. p. 249.

<sup>31</sup> Diretiva 99/93/CE do Parlamento Europeu e do Conselho da União Européia- relativa a um quadro legal comunitário para as assinaturas eletrônicas (versão ONU em português).

<sup>32</sup> De acordo com os princípios da subsidiariedade e da proporcionalidade, tal como constam do artigo 5º do Tratado – Tratado que institui a Comunidade Européia, nomeadamente o nº 2 do artigo 47º e os artigos 55º e 95º, o objetivo da criação de um quadro legal harmonizado para a oferta de assinatura eletrônicas e serviços conexos não pode ser suficientemente realizado pelos Estados-membros e pode, pois, ser melhor alcançado pela Comunidade; as disposições da presente diretiva não excedem o necessário para atingir esse objetivo – item 28 da introdução à Diretiva.

“A Diretiva adotou um sistema tecnológico neutro, afastando menções às chaves criptográficas de assinatura que indicam a adoção da tecnologia da criptografia assimétrica, substituindo-as pelos conceitos genéricos de dados de assinatura e dispositivos de criação e verificação de assinaturas. As regulamentações da Diretiva e das leis nacionais de transposição, no entanto disciplinam apenas o uso da criptografia assimétrica que é, até agora, a única tecnologia conhecida capaz de prover os requisitos de PKI impostos pela Diretiva. A utilização de uma nomenclatura genérica, porém, permite que novas tecnologias sejam diretamente aproveitadas nos sistemas de infra-estruturas que vêm sendo implementados.”<sup>33</sup>

Desse modo, verifica-se que a Diretiva se baseia em modelo mais próximo ao sistema jurídico da *civil Law* do que ao sistema norte americano, da *common Law*, no qual há mais liberdade e valorização da autonomia contratual das partes, concedendo aos Estados poderes de intervenção na atividade de certificação digital e impondo deveres de fiscalização. Já o sistema adotado no Brasil se baseia na sistemática fixada na Diretiva.

## CONCLUSÃO

A evolução tecnológica fez surgir um novo ramo do Direito denominado Direito Digital ou Direito Eletrônico, que traduz a evolução do próprio direito, não se tratando de um ramo novo, mas sim de todas as áreas do direito que em seu particular, trazem relação com a tecnologia e o mundo digital.

O direito deve evoluir para acompanhar o desenvolvimento tecnológico que caminha em contínuo

---

<sup>33</sup> OTTONI, Márcia Benedicto. Op. cit., p. 250.

crescimento, devendo trazer em seu bojo a regulamentação de inúmeras questões legais atreladas ao uso da internet e da mudança comportamental da sociedade digital.

Infelizmente, no Brasil as leis ainda continuam muito ultrapassadas no que diz respeito às questões digitais, sendo certo que merece uma melhor atenção por parte dos legisladores nesse tocante, com a regulamentação da lei do comércio eletrônico, entre outros, sendo que recentemente foi modificado o Código Penal, a fim de inserir alguns tipos penais ligados a crimes praticados pela rede mundial de computadores.

De certo que devemos estar cientes de que as tecnologias estão em constante avanço e desenvolvimento, sendo certo que o Direito não consegue acompanhá-lo na mesma velocidade, porém, deve-se ao menos, regular as questões básicas que encontramos em discussão em nossa sociedade digital.

Não se pode ignorar o avanço quando a regulamentação dos documentos eletrônicos da certificação digital e firma digital, por meio da MP 2.200, sendo certo que tais recursos estão em constante aperfeiçoamento.

Especificamente no que se refere aos meios que visam conferir segurança aos instrumentos contratuais firmados digitalmente, apontam-se as chaves de segurança pública, a criptografia e a assinatura digital.

A regulamentação da eficácia e do valor legal dos documentos e transações eletrônicas, a infra estrutura de Chaves Públicas Brasileiras (ICP-Brasil), instituída pela MP 2.200, ampliou os objetivos que inicialmente se restringiam apenas ao âmbito da administração pública federal.

A ICP-Brasil apresenta grande influência do sistema europeu, mas utilizam termos da indústria da tecnologia americana, como Autoridade Certificadora (AC) e Autoridade de Registro (AR), nomenclaturas estas que não são utilizadas na regulamentação européia.



Estamos num processo de evolução e aprimoramento, sendo que o foco é a segurança, tanto no que diz respeito à utilização da internet, quanto à proteção legal das relações jurídicas virtuais, visando maior segurança do usuário, tanto no que diz à propriedade intelectual, direito contratual, consumidor, penal, trabalhista, tributário, entre tantos outros ramos do direito que cotidianamente envolvem as relações legais que ocorrem por meio da rede mundial de computadores.

Como já dito anteriormente, sabe-se que os meios que visam a conferir segurança aos instrumentos contratuais firmados digitalmente são idôneos, no entanto, tendo em vista a constante evolução dos meios digitais ainda inspiram cuidados em razão de sua vulnerabilidade. Todavia, tais meios apresentam grande avanço para o processo de regulamentação e instrumentalização dos meios digitais a que lançamos mão diariamente e que tanto facilitam a vida privada e a laboral.

## REFERÊNCIAS

ALBERTIN, Alberto Luiz. *Comercio Eletrônico: modelos, aspectos e contribuições de sua aplicação*. São Paulo:Atlas, 2010.

CALMON, Petrônio. *Comentários à Lei de Informatização do Processo Judicial*. Rio de Janeiro: Forense, 2007.

DINIZ, Davi Monteiro. *Documentos Eletrônicos, Assinaturas Digitais: Da qualificação jurídica dos arquivos digitais como documentos*. São Paulo: LT, 1999.

Diretiva 99/93/CE do Parlamento Europeu e do Conselho da União Europeia- relativa a um quadro legal comunitário para as assinaturas eletrônicas (versão ONU em português).

GAGLIANO, Pablo Stolze, PAMPLONA FILHO, Rodolfo. *Novo Curso de Direito Civil*. São Paulo: Saraiva, 2004. v. 1.

KRUEL, Eduardo. *Processo Judicial Eletrônico & Certificação digital na advocacia*. Brasília: OAB, 2009.

LEI Nº 9.610, DE 19 DE FEVEREIRO DE 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências e posteriores alterações.

LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coord.). *Direito e Internet: Aspectos Jurídicos Relevantes*. Bauru: Edipro, 2001.

MARINONI, Luiz Guilherme, ARENHART, Sérgio Cruz. *Comentários ao Código de Processo Civil*. São Paulo: Revista dos Tribunais, v. 5., t. 2., 2000.

OTTONI, Márcia Benedicto. *Certificação digital*. In: BLUM, Renato M. S. Opice (COORD.). *Manual de Direito Eletrônico e Internet*. São Paulo: Lex Editora, 2006.

PAIVA, Mario Antônio Lobato de. *Processo Virtual*. Revista Jurídica Consulex, ano VII, nº 154, abr. 2003.

PAIVA, Mario Antônio Lobato. *Primeiras Linhas em Direito Eletrônico*. Disponível em: <<http://jus.com.br/revista/texto/3575/primeiras-linhas-em-direito-eletronico>>. Acesso em: 10 dez.2012.

ROHRMANN, Carlos Alberto. *Notas acerca do Direito à Privacidade na Internet: A perspectiva comparativa*. Revista da Faculdade de Direito Milton Campos. Belo Horizonte, v. 9, 2002.