# A EFICÁCIA DA PROVA ELETRÔNICA

Marcos Vinícius Martins Castro[1]
Mariana Mello Santos

**SUMÁRIO:** 1. Introdução; 2. Prova Eletrônica; 3. Provas Típicas e Atípicas; 4. Requisitos de Validade da Prova Eletrônica; 5. Técnicas de Segurança Digital; 5.1. Criptografia; 5.2. Assinatura Digital; 5.3. Certificação; 6. Os Operadores do Direito e a Prova Eletrônica; 7. A eficácia da Prova Eletrônica na Jurisprudência; 8. Conclusão; Referências

## 1 INTRODUÇÃO

Com o avanço da tecnologia da informação alcançamos à rápida e tão sonhada distribuição do conhecimento científico. As distâncias ficaram pequenas e a tecnologia alcançou o seu apogeu. Com tais avanços as pessoas passaram a se comunicar em tempo real (Real time), mas não necessariamente de forma presencial, estabelecendo assim relações à distância e ampliando o conceito de comunicação.

Contudo, o avanço tecnológico nas comunicações também trouxe novos conflitos, pois os indivíduos dessas relações também precisam de uma tutela jurisdicional mais adaptada com as transformações. Dessas relações, nasceram conceitos jamais pensados antes da pós-modernidade, como realizar compras através de contrato eletrônico (comércio eletrônico); trocar mensagens por correio eletrônico quase que instantâneas; realizar reuniões e fechamentos de contratos através de vídeo conferencia e etc.

A todo o momento nos deparamos com situações seja no “ciberespaço” ou mesmo na transformação de documentos físicos em meios eletrônicos, onde podemos vislumbrar o nascimento de relações jurídicas entre sujeitos de direito e consequentemente a necessidade de comprovação de fatos ocorridos no mundo digital. O problema ganha maior contorno no momento que essas relações saem apenas do mundo fática e precisam entrar no mundo jurídico.

[1] Bacharelandos em Direito pela Universidade Salvador – UNIFACS

Com todas essas transformações o direito não pode e não deve ficar a margem. Os seus institutos devem ser atualizados para se adaptar as mudanças. Quando se fala em mudanças, não nos referimos apenas em mudanças legislativas, de certo que necessárias, mas também em mudanças no próprio poder judiciário e nos seus interpretes e aplicadores do direito, que na omissão legislativa, precisam tomar as rédeas da justiça nesse país.

Hodiernamente, o magistrado quando se depara com questões probatórias não tradicionais, onde, certamente tem que fazer uma analise mais apurada das provas e muitas vezes não possui o conhecimento especifico, tende a não reconhecer eficácia probatória daquela prova. Traduzindo em uma única expressão: aquilo que não conheço é porque não existe. Perceba que nesse caso, uma das partes ou até mesmo ambas as partes, não terão a sua tutela jurisdicional plenamente satisfeita, pois a justiça falhou quando não estava preparada para compreender as transformações sociais e adaptá-las a legislação vigente.

Na jurisprudência brasileira tem se verificado que os magistrados ao fazerem um juízo probatório acerca das provas de um processo, quando se deparam com provas eletrônicas associadas a provas tradicionais, fazem um juízo das provas digitais com fulcro nas provas tradicionais. Note que nesse caso, a prova digital teve quase ou nenhuma eficácia probatória.

Contudo, a grande problemática surge no momento em que os magistrados se deparam apenas com as provas eletrônicas e precisa atribuir-las eficácia probatória. Assim, é nesse momento que surgem as dúvidas, seja pela ignorância acerca do desconhecido, seja pela falta de confiabilidade atribuída a alguns meios probatórios pelo mesmo.

O certo é que, os operadores do direito não estão preparados para enfrentar essas questões e a conseqüência desse despreparo está sendo sentida por toda a sociedade.

Por tudo que foi dito acima podemos chegar à conclusão que as relações estabelecidas no mundo digital são realidade, e que não adianta os operadores do direito as ignorarem. Pois, tais relações, mais cedo ou mais tarde, procuram o mundo jurídico para dirimirem seus conflitos.

Logo, com tais avanços tecnológicos, é inconcebível que o mundo jurídico não passe a compreender e utilizar as provas eletrônicas que nascem das relações fáticas atuais. Pois, tais relações, quando em conflito, clamarão por soluções, as quais, apenas o direito poderá dar. Neste caso, devendo-se buscar a mesma valoração probatória que é dada na prova tradicional.

Diante disso, nasce a grande pergunta: Quando analisadas pelos operadores do direito as provas eletrônicas possuem a mesma eficácia probatória que as provas tradicionais?

A resposta não é simples como parece, deve-se trazer a discussão acerca das questões que envolvem a autenticidade (autoria), veracidade (integridade) e confiabilidade da prova eletrônica. Tratando desta forma, sua validade jurídica e acabando por admitir, ou não, eficácia probatória perante nosso sistema processual.

Com fulcro nessa discussão pretende-se alcançar os motivos que são causadores dessa difícil aplicação das provas eletrônicas pelos operadores do direito. Destarte, ao facilitar tal compreensão podemos identificar pontos vulneráveis na eficácia probatória da prova eletrônica e através da informação esclarecer dúvidas acerca da difícil compreensão da matéria.

É nesse diapasão que o trabalho busca trazer a discussão acerca da existência da eficácia probatória da prova eletrônica no nosso direito. Desmistificando a idéia de que a prova eletrônica não possui confiabilidade e autenticidade. Esclarecendo as questões mais debatidas acerca do tema, produzindo assim uma atmosfera de saber sobre a eficácia probatória da prova eletrônica.

## 2. PROVA ELETRÔNICA

É regra basilar no nosso Código Processual Civil que o autor é quem está incumbido de provar o fato constitutivo do seu direito alegado e o réu o de provar o fato impeditivo, modificativo ou extintivo do direito do autor. Destarte, quando o autor alega determinado fato ou ato jurídico, tem o direito e a faculdade de prová-lo. Prova se quiser e puder, não provando arca com ônus da sua omissão, sob pena de perder a demanda. De certo que a mesma regra se aplica ao réu, que deve provar a existência do fato impeditivo, modificativo e extintivo do direito da parte autora.

No mundo das provas, “cada uma das partes conta a sua versão sobre o que aconteceu. A versão mais bem provada, aquela que vier a convencer o julgador, tem tudo para ser a vencedora” (DIDIER, BRAGA, OLIVEIRA 2009, pg. 24).

> No módulo processual de conhecimento, para que o juiz possa formar seu convencimento e decidir o objeto do processo, faz-se fundamental a colheitas das provas que se façam necessárias, e que serão o material com base em que o juiz formará seu juízo de valor acerca dos fatos da causa. Este é, pois, o momento de se passar ao exame das normas e princípios que regem a prova, conjunto esse que recebe de alguns doutrinadores o nome de direito probatório. (CAMARA, 2009, p. 89)

O direito a prova é considerado um direito fundamental, uma vez que se deriva do contraditório e do acesso a justiça, estruturas basilares da tutela jurisdicional. Todos possuem o direito a provar aquilo que relatam, assim como possuem o direito a discutir a respeito das provas apresentadas por outros, ainda que incontestáveis.

As provas acabam por tomar forma à medida que convencem o julgador, seja pelo grau de confiabilidade a que possuem, ou até mesmo, pelo seu encaixe em um quebra-cabeça formado por uma variedade de provas entrelaçadas. Destarte, devem-se utilizar todos os meios probatórios legalmente possíveis para a confirmação dos fatos, sob pena de suprimir o contraditório e prejudicar a tutela jurisdicional.

Com o avanço da tecnologia e o desenvolvimento da internet, novas formas de relações são criadas, onde a presença é indiferente na formação de conflitos. Destarte, nasce uma nova demanda de conflitos que precisam ser dirimidos. È nesse contexto que nasce um novo gênero probatório, chamado de prova digital, onde existem muitas espécies como: o documento eletrônico; depoimento testemunhal online; interrogatório de réu preso via videoconferência; imagens digitais; mensagens eletrônicas; arquivo de áudios e gravações, entre outras.

O projeto de Lei brasileiro nº 4.906/01, em seu artigo 2º, inciso I, define o que seria documento eletrônico como: “a informação gerada, enviada, recebida, armazenada ou comunicada por meios eletrônicos, ópticos, opto-eletrônicos ou similares”.

Assim, não apenas os escritos em papel são considerados como documento, pois uma gravação, uma imagem, um vídeo, um contrato eletrônico e muitas outras formas digitais podem ser consideradas documentos, uma vez que documentam um fato ou ato da vida social. Se essa documentação registrada, é digital e como tal se

utiliza de alguma técnica atual com a criptografia assimétrica, permitindo assim a inalterabilidade do registro, não há como não chamá-lo de documento.

Importante que se diga que o Código de Processo Civil é claro em não estabelecer um rol taxativo (*numerus clausus*) de documentos para a produção de provas:

> Art. 383 - Qualquer reprodução mecânica, como a fotográfica, cinematográfica, fonográfica ou de outra espécie, faz prova dos fatos ou das coisas representadas, se aquele contra quem foi produzida lhe admitir a conformidade.
>
> Parágrafo único - Impugnada a autenticidade da reprodução mecânica, o juiz ordenará a realização de exame pericial.

Destarte, percebe-se que não haveria uma diferença substancial entre o documento tradicional e o documento digital, pois tanto um quanto outro, seria um meio para registra um determinado acontecimento. Logo, ontologicamente não haveria nenhuma diferente, pois a única diferença está na estrutura da sua forma.

Assim, a Prova digital ou eletrônica é toda prova produzida em meio digital, onde a sua validade jurídica e eficácia probatória sejam reconhecidas e garantidas pelas técnicas de segurança digital.

**3. PROVAS TÍPICAS E ATÍPICAS**

O CPC em seu bojo traz as provas típicas, que nada mais seriam que as provas tipificadas, ou seja, previstas em lei de forma expressa. Nesse caso não haveria dúvida quanto a sua utilização, pois há uma previsão legal especifica que legitima o seu uso.

Contudo, a questão das provas atípicas é que merece uma maior atenção e analise, já que, nessas provas não existe uma previsão legal especifica, destarte, não sendo tipificados no ordenamento.

> Outro meio de prova não previsto no Código de Processo Civil, mas também admissível, em decorrência das regras dos arts. 332 e 170 do Diploma processual, é tecnicamente chamada de prova atípica ou meio atípico de prova, tendo como exemplo a prova emprestada que cautelosamente, os tribunais vêm admitindo, desde de que seu emprego não ofenda a garantia constitucional do contraditório. (MARQUES, 2010, p. 83)

Faz-se mister, fazer uma distinção entre “meios típicos” e “meios legais”: Os primeiros seriam aqueles que estariam especificados expressamente em lei. Enquanto, que os segundos, seriam aqueles que mesmo sem existir um tipo especifico que os defina como meio válido, estariam de acordo com o ordenamento pátrio.

> Os meios de prova, ao menos em princípio, devem estar de acordo com as normas legais, pouco importando se expressamente previstos na lei. Essa ultima idéia – de expressa previsão legal – obviamente não tem relação com a prova estar de acordo com o direito ou não, mas sim com a tipicidade. (MARINONI e ARENHART, 2008, p. 387)

A prova emprestada é um exemplo de prova atípica, onde uma determinada prova que produzira efeitos em um determinado processo transcende os seus efeitos, alcançando um novo processo. São consideradas como prova emprestada, apenas aquelas produzidas no processo, tendo como exemplos: a prova oral, a prova pericial, a inspeção judicial entre outras. Desde modo, uma simples cópia de documentos em um processo, não serão consideradas como prova emprestada, uma vez que tal prova precisa ser produzida no processo.

A jurisprudência pátria tem aceitado a prova emprestada, desde que seja respeitado o principio do contraditório, haja vista que a sua validade e eficácia também será admitida sob aqueles que participaram do processo anterior, tornando-se imprescindível a sua participação na produção probatória.

É bom que se diga que prova digital também pode servir como prova emprestada, desde que a mesma tenha validade e eficácia probatória reconhecida em outro processo. Assim, imagine que após uma perícia em um servidor de computadores foram encontradas fotos digitais que vieram a se torna prova em um processo. Desde que respeitado o contraditório, seria perfeitamente possível utilizá-la como prova emprestada em outro processo, já que a mesma atendeu a todos os requisitos de admissibilidade da prova emprestada.

Preocupado com a insegurança trazida pelos meios probatórios atípicos o art. 332, do CPC, vem limitar a utilização das provas atípicas dizendo que: “Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa.”

Veja que o artigo atribui a validade dos meios probatórios atípicos a sua moralidade. Contudo,

> O fato de um meio de prova não estar expresso na lei nada tem a ver com a sua moralidade, pois o que define a possibilidade da utilização de uma prova é a sua conformação com o direito, e apenas nesse aspecto é que se pode aceitar que um meio moralmente ilegítimo seja considerado um meio de prova não conforme ao direito e, assim ilegal. (MARINONI e ARENHART, 2008, p. 387)

Devido a pouca evolução da legislação brasileira em relação às questões de validade e eficácia dos meios probatórios eletrônicos, não existindo na maioria dos

casos um tipo especifico para regulação do meio probatório. Deve-se na maioria dos casos atribuírem-la o status de prova atípica, sob pena de torná-la invalida ou ineficaz.

## 4. REQUISITOS DE VALIDADE DA PROVA ELETRÔNICA

Importante salientar que a validade dos documentos não está associada a sua estrutura. Podendo, em uma instrução probatória, se verificar que um documento físico é invalido, pois não foram respeitados os requisitos de validade, enquanto outro documento de natureza digital possui plena validade, uma vez que foram respeitados todos requisitos. Destarte, o que garante a validade e eficácia da prova eletrônica é a garantia que todos os requisitos de validade foram respeitados e não a sua origem.

No Brasil ainda não existe uma legislação que trate especificamente da validade dos documentos eletrônicos. Contudo, o projeto de Lei nº 4.906/2001, no seu artigo 3º diz que "não serão negados efeitos jurídicos, validade e eficácia ao documento eletrônico, pelo simples fato de apresentar-se em forma eletrônica".

Assim, como nas provas tradicionais a validade do documento eletrônico depende de alguns requisitos como a autenticidade (autoria) e integridade (veracidade) para produzirem eficácia.

Quando falamos de autoria estamos nos referindo à identidade do agente, ou seja, aquela pessoa que precisa ter sua autoria identificável, trazendo assim autenticidade à relação. A autenticidade é de suma importância, pois se tal identificação não for segura, pode uma das partes se utilizar dessa fragilidade para obter ganho de forma ilícita, como por exemplo, em um site falso na internet que coleta informações dos cartões dos usuários para posterior utilização.

> Geralmente, o que demonstra a paternidade, a autoria de um documento tradicional é a assinatura lançada no suporte material; em se tratando de documento eletrônico, é a assinatura digital que tem a função de autenticação (MARQUES, 2010, p. 133).

A autenticidade nos documentos eletrônicos é garantida através das técnicas de segurança digital como a assinatura digital, a certificação, a criptografia assimétrica entre outras, que confirmam a autoria do documento. Tais técnicas serão abordadas mais adiante.

> Conclui-se, portanto que a validade de um documento eletrônico depende de sua autenticidade (autenticação), que pode ser obtida pelo

> desenvolvimento de um processo que confirme a identidade das partes e garanta a fonte (origem) das mensagens eletrônicas. (LEAL, 2009, p. 154).

Insta salientar, a importância da autenticidade no documento, seja ele digital ou não, uma vez que, não sendo possível a confirmação da sua autoria o documento perde a sua validade e eficácia, tornando-se vazio a luz da analise probatória.

Importante ressaltar que uma parte da nossa legislação, atribuída à prova, foi elaborada para aplicação em documentos físicos, uma vez que o legislador não teria como antever todas as mudanças sociais e tecnológicas. Contudo, o mesmo estabeleceu de forma genérica e adaptativa, muitos artigos que tratam das provas. Destarte, desenhando um caminho mais amplo para o interprete adaptar-se aos novos conceitos sociais.

Tais requisitos para validade do documento tradicional e digital estão no bojo do Código de Processo Civil:

> Art. 372 - Compete à parte, contra quem foi produzido documento particular, alegar no prazo estabelecido no Art. 390, se lhe admite ou não a autenticidade da assinatura e a veracidade do contexto; presumindo-se, com o silêncio, que o tem por verdadeiro.

O próprio Código de Processo Civil em seu artigo 371 e define a autoria do documento:

> Art. 371 - Reputa-se autor do documento particular:
>
> I - aquele que o fez e o assinou;
>
> II - aquele, por conta de quem foi feito, estando assinado;
>
> III - aquele que, mandando compô-lo, não o firmou, porque, conforme a experiência comum, não se costuma assinar, como livros comerciais e assentos domésticos.

Os artigos 373 e 388 trarão situações aonde a autoria poderá ser questionada:

> Art. 373 - Ressalvado o disposto no parágrafo único do artigo anterior, o documento particular, de cuja autenticidade se não duvida, prova que o seu autor fez a declaração, que lhe é atribuída.
>
> Art. 388 - Cessa a fé do documento particular quando:
>
> I - lhe for contestada a assinatura e enquanto não se lhe comprovar a veracidade;
>
> II - assinado em branco, for abusivamente preenchido.
>
> Parágrafo único - Dar-se-á abuso quando aquele, que recebeu documento assinado, com texto não escrito no todo ou em parte, o formar ou o completar, por si ou por meio de outrem, violando o pacto feito com o signatário.

Os artigos trazidos acima explicam com clareza a *voluntas legis* diante da presunção de veracidade quanto à autenticidade dos documentos particulares. Assim, tanto os documentos tradicionais como os documentos informáticos se presumem autênticos, exceto nos casos onde houver impugnação das partes ou o julgador através do livre convencimento motivado entender pela inautenticidade.

Perceba que tais artigos foram elaborados com um só pensamento, o de trazer validade e eficácia probatória as provas tradicionais. Requisitos como assinatura digital, autenticação digital, criptografia entre outros, se quer foram citados nas suas estruturas. Contudo, tais dispositivos devem ser aplicados na medida do possível aos documentos digitais, levando-se em consideração a natureza distinta dos documentos.

A transmissão da informação eletrônica pode percorrer vários caminhos remotos até chegar ao destino final, nesse percurso pode ocorrer a interceptação e adulteração da informação por pessoas não autorizadas, comprometendo a sua integridade. Assim, a integridade diz respeito ao conteúdo da informação transmitida, se aquela informação de fato é a mesma que fora enviada pelo remetente ou se foi interceptada e alterada por um terceiro a relação.

> Assim, a integridade de um documento eletrônico está ligada ao fato de se poder assegurar que este documento não foi atacado, não sofreu alterações ou adulterações de conteúdo (LEAL, 2009, p. 156).

Destarte, a integridade está diretamente relacionada com a certeza de que determinado documento não foi corrompido no caminho da transmissão por um estranho a relação, ou até mesmo, manipulado por um dos integrantes da relação para fraudá-la. Sendo alterado, é de crucial importância que seja identificado facilmente através de técnicas de segurança especificas para tal finalidade.

> No concernente a integridade do documento, consiste em ter segurança, para saber se as mensagens enviadas coincidem, ou não, com as mensagens recebidas, pondo em pauta o tema do corrompimento das informações durante a sua transmissão (MARQUES, 2010, p. 134).

Logo, tais requisitos visam garantir que o documento chegue ao destino sem nenhum tipo de alteração e que a autoria desse documento seja conhecida e segura.

A validade da prova eletrônica está associada aos mesmos requisitos da prova tradicional, tendo em vista que tanto as provas tradicionais quanto as provas digitais,

precisam garantir a sua autenticidade e integridades para se tornarem válidas. Todavia, a forma como garantir essa autenticidade e integridade é que muda.

Nas provas tradicionais, conforme alhures, a autenticidade é verificada na maioria das vezes com a uma simples comparação de assinatura ou através de uma analise grafotécnica ou grafológica. Já nas provas eletrônicas ou digitais, a sua autenticidade é verificada através do uso das técnicas de segurança digital, como exemplo: a assinatura digital, criptografia, certificação, autenticação biométrica, entre outras.

Deste modo, a regra geral é que qualquer meio de prova, desde que não esteja proibido pela lei, deve ter sua validade garantida, sob pena de suprimir a ampla defesa e o contraditório, corolários da nossa constituição. Logo, o ciberdocumento é tão válido quanto o documento tradicional.

O fato de o documento ser considerado válido não garante que o mesmo produzirá os efeitos almejados pelas partes no curso do processo. Pois, imagine, por exemplo, que um determinado documento tenha a sua autenticidade e integridade reconhecida pelo julgador, mas que o mesmo chegue à convicção que o referido documento não serviria como prova para o caso em tela. Assim, o documento seria valido, mas a prova ineficaz.

## 5. Técnicas de segurança digital

Tentando garantir a segurança das relações estabelecidas no meio informático, foram desenvolvidas técnicas de segurança digital que possuem a finalidade de confirmar à autenticidade e integridade, garantindo assim confiabilidade as provas nascidas ou convertidas ao meio eletrônico.

> De toda a sorte, já é possível atestar a autenticidade e integridade dos documentos produzidos no meio digital , assim como no ambiente virtual, mediante, mediante o uso da criptografia assimétrica e da assinatura digital. É nesse compasso que alguns países, mais adiantados no uso da internet, já dispõem de Autoridades certificadoras, que funcionam como verdadeiros tabeliães virtuais, conferindo segurança aos documentos representativos das relações jurídicas celebradas entre aqueles que acreditam e se utilizam da rede (LAGO JUNIOR, 2001, p. 34)

Dentre as técnicas podemos citar a criptografia (simétrica e assimétrica) que tem a finalidade de esconder os dados tornando-os indecifráveis de tal maneira que só os interlocutores podem ter acesso ao conteúdo da informação, garantindo a sua integridade

(veracidade). Tal técnica associada à assinatura digital garante também a autenticidade (autoria) da informação transmitida.

> A partir dessa questão, surgiram modos ou técnicas de cifrar e decifrar as mensagens, de forma que apenas o remetente e o destinatário possam ter acesso ao conteúdo dos documentos envolvidos, através de um suporte técnico pessoal, que garante o sucesso da relação. (MARQUES, 2010, p. 151)

Tem também a certificação digital que através da autoridade certificadora, que é uma terceira entidade de confiança das partes, tem como finalidade garantir a certeza e confiança na identificação do remetente e integridade do conteúdo do documento digital.

Falaremos de algumas técnicas de segurança digital na atualidade. Contudo, é bom que se diga tais técnicas não são as únicas existentes, uma vez que a todo o momento novas técnicas são desenvolvidas para tornar os documentos digitais mais seguros.

## 5.1 Criptografia

Etimologicamente falando, a palavra criptografia origina-se do *kriptós*, que significa escondido, oculto, e *grafo*, que significa escrever. Então, a criptografia é a técnica de esconder aquilo que se escreve através de códigos, onde apenas as partes envolvidas na comunicação terão acesso ao verdadeiro conteúdo.

> Portanto, uma mensagem só será criptografada se tiver sido gerada a partir de um sistema metalingüístico, tendo como intenção o enigmático e mais que os efeitos passem a ser reversíveis, isto é, que haja entre os interlocutores elementos possíveis de decifrar a mensagem embaralhada, produzindo o efeito desejado (MARQUES, 2010, p. 158)

A criptografia, ferramenta criada com a finalidade de proteger a integridade dos documentos, tornando-os confiáveis através de um conjunto de códigos indecifráveis aos olhos dos não destinatários. A técnica de criptografia usa um padrão criptográfico para cifrar e decifrar. Tal padrão é denominado de chave.

> A criptografia teve origem militar. Segundo conta a história, os romanos se valiam de uma rudimentar, porém eficiente para a época, técnica criptográfica para enviar mensagem aos centuriões nos campos de batalha, evitando-se o risco de interceptação por parte dos inimigos ou de traição dos mensageiros. A chamada “escrita cifrada pó Cezar” consistia na substituição das letras do texto pela terceira letra seguinte do alfabeto: a letra “a” passava a ser substituída pela letra “d”, o “b” pelo “e” e assim sucessivamente (LAGO JUNIOR, 2001, p. 35)

Ressalta-se que mesmo a criptografia sendo considerada uma técnica que oferece segurança na transmissão de dados, não se pode atribuí-la o grau absoluto, tendo em vista que existem muitas técnicas de criptografia. Sendo as mais conhecidas na modernidade:

A criptografia simétrica ou de chave privada que utiliza a mesma chave para cifrar e decifrar a mensagem. Sendo muito usada em redes fechadas de computadores que ficam isolados, utilizada para garantir o sigilo de arquivos pessoais armazenados.

> Uma mensagem é cifrada por uma senha (chave privada) e decifrada com a utilização dessa mesma chave, que deve ser mantida em sigilo para preservar a segurança da comunicação.
>
> Assim, o emissor e o receptor combinam de antemão a senha (chave privada) e dela se utilizam da codificação e decodificação da mensagem. Este sistema não é absolutamente seguro porque se utiliza de operações matemáticas com retorno e não serve para provar a identidade da pessoa. (LEAL, 2009, p. 160)

Na criptografia assimétrica ou de chave pública utiliza-se duas chaves distintas, uma chave para cifrar a mensagem e outra para decifrá-la. Sendo utilizadas em redes abertas como rede mundial de computadores.

Nessa modalidade de criptografia, é criada, a partir de cálculos matemáticos, uma chave pública e uma chave privada. A chave privada ficará exclusivamente em posse do proprietário do sistema, enquanto a chave pública será distribuída todos aqueles que mantenham uma comunicação com o proprietário.

Importante que se diga que tanto a chave pública quando a chave privada poderá ser usada para cifrar, enquanto a outra será capaz de decifrar e vice versa. Não sendo possível a utilização da mesma chave para cifrar e decifrar a mesma mensagem.

Insta salientar que o projeto de Lei de nº 4.906/01, em seu artigo 2º, inciso III, traz a definição do modelo de criptografia assimétrica como: “modalidade de criptografia que utiliza um par de chaves distintas e interdependentes, denominadas chaves pública e privada, de modo que a mensagem codificada por uma das chaves só pode ser decodificada com o uso da outra chave do mesmo par”.

A criptografia assimétrica é mais segura que a criptografia simétrica, uma vez que se utiliza de duas chaves, uma publica e uma privada, bem como o fato de chave privada não necessitar ser combinada entre as partes nem revelada a ninguém. Também tem a questão dos cálculos das operações matemáticos para criptografar que alem de serem mais complexos, não possuem uma operação inversa.

A segurança trazida às comunicações pela criptografia é algo que merece aplausos, nunca foi tão seguro transmitir informações aos mais distantes destinatários. Todavia, nem tudo é um “mar de rosas”. A criptografia por ser uma técnica que visa ocultar as informações transmitidas, pode facilmente ser usada por criminosos inescrupulosos para esconder a prática de ilícitos.

Vários países vêm estabelecendo regras ao uso da criptografia, controlando o emprego de suas técnicas, exigindo licença governamental e limitando as exportações de sistemas criptográficos. Deste modo, tratando a criptografia como uma questão de ordem pública e defesa nacional.

Um bom exemplo da limitação imposta pelos países aos desenvolvedores de sistemas criptográficos está no tamanho em bits da sua chave, pois quanto maior o tamanho da chave, mais difícil será a sua decodificação. Assim, a maioria dos países limita a exportação do software criptográfico a uma chave de tamanho não maior que 40 bits.

### 5.2. Assinatura digital

No documento tradicional, aquele de papel, a assinatura física possui a finalidade de garantir a certeza quanto a sua autenticidade. Já no documento eletrônico, tal assinatura seria impossível, uma vez que se trata de algo intangível, necessitando assim, de uma criação tecnológica que garantisse a certeza da sua autoria. Diante da dificuldade de garantir a confiabilidade, fora desenvolvida a assinatura digital.

> Pelas próprias características do meio digital, identificar o emissor de uma mensagem não é uma tarefa das mais fáceis. Contudo, conforme já salientado, a utilização de assinatura digital baseada na criptografia assimétrica é apontada, na atualidade, como uma forma segura o suficiente para se garantir validade jurídica a documentação dos atos realizados por meio eletrônico (LAGO JUNIOR, 2001, p. 38)

Com facilidade de adulteração dos documentos informáticos, a Lei modelo da UNCITRAL, estabeleceu como regra para garantir a mesma confiabilidade dos documentos tradicionais o uso da assinatura digital criptográfica acompanhado da certificação digital.

Importante que se esclareça que a assinatura digital assimétrica não é uma "assinatura tradicional" digitalizada, mas sim um conjunto de instruções chamado de algoritmo, criptografado assimetricamente. Na assinatura tradicional digitalizada, existirá sempre a mesma seqüência de bits, tornado-a mais insegura quanto a sua manipulação, enquanto na assinatura digital existirá sempre uma seqüência de bits distinta, garantido uma maior segurança ao ciberdocumento.

A assinatura digital seria um dado especifico e codificado que acompanha um determinado ciberdocumento codificado, onde seria possível comprovar a autoria da mensagem, bem como se a mesma foi modificada após a sua saída da origem.

> A assinatura digital é produzida cifrando a mensagem com a própria chave privada, que só poderá ser decifrada com a chave pública. Ou seja, se for possível decifrar a mensagem com o uso da chave pública, é sinal que ela só pode ter sido codificada com a chave privada correspondente e, portanto, somente aquele, somente aquele que detém esta chave privada poderia tê-lo feito.
>
> As assinaturas digitais preenchem os requisitos antes comentados da autenticidade, integridade e não repúdio dos documentos eletrônicos. A identidade do "signatário" da firma eletrônica é feita pela prova da posse da chave privada, o autor sabe que só sua chave pública correspondente poderá decifrá-la, assim, o destinatário da mensagem é a identidade do emitente (LEAL, 2009, p. 163 e 164).

Em síntese, a criação da assinatura digital ocorre da seguinte forma: primeiramente gera-se um resumo da mensagem por um algoritmo, logo após aplica-se a chave privada a esse resumo, transformando-o em um resumo criptografado, onde anexa o certificado digital do autor com a sua chave pública.

> Ao final, fazendo a comparação entre o resumo da mensagem gerado e aquele recebido e codificado, indicará que a mensagem não foi alterada, mantendo-se, por conseguinte, intacta (MARQUES, 2010, p. 169).

Deste modo, é importante que se diga que qualquer alteração na seqüência de bits que estrutura o documento digital, invalidará a sua assinatura, haja vista que a mesma está única e exclusivamente vinculada aquele documento.

Alguns países como os EUA, e a própria União Européia, há muito tempo já possuem uma legislação especifica sobre a assinatura digital. No Brasil em vigor, existem decretos que regulam a atividade na Administração Pública Federal, como o Decreto nº 3.505/2000, que implementou a política de segurança da informação nos órgãos da administração e o Decreto nº 3.587/2000, que implementou a infra-estrutura de chaves públicas no pode executivo e a medida provisória nº 2.200-1/2001, que implementou a infra-estrutura das chaves públicas no Brasil (ICP-Brasil).

Ademais, O projeto de Lei 4.906/2001, em seu artigo 4º, estabelece como requisitos de validade do documento eletrônico que a sua autenticidade seja corroborada através de uma assinatura digital com os seguintes parâmetros:

> Art. 4º – As declarações constantes de documento eletrônico presumem-se verdadeiras em relação ao signatário, nos termos do código civil, desde que a assinatura digital:
>
> I - seja única e exclusiva para o documento assinado;
>
> II - seja passível de verificação pública;
>
> III - seja gerada com chave privada cuja titularidade esteja certificada por autoridade certificadora credenciada e mantida sob o exclusivo controle do signatário;
>
> IV - esteja ligada ao documento eletrônico de tal modo que se o conteúdo deste se alterar, a assinatura digital estará invalidade;
>
> V - não tenha sido gerada posteriormente a expiração, revogação ou suspensão das chaves;

Quanto a questão de segurança, um ponto que merece atenção está na possibilidade da falsidade do documento digital. Conforme alhures, na assinatura criptografada, a chave privada é a responsável pela assinatura do documento, enquanto a chave publica pela sua confirmação. Então, é perfeitamente possível que possa ocorre uma apropriação indevida da chave privada, seja por descuido ou até mesmo por coação. Destarte, faz-se mister dizer, que tanto a assinatura do documento eletrônico quanto o documento digital são passíveis de serem conseguidas através da coação.

O julgador ao se deparar com um caso onde um terceiro, se utilizando de uma chave privada alheia, realizou alterações em um documento como se fosse o seu titular, deve o magistrado avaliar através do conteúdo probatório se houve apropriação indevida e uso ilícito da assinatura, invalidando o documento caso se confirme.

Destarte, como a assinatura digital está vinculada exclusivamente aquele documento através da criptografia assimétrica, o documento eletrônico torna-se muito mais confiável que o documento tradicional, uma vez que o documento cartáceo necessita de um exame pericial para confirmar sua manipulação.

Com relação ao ônus probatório da autenticidade documental, o Código de Processo Civil em seu artigo 389, inciso II, diz que o ônus de provar a autoria de determinado documento recairá sobre o seu autor.

> Art. 389 - Incumbe o ônus da prova quando:
>
> I - se tratar de falsidade de documento, à parte que a argüir;
>
> II - se tratar de contestação de assinatura, à parte que produziu o documento

Tal artigo deve ser usado tanto para os documentos cartáceos quanto para os documentos digitais. Assim, no caso dos documentos digitais, onde a chave pública tem a função de confirmar determinada assinatura eletrônica, competirá a parte que produziu o documento, provar a autenticidade da chave pública.

Por outro lado se a assinatura estiver adequada, porém, tenha sido usada por outra pessoa, estaremos diante de uma falsidade de documento, incumbindo assim o ônus de provar, a parte que alegou o fato. Perceba que nesse caso, trata-se do uso indevido da chave privada (responsável pela assinatura), devendo-se aplicar o inciso I, do artigo 389, do Código de Processo Civil.

### 5.3 Certificação

Existem sistemas de assinatura digital que se baseiam na confiança entre os interlocutores, onde os usuários que se utilizam desses sistemas garantem a autenticação da chave a qual foi criada a assinatura. Contudo, o grande problema esta em garantir essa mesma autenticidade e integridade naquelas comunicações, onde há uma necessidade de distribuição e individualização da chave pública.

Todos os dias através dos portais de comércio eletrônico são distribuídas em massa chaves públicas, que produzem através da troca de informações, relações comerciais que precisam ter a sua identidade e integridade garantida.

> Poderá, perfeitamente, uma pessoa mal intencionada interceptar a mensagem, gerando uma chave pública e retransmitir a mensagem ao destinatário, sem que ele desconfiei das adulterações do conteúdo do documento, no momento em que decifrar a mensagem.

> Para evitar, então, essa fraude, institui-se a certificação digital, onde a identidade do proprietário das chaves é previamente verificada por uma terceira entidade de confiança dos interlocutores, que terá a incumbência de certificar a ligação entre a chave pública e a pessoa que a emitiu, como também a sua validade (MARQUES, 2010, p. 174).

Os certificados digitais possuem a função de garantir que uma determinada chave pública pertence a uma determinada entidade (usuário e máquina). Deste modo, associando o nome da entidade a seu par de chaves (pública e privada). O responsável pela elaboração dos certificados digitais é a Autoridade Certificadora, que possui como atribuições a emissão, revogação, manutenção e publicidade dos certificados.

> Geralmente os certificados digitais são assinados com a chave privada do usuário e contém a sua chave pública, seu nome, prazo de validade do certificado, nome da autoridade certificadora que emitiu o certificado e o número de serie do certificado. Cabe ao usuário a responsabilidade de manter a sua chave privada, em segredo, sob pena de comprometer toda a segurança do processo. (LEAL, 2009, p. 167).

No modelo de certificação digital, caso ocorra a interceptação da mensagem por um terceiro, será perfeitamente possível determinar veracidade do conteúdo do documento:

O ICP-Brasil, que fora instituído pela medida provisória nº 2.200-1/2001, adota um sistema de certificação digital, onde garante a mesma validade ao documento digital que é garantida ao documento tradicional. Contudo, deve-se ressaltar que tal garantia só será possível em situações onde sejam respeitados os requisitos de segurança da assinatura digital criptografada.

Importante ressaltar que a Medida provisória que criou esse órgão, também estabeleceu que a assinatura digital terá a mesma validade e eficácia da assinatura tradicional. Todavia, foi mais longe ainda ao estabelecer como validas outras certificadoras, além da ICP-Brasil e até mesmo como opcional o uso da certificação.

A certificação também tem como finalidade garantir eficácia probatória e validade jurídica perante terceiros, pois caso a assinatura não possua certificação, os efeitos produzidos alcançaram apenas as partes envolvidas.

O projeto de Lei 4.906/2001, em seu artigo 11, estabelece critérios que precisam ser respeitados para que os certificados digitais tenham eficácia probatória em juízo:

> Art. 11º – Para fazer prova, em juízo, em relação ao titular indicado no certificado, é necessário que, no ato da sua expedição:
>
> I – o titular tenha sido pessoalmente identificado pela autoridade certificadora;
>
> II – o titular haja reconhecido ser o detentor da chave primária correspondente a chave pública para a qual tenha solicitado o certificado;
>
> III – tenha sido arquivados registros físicos comprobatórios dos fatos previstos nos incisos anteriores, assinados pelo titular.

Deste modo, a técnica de certificação digital, tem a função de garantir que ninguém receberá uma chave pública, se não for certificado por uma entidade certificadora confiável.

## 6. OS OPERADORES DO DIREITO E A PROVA ELETRÔNICA

Se discute no mundo inteiro a criação de uma legislação especifica para regular as relações informáticas. Alguns países com o Reino Unido, EUA, e Índia, avançaram muito nessa questão, já possuindo uma legislação mais atual as suas necessidades. Todavia, no Brasil, com exceção de algumas alterações legislativas como a lei do processo eletrônico e pequenas alterações no código de processo civil, pouco ou nada foi realizado para trazer uma legislação mais especifica as questões digitais. Assim, nasce a pergunta: como o operador do direito deve se comporta diante da omissão legislativa?

> Os contratos eletrônicos realizados via internet ainda não se encontram regulamentados por lei no Brasil. Trata-se de uma nova forma de contrato que, dada a vulnerabilidade do mundo virtual, expõe os contratantes a riscos e possibilita os mais variados tipos de fraudes. Como exemplos, podem ser mencionados a violação a direitos da personalidade, recebimento de mensagens indesejadas (spam), adulteração, receptação e retardamento no envio e recepção de mensagens eletrônicas. (LEAL, 2009, p. 96)

No que pese o Código Civil e o Código de Processo Civil não tratar de forma direta de questões como a assinatura digital, certificação, criptografia, entra outras, devem os operadores do direito, aplicar os seus ditames naquilo que seja possível de ser aplicado quanto a prova digital.

> Assim, interpretando-se alguns dispositivos legais do nosso ordenamento jurídico, possibilita-se, sem maiores problemas, atribuir ao documento eletrônico validade e eficácia jurídica probatória, porque o legislador brasileiro elaborou norma elástica, para a aceitação de meios de prova,

> atendendo ao presente e as futuras modificações e inovações de novas formas de suporte para as provas (MARQUES, 2010, p. 145)

Na omissão legislativa deve o operador do direito se utilizar de uma interpretação sistemática do ordenamento, aplicando a analogia aos casos onde exista tal omissão. Assim, utilizando a legislação pertinente ao caso concreto, como por exemplo: nos casos onde há uma relação de consumo deve-se aplicar a norma consumerista; já em outras onde exista um contrato paritário ou que trate de responsabilidade civil deve-se utilizar o Código Civil e o Código de Processo Civil.

O próprio Código de Processo Civil, em seu art.126, já norteia como devem ser tratadas as questões de omissão legislativas:

> Art. 126 - O juiz não se exime de sentenciar ou despachar alegando lacuna ou obscuridade da lei. No julgamento da lide caber-lhe-á aplicar as normas legais; não as havendo, recorrerá à analogia, aos costumes e aos princípios gerais de direito. (Alterado pela L-005.925-1973)

Por incrível que parece a Lei de processo eletrônico é o que temos de mais moderno na legislação digital brasileira, uma vez que temos apenas uma medida provisória e alguns projetos de lei em curso. A lei trata de temas relacionados a segurança nas relações digitais, estabelecendo diretivas acerca da utilização da assinatura eletrônica e certificação digital.

Numa analise mais criteriosa da lei, percebe-se que a mesma foi omissa no tratamento quanto às provas digitais (originárias) de fora do processo eletrônico, regulando apenas as provas tradicionais convertidas ao meio digital e as provas produzidas no próprio processo eletrônico. De toda sorte, a lei, ao reconhecer eficácia probatória das provas originárias do próprio processo eletrônico, mediante o emprego de técnicas como a certificação e a assinatura digital, deu um passo enorme para o reconhecimento das provas fora do processo.

Foi instituída pelo Governo Federal em 28.08.2001, a Medida Provisória 2.200-2, que estabeleceu o órgão ICP-Brasil (nfra-Estrutura de Chaves Públicas Brasileiras), que por sua vez, criou a Autoridade Certificadora para reconhecer eficácia probatória e validade jurídica aos documentos informáticos. Assim, os operadores do direito na omissão legislativa, devem utilizar a Medida provisória que segundo a constituição possui força normativa.

> A ICP-Brasil passou a assumir para si a incumbência de providenciar as condições necessárias para a validação jurídica do comércio eletrônico no país, garantindo, desta sorte, a autenticidade, integridade, eficácia e validade jurídica dos documentos eletrônicos, além das aplicações habilitadas que utilizem certificados digitais (MARQUES, 2010, p. 182)

Insta salientar, que existem alguns projetos de lei em tramite nas nossas casas legislativas:

O projeto que regulamenta os contratos eletrônicos, como é o caso do Projeto de Lei nº 1.589/99 da OAB de São Paulo, que trata do comércio eletrônico e dos requisitos de validade jurídica do documento digital e a sua assinatura. Traz alguns traços da Lei Modelo da UNCITRAL, quando trata do comércio eletrônico e suas transações e quando atribui a mesma força probante do documento tradicional ao documento eletrônico assinado criptograficamente.

O projeto é bastante inovador, uma vez que traz questões como: proteção aos diretos consumeristas adaptados ao comercio eletrônico; estabelece diretivas de conduta para o fornecedor com a intenção de evitar responsabilidade por ineficácia contratual; armazenamento e privacidade das informações no provedor, além de regular os certificados digitais e estabelecer a certificação de chave pública feita por tabelião.

Tem também o Projeto de Lei nº 4.906/2001 que dispõe sobre o valor probante do documento eletrônico e da assinatura digital, bem como institui normas para o comércio eletrônico.

Contudo, o Projeto de Lei nº 672/99, proposto pelo senador Lúcio Alcântara, baseado no modelo da UNCITRAL é o que está mais adiantado, aguardando o parecer da comissão de constituição e justiça.

Outra solução temporária seria a utilização do modelo de legislação de comércio eletrônico da UNCITRAL (Comissão das nações unidas para o direito internacional comercial), que trata da validade dos documentos e da assinatura digital. Importante ressaltar que não haveria problema algum quanto a sua utilização, haja vista que o Brasil é signatário. Contudo, é bom que se diga que tal legislação é um modelo genérico e como tal precisa ser adaptada a cada estado.

Assim, os operadores do direito não devem e não podem ficar inertes diante das alterações sociais, nem mesmo se utilizar da desculpa de não ter uma legislação especifica regulando a matéria. Devendo o mesmo se utilizar do estudo da ciência do direito para se chegar as soluções, seja pelo uso da analogia, das legislações internacionais ou até mesmo pelas construções doutrinarias e jurisprudenciais.

> Se a revolução econômica é tecnológica é inegável, cabe ao jurista acompanhá-la, revendo até as premissas de sua dogmática, reconhecendo as mudanças que estão ocorrendo com a globalização e adotando as medidas uteis ou necessárias, no mundo do qual muitos dos conflitos do passado, entre nações, empresas e indivíduos, estão sendo substituídos por parcerias realizadas no interesse comum. (LEAL, 2009, p. 127)

Superada a aplicação normativa, os operadores do direito devem reconhecer a eficácia da prova eletrônica, desde que a mesma demonstre os requisitos para sua validade. Logo, em uma relação jurídica as partes devem demonstrar por todos os meios de provas que na formação de determinado documento (sentido *lato sensu*), foram respeitados os requisitos de autenticidade e integridade.

Importante ressaltar, que o julgador pode de oficio ou a requerimento das partes, averiguar os requisitos de autenticidade e integridade de um determinado documento, para deste modo, facilitar o seu juízo probatório acerca da questão.

> É absolutamente, possível que o magistrado, por interesse próprio ou a requerimento das partes, acesse a rede de informações e determine que o provedor ou a autoridade certificadora, libere, de seus registros cadastrais, informações especificas, relativas a analise judicial feita, sem invadir a esfera jurídica de terceiros, evidentemente, para provar se o documento eletrônico averiguado nele foi originado de uma determinada pessoa, para localizá-la e se chegar a sua autoria com um certo grau de certeza (MARQUES, 2010, p. 136)

Deste modo, é perfeitamente possível que o magistrado nomeie um perito para fazer uma analise mais apurada acerca do documento. Tal analise pode se da, por exemplo, com o rastreamento em um servidor para encontrar um arquivo que fora formatado, ou garantir que uma determinada imagem não tenha sido manipulada.

> Art. 383 - Qualquer reprodução mecânica, como a fotográfica, cinematográfica, fonográfica ou de outra espécie, faz prova dos fatos ou das coisas representadas, se aquele contra quem foi produzida lhe admitir a conformidade.
>
> **Parágrafo único - Impugnada a autenticidade da reprodução mecânica, o juiz ordenará a realização de exame pericial. (grifo nosso)**

Sabe-se da grande dificuldade em garantir a aplicação das técnicas de segurança a uma variedade incalculável de documentos eletrônicos (sentido *lato sensu*). Assim, não seria possível, por exemplo, aplicar uma técnica de assinatura criptografada ao tirar uma fotografia em uma máquina digital ou ao realizar uma gravação de um vídeo em uma webcam. Questões como essas devem ser superadas, através do principio do livre convencimento motivado, onde o magistrado se utilizando das circunstâncias que envolvem a produção e transmissão do documento forma a sua convicção.

Os operadores do direito não podem ficar inertes a evolução tecnológica e social, devendo aplicar o direito de acordo com as necessidades sociais. A falta de um amparo normativo especifico não pode servir como desculpa para sua omissão, pois através de uma interpretação sistematicamente normativa, pode-se enquadrar ao novos fenômenos  sociais as normas preexistentes.

## 7. A EFICÁCIA DA PROVA ELETRONICA NA JURISPRUDÊNCIA

Conforme alhures, o mundo no ultimo século passou por muitas transformações de ordem políticas, religiosas, econômicas e principalmente tecnológicas. As relações sociais tornaram-se muito mais complexas no que tange a comprovação probatória de fatos ocorridos hodiernamente.

O meio digital passou a fazer parte do cotidiano social, criando-se novas formas de interação entre indivíduos, que passaram a estabelecer relações afetivas e comerciais em um mundo virtual. É nesse contexto que nascem os “conflitos digitais”, aqueles originados dessas relações afetivas e comerciais.

Diante do explanado, será discutido como a jurisprudência pátria tem tratado de temas como: o reconhecimento da foto digital; a utilização do correio eletrônico como prova; a validade e eficácia dos contratos realizados através do comercio eletrônico (e-commerce), entre outros.

Um tema bastante discutido na doutrina é a utilização da foto digital como meio probatório. Conforme dito acima, a discussão gira em torno da imposição do Código de Processo Civil em estabelecer como obrigatório o acostamento dos negativos ao processo para garantir a sua validade e eficácia probatória.

No que pese o Código Processual Civil em seu artigo 385, §1, vincular a fotografia ao seu negativo, a jurisprudência majoritária tende a reconhecer a validade e eficácia da fotografia originada em meio digital, com base nos artigos 225, CC e 383 do CPC, que tratam das reproduções mecânicas.

> Ementa: "DIREITO AUTORAL. FOTOGRAFIA. AÇÃO DE INDENIZAÇÃO. REPRODUÇÃO NÃO AUTORIZADA DE OBRA ARTÍSTICA. CONTRAFAÇÃO. PROVA EFETIVA DE TITULARIDADE DE DIREITO AUTORAL. **O negativo a que se refere a lei anterior não é a única forma de produção de obra fotográfica à vista da evolução da tecnologia, já se reconhecendo sua feitura por slides ou impressão digital.** Desnecessidade de indicação de valor certo e determinado referente aos danos pleiteados." TJRJ, 5ª Câmara Cível. Apelação Cível 1999.001.15076. Rel. Des. Roberto Wider. Julgado em 07/12/1999 (grifo nosso)

Tem se aceitado sem nenhum problema as fotos digitais originadas em perícias, ressalvados os casos onde exista impugnação por assistente técnico quanto ao laudo pericial. Deste modo, por cautela, se faz necessário que o perito ao realizar a vistoria esteja na presença do assistente. Nos casos das perícias judiciais, como se trata de um perito de confiança do magistrado a presunção de validade é bem maior que na pericia convencional.

> Ementa: "APELAÇÃO CRIMINAL Nº 404.076-8 - UBERABA - 6/8/2003 EMENTA: FURTO QUALIFICADO - AUTORIA - PROVA SUFICIENTE - RES FURTIVA - POSSE PACÍFICA - CONSUMAÇÃO - TENTATIVA - NÃO-OCORRÊNCIA - PENA-BASE - ANTECEDENTES - MAJORAÇÃO - REGIME E SUBSTITUIÇÃO DA PENA - ASPECTOS SUBJETIVOS. Encontrando-se a res furtiva na posse do acusado, sem que esse possa explicar com verossimilhança como se deu o acesso aos bens e estando a prova indiciária em consonância com os demais elementos, há contexto fático suficiente à expedição do decreto condenatório. Existindo provas de que o réu tinha a posse pacífica dos bens furtados, entende-se como consumado o delito. **A perícia técnica que atesta o rompimento do obstáculo, inclusive com FOTO DIGITAL do local, comprova o furto qualificado.** A pena-base, sendo amplamente desfavoráveis as circunstâncias judiciais, pode ser arbitrada além do mínimo legal. A pena de multa deve guardar certa proporcionalidade com a sanção privativa de liberdade, tendo-se ainda em consideração a capacidade econômica do réu. Inteligência do art. 60, CPB. Apelo conhecido e parcialmente provido TJMS Apelação N° 2.0000.00.404076-8/000(1) – Rel. Des. E DIWAL JOSÉ DE MORAIS. Julgado 06.08.03. (grifos nosso)

Deste modo, a jurisprudência tem entendido que há uma presunção relativa em relação a validade e eficácia da foto digital. Devendo, em caso de dúvida quanto a autenticidade, a parte contrária impugná-la, sob pena de aceitação tácita.

O correio eletrônico ou correspondência eletrônica, devido o avanço nas comunicações vem sendo utilizado com maior freqüência do que as comunicações cartáceas. Destarte, crescendo a demanda pela comprovação de fatos através do correio eletrônico e com isso a necessidade de reconhecê-lo como meio probatório eficaz.

> Ementa: PRETENSÃO DE REPARAÇÃO CIVIL CUMULADA COM CAUTELAR INCIDENTAL DE EXIBIÇÃO DE DOCUMENTOS. **SUPOSTO DANO MORAL ADVINDO DE MENSAGENS ELETRÔNICAS OFENSIVAS À HONRA DA APELANTE.** alegação de nulidade da sentença afastada, porquanto, além de insubsistente, a suposta deficiência na avaliação de prova consubstancia error in judicando. requerimento extemporâneo de inversão do ônus da prova, na esteira da súmula 91 do TJ/RJ. provedores de correio eletrônico que não possuem responsabilidade quanto ao conteúdo dos e-mails enviados ou recebidos por seus usuários. obrigação de filtragem ou fiscalização que não lhe é possível imputar, tendo em vista a proteção constitucional à inviolabilidade das correspondências (artigo 5º, xii, da CF/88). esfera obrigacional daquelas pessoas jurídicas que se restringia à viabilização da identificação e localização do computador conectado à internet da onde foram enviadas as mensagens, o que de fato foi observado. inexistência de defeito no serviço. inaplicabilidade do artigo 14 do cdc. não identificação do autor das mensagens, o que impossibilita a condenação do segundo apelado com base em meros indícios e prova da autoria que cabia à apelante, na forma do artigo 333, i, do CPC. pretensão temerária de que o segundo apelado comprove fato negativo. caracterização da famigerada prova diabólica. recurso conhecido e em parte provido tão somente para reduzir os honorários de advogado para r$ 2.000,00, para cada réu. TJRJ Apelação N° 0013070-5 4.2007.8.19.0028 – Rel. Des. GABRIEL ZEFIRO. Julgado 21.07.10. (grifos nosso)

O caso em tela trata de um suposto dano a honra, onde o acionado fora acusado de enviar mensagens eletrônicas de cunho ofensivo a honra do Acionante. Tais mensagens foram enviadas ao Acionante, bem como a um determinado número de pessoas do seu convívio social. Fora requerido pelo Acionante que o Provedor de correio eletrônico, bem como a concessionária de telefonia, informassem a autoria e a origem do remetente das mensagens, sob pena de assumir a responsabilidade.

Deste modo, o entendimento jurisprudência é pacífico quanto a utilização do correio eletrônico como meio probatório, devendo em caso de suposta falsificação da autoria e/ou conteúdo da mensagem, ser impugnada pela parte contraria.

Quanto aos contratos eletrônicos a jurisprudência tem se deparado na maioria dos casos com questões como: a responsabilidade dos provedores de hospedagem nos

contratos gratuitos ou onerosos de locação de espaço eletrônico e contratos realizados através do comercio eletrônico.

Os contratos de locação de espaço eletrônico são aqueles em que um provedor de dados (locador), disponibiliza um determinado espaço, gratuito ou oneroso, na internet, para armazenamento de dados para uma entidade ou pessoa (locatário). Dessa espécie de contrato eletrônico têm nascido grandes discussões acerca da responsabilidade dos provedores quanto ao conteúdo armazenado e publicizado pelos seus locatários.

No que pese não existir uma legislação especifica para da tratamento aos casos de responsabilidade dos provedores de hospedagem, segundo a jurisprudência deve-se utilizar outra legislação para sanar tal falta. Deste modo, com base na teoria da responsabilidade civil, em regra o provedor não é responsável, pois não tem o dever legal de fiscalização dos locatários, salvo se interromper o serviço prestado ao agente; em caso de ocorrência de ato ilícito ou recusar a identificar o locatário que cometer ato ilícito.

> AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS - PUBLICAÇÃO DE TEXTO OFENSIVO EM SÍTIO VIRTUAL - RESPONSABILIDADE CIVIL - APLICAÇÃO DA LEI DE IMPRENSA - IMPOSSIBILIDADE - PROVEDOR DE HOSPEDAGEM - AUSÊNCIA DO DEVER DE INDENIZAR - AÇÃO CAUTELAR - NULIDADE DA SENTENÇA - AUSÊNCIA DE FUNDAMENTAÇÃO - INOCORRÊNCIA - ABSTENÇÃO DE PUBLICAR TEXTOS FUTUROS - IMPOSSIBILIDADE - À falta de legislação específica, comumente tem-se aplicado às relações travadas na rede mundial de computadores o regramento atinente à lei de imprensa, equiparando-se o sítio virtual - ou site, para os menos apegados à língua pátria - à figura da "" agência noticiosa "" contemplada nos artigos 12 e 49, § 2º, da Lei nº. 5.250/67. - No entanto, essa exegese do referido artigo não pode ser feita de forma irrestrita, devendo-se atentar para as peculiaridades do meio de comunicação considerado. - A internet consiste em um conglomerado de redes de computadores dispersos em escala mundial, com o objetivo de realizar a transferência de dados eletrônicos por meio de um protocolo comum (IP = internet protocol) entre usuários particulares, unidades de pesquisa, órgãos estatais e empresas diversas. - **Ainda que a internet seja um meio de comunicação relativamente recente, não há que se falar em necessidade de norma especial para sua regulamentação, salvo casos que versem sobre especificidades técnicas de sistemas de informática**. - **O provedor de hospedagem permite que o usuário publique informações a serem exibidas em páginas da rede. A relação jurídica aproxima-se de um CONTRATO DE LOCAÇÃO DE ESPAÇO ELETRÔNICO, com a ressalva de que poderá ter caráter oneroso ou**

> **gratuito. -** Em regra, o provedor de hospedagem não é responsável pelo conteúdo das informações que exibe na rede, salvo se, verificada a ocorrência de ato ilícito, se recusar a identificar o ofensor ou interromper o serviço prestado ao agente. Isso porque não há que se falar em dever legal do provedor de fiscalizar as ações de seus usuários. Destarte, a responsabilidade civil do provedor de hospedagem é regida pelas normas do Código Civil, afastando-se a aplicação da lei de imprensa. - A sentença destituída de fundamentação é nula de pleno direito, por faltar-lhe um dos requisitos indispensáveis, insculpidos no art. 485 do CPC. Todavia, o fato de a fundamentação ser exposta de forma concisa não macula a decisão. - Não se pode perder de vista que, além de inexistir norma que impute ao provedor de hospedagem o dever legal de monitoramento das comunicações, esse procedimento seria inviável do ponto de vista jurídico, pois implicaria fazer letra morta da garantia constitucional de sigilo (art. 5º, XII da CF/88). TJMS Apelação Cível N° 1.0105.02.069 961-4/001 – Rel. Des. ELPÍDIO DONIZETTI. Julgado 18.11.08. (grifos nosso)

Deste modo, é fácil perceber que a jurisprudência reconhece os contratos de locação de espaço eletrônico como prova, ainda que não sejam previstos em lei.

Nos contratos de comercio eletrônico, aqueles em que o consumidor realiza uma compra ou a contratação de um serviço pela internet, a jurisprudência tem entendido que se trata de um contrato de natureza informal e como tal não se exige forma prescrita em lei, conforme preceitua o art. 104 do Código Civil que trata da validade do negocio jurídico.

A mesma também tem afastado a assinatura como condição indispensável para validade do contrato de comércio eletrônico, uma vez que nessa espécie de contrato é possível aferir a autenticidade através de outros indícios na contratação, como: o fato do contratante ter acessado a site e disponibilizado seus dados no cadastramento; ter em sua posse o código de adesão que geralmente é fornecido ao finalizar a contratação; a utilização de cartões de credito (“dinheiro de plástico”) na contratação, entre outros.

> AÇÃO COBRANÇA - PRESTAÇÃO DE SERVIÇOS EDUCACIONAIS - MENSALIDADES - **CONTRATO ELETRÔNICO** - RELAÇÃO JURÍDICA DEMONSTRADA. **o contrato de prestação de serviços educacionais é informal e não exige forma prescrita em lei, de maneira que o instrumento contratual firmado por meio eletrônico é apta a demonstrar a relação jurídica entre as partes.** TJMS Apelação Cível N°0024.06.132216-0/002 – Rel.:. Des. NICOLAU MASSEL LI. Julgado 19.12.07. (grifos nosso)
>
> AÇÃO DE COBRANÇA - MENSALIDADE ESCOLAR - **CONTRATO DE PRESTAÇÃO DE SERVIÇOS FIRMADO VIRTUALMENTE** -

> POSSIBILIDADE. **- Desde que não haja prova em contrário, o documento ELETRÔNICO possui força probante suficiente, conforme se extrai do art. 383, do Código de Processo Civil. Portanto, não há que se falar em ausência da relação jurídica firmada entre as partes, por faltar assinatura de próprio punho das partes contratantes.** Além do mais, o documento de fls. 16 demonstra que os serviços contratados pelo apelado lhe foram prestados. TJMS Apelação Cível N° 1.0024.08.060388-9/001 – Rel. Des. NICOLAU MASSELLI. Julgado 16.09.10. (grifos nosso)

Destarte, com base no artigo 104 do Código Civil, que trata da validade do negocio jurídico, somado aos artigos 225 do Código Civil e 383 do Código de Processo Civil, que atribuem validade e eficácia a prova eletrônica, a jurisprudência tem entendido que os documentos eletrônicos gozam de valor probante, ainda que os mesmos não estejam assinados eletronicamente. Entendendo, que devido a aspectos específicos do contrato eletrônico, a sua autenticidade e integridade podem ser garantidas através da analise das circunstâncias que orbitam os fatos.

Por derradeiro, ao analisar alguns meios probatórios como o a foto digital, correio eletrônico e o contrato eletrônico, fica fácil perceber que a jurisprudência hodierna tem atribuído força probante aos documentos digitais, ainda que não estejam acompanhados de técnicas de segurança como a criptografia, assinatura digital, certificação, entre outras. Tal decisão está fulcrada na aplicação da legislação existente que amplia o conceito de prova, bem como nas características do meio eletrônico que requer um não engessamento do conceito de autenticidade e confiabilidade das provas.

## 8. CONCLUSÃO

Para aqueles que não acreditam na validade e eficácia da prova digital o discurso está pautado na falta de uma legislação especifica acerca da matéria ou pela dificuldade em garantir confiabilidade ao meio digital.

De certo que a falta de uma legislação especifica sobre o meio digital dificulta o tratamento dado pelos operadores do direito a matéria. Contudo, não deve servir como pretexto para a sua inércia, uma vez que a própria Constituição da República veda tal omissão através do princípio da inafastabilidade do judiciário.

A não tipificação da prova digital, não pode servir como justificativa para a omissão dos julgadores na hora de valorá-las. Destarte, não podemos atribuir a validade e eficácia da prova, a sua tipificação. Pois, desta forma, estaríamos engessando a possibilidade do

sujeito garantir a veracidade de determinado fato ou ato, carente de comprovação, e com isso suprimir a sua tutela jurisdicional.

Sem contar que o próprio Código de Processo Civil em seu bojo, foi bem claro em atribuir validade as provas atípicas em conformidade com o direito, bem como em estabelecer outros meios probatórios como no caso das reproduções mecânicas e fotográficas, corroborando a existência de um rol de provas meramente exemplificativo (*numerus apertus*).

Ainda que se entenda que o Código de Processo Civil trouxe um rol taxativo (*numerus clausus*) de meios probatórios validos. Deve-se ampliar o conceito de documento (sentido *lato sensu*), buscando a sua verdadeira etimologia. Onde, documento seria todo aquele meio que tem o condão de documentar um fato para posterior comprovação. Perceba que com esse entendimento ontológico, tanto os documentos cartáceos quanto os documentos digitais, são meios probatórios validos.

Destarte, quanto a questão da falta da tipicidade dos documentos digitais, por tudo que foi dito, a mesma já se encontra superada, deste modo, não há que se retirar o valor probante das provas digitais.

Quanto aos requisitos de validade da prova eletrônica deve se imputar a presunção da autenticidade (autoria) e integridade (conteúdo) imposta pelo Código de Processo Civil, onde todo meio probatório que esteja em conformidade com o direito deve ter a sua legitimidade presumida, uma vez que o mesmo não faz qualquer distinção acerca da prova eletrônica e a tradicional.

Ademais, em caso de dúvida quanto a falsidade ou ilegitimidade da prova, seja ela eletrônica ou tradicional, o magistrado pode de oficio ou a requerimento das partes, estabelecer um perito técnico para avaliar a sua legitimidade. Nesse caso podemos trazer como exemplo: a perícia de uma prova tradicional através de um exame grafotécnico ou grafológico; enquanto na prova digital a analise pericial de um computador recém formatado.

No que pese a existência da presunção de validade das provas digitais, também foram desenvolvidas técnicas de segurança para aumentar a confiabilidade da prova eletrônica e consequentemente a sua eficácia. Tais técnicas como criptografia, assinatura digital, certificação, entre outras, são responsáveis pelo grau de excelência a que se chegou a segurança na transmissão de dados na atualidade. Destarte, aplicando as técnicas e seguindo corretamente as diretivas de segurança digital, garante-se uma maior

confiabilidade das provas, excluindo assim a necessidade de perícia em caso de dúvida quanto a sua legitimidade.

A jurisprudência vem tratando da matéria com um olhar mais voltado para as circunstâncias do caso concreto, realizando uma interpretação menos literal dos dispositivos e ampliando o conceito de prova e seu alcance.

Foi visto em alguns julgados, que o contrato realizado através do comércio eletrônico será valido e produzirá efeitos probatórios, ainda que não exista assinatura, pois sua autenticidade será corroborada pelas circunstâncias da contratação. Visto também que o Código Civil quando trata da validade do negócio jurídico estabelece como regra que a sua forma será livre com a exceção prevista em lei, deste modo, sendo o contrato eletrônico uma forma livre e valida de contratação.

Com relação a foto digital, foi desmistificada a idéia de que a mesma não produz eficácia probatória, pois segundo entendimento, o Código de Processo Civil apenas atribuiria validade as fotos geradas através de negativos. Assim, a jurisprudência não só reconheceu o seu uso nas perícias técnicas e sensores de limitação velocidade do trânsito, bem como a sua validade na comprovação de crimes e danos na esfera civil.

Da analise jurisprudencial do trabalho, percebe-se a todo o momento a aplicação do sistema de valoração do livre convencimento motivado, onde o magistrado com base em sua convicção tem a liberdade para valorar determinada prova, em contrapartida, devendo sempre fundamentar a sua decisão, sob pena nulidade.

Para que a maioria dos operadores do direito possa reconhecer a validade e eficácia da prova eletrônica será necessário extirpar o pré-conceito que se tem em relação as provas digitais, haja vista que as questões de falta de uma legislação especifica e dúvida quanto a confiabilidade do meio digital, podem ser facilmente contornadas conforme alhures.

Por tudo que foi exposto no presente trabalho, fica fácil vislumbrar que as provas digitais possuem o mesmo valor probante que as provas tradicionais. Devendo o operador do direito se despir do seu preconceito e se utilizar do seu posconceito acerca das provas digitais.

Destarte, a solução mais adequada para a questão do pré-conceito está na disseminação do conhecimento acerca do tema. Pois, como já diria o filósofo: “A ignorância atrai desgraça”.

O direito a prova corolário da Magna Carta, tradutor espontâneo dos fatos jurídicos, garantidor do acesso a justiça e da inafastabilidade do judiciário. A tutela jurisdicional somente pode ser totalmente alcançada com o respeito à prova, seja ela de natureza

corpórea ou incorpórea, pois deste modo garantiremos o contraditório e ampla defesa na sua plenitude.

**REFERÊNCIAS**


ABRÃO, Carlos Henrique. **Processo Eletrônico.** 2. Ed. São Paulo: Editora Revista dos Tribunais LTDA, 2010.

BRASIL. Novo Código Civil Brasileiro. Disponível em: <www.planalto.gov.br> Acesso em: 15 out. 2010.

BRASIL. Código de Processo Civil. Disponível em: <www.planalto.gov.br> Acesso em: 15 out. 2010.

BRASIL. Informatização do Processo Eletrônico. Lei nº 11.419, de 19/12/2006. Disponível em: <www.planalto.gov.br>. Acesso em 15 out. 2010.

BRASIL. Infra-Estrutura de Chaves Públicas Brasileira (ICP-BRASIL).Medida Provisória nº 2.200-2, de 24/08/2001. Disponível em: <www.planalto.gov.br>. Acesso em 15 out. 2010.

BRASIL. Projeto de Lei nº 4.906-A do Senado Federal de 2001. Disponível em: <www.planalto.gov.br>. Acesso em 15 out. 2010.

BRASIL. Projeto de Lei nº 1.589 da Câmara Federal de 1999. Dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e dá outras providências. Disponível em: <www.camara.gov.br>. Acesso em 15 out. 2010.

BRASIL. Projeto de Lei nº 672 do Senado Federal de 1999. Disponível em: <www.planalto.gov.br>. Acesso em 15 out. 2010.

BRASIL. TRIBUNAL DE JUSTIÇA DO RIO DE JANEIRO. Apelação Cível nº 1999.001.15076, Relator: Des. Roberto Wider, Quinta Câmara, julgamento 07/12/1999. Disponível em: <http://www.tjrj.jus.br/scripts/weblink.mgw>. Acesso em: 10 jul. 2010.

_____TRIBUNAL DE JUSTIÇA DO RIO DE JANEIRO. Apelação Cível nº 0043811-90.2009.8.19.0001, Relator: Des. Marcos Alcino A.Torres, Quinta Câmara, julgamento 22/07/2010. Disponível em: <http://www.tjrj.jus.br/scripts/weblink.mgw>. Acesso em: 10 jul. 2010.

_____TRIBUNAL DE JUSTIÇA DO RIO DE JANEIRO. Apelação Cível nº 0013070-54.2007.8.19.0028, Relator: Des. Gabriel Zefiro, Décima Terceira Câmara, julgamento 21/07/2010. Disponível em: <http://www.tjrj.jus.br/scripts/weblink.mgw?MGWLPN=JURIS&LAB=CONxWEB&PORTAL=1&PORTAL=1&PGM=WEBPCNU88&N=201000139905&Consulta=&CNJ=0013070-54.2007.8.19.0028>. Acesso em: 10 set. 2010.

_____TRIBUNAL DE JUSTIÇA DE MINAS GERAIS. Apelação Cível nº 0024.06.132216-0/002, Relator: Des. Nicolau Masselli, Terceira Câmara, julgamento 19/12/2007. Disponível

em:
<http://www.tjmg.jus.br/juridico/jt_/inteiro_teor.jsp?tipoTribunal=1&comrCodigo=439&ano=6&txt_processo=49225&complemento=1&sequencial=0&palavrasConsulta=contrato%20eletronico&todas=&expressao=&qualquer=&sem=&radical=>. Acesso em: 25 set. 2010.

_____SUPERIOR TRIBUNAL DE JUSTIÇA. Recurso Especial nº 617121/RJ – Rio de Janeiro, Relator: Ministro Gilson Dipp, Quinta Turma, julgamento 09/02/2005. Disponível em:<http://www.stj.jus.br/SCON/jurisprudencia/toc.jsp?tipo_visualizacao=null&processo=617221&b=ACOR>. Acesso em: 10 jul. 2010.

CÂMARA, Alexandre Freitas. **Lições de Direito Processual Civil.** 19. Ed. Rio de Janeiro: Editora Lumen Juris, 2009.

DIDIER JR, Fredie. BRAGA, Paula Sarno. OLIVEIRA, Rafael. **Curso de Direito Processual Civil.** 3. Ed. Salvador: Editora Juspodium, 2009.

GRAU, Eros Roberto. **Ensaio e discurso sobre a interpretação/aplicação do Direito**. São Paulo: Malheiros, 2002.

LAGO JR., Antônio. **Responsabilidade Civil por Atos Ilícitos na Internet**. São Paulo: Editora LTR, 2001.

LEAL, Sheila do Rocio Cercal Santos. **Contratos Eletrônicos.** 1. Ed. São Paulo: Editora Atlas S.A, 2009.

MAIA, Álvaro Marcos Cordeiro. **Disciplina Jurídica dos Contratos Eletrônicos no Direito Brasileiro**. Recife: Editora Nossa Livraria, 2004.

MARINONI, Luiz Guilherme. ARENHART, Sérgio Crus. **Processo de Conhecimento**. 7. Ed. Rio de Janeiro: Editora Revista dos Tribunais, 2008.

MARQUES, Antônio Terêncio G. L. **Direito Constitucional e Teoria da Constituição.** 5. Ed. Curitiba: Juruá Editora, 2010.

ONU. Lei Modelo da Uncitral sobre o Comércio Eletrônico. Resolução 51/162, de 16/12/1996. Disponível em: < http://www.lawinter.com/1uncitrallawinter.htm>. Acesso em 15 out. 2010.