POSSIBILIDADE JURÍDICA DA CONTESTAÇÃO DA ASSINATURA DIGITAL*

Claudio Felipe Alexandre Magioli Núñez**

RESUMO: O artigo estuda a possibilidade jurídica da contestação da assinatura digital, bem como o regime jurídico e a distribuição do ônus probatório no incidente de verificação de autoria do documento eletrônico impugnado. O não repúdio, sendo conceito técnico de criptografia, é apenas uma presunção *hominis*, não sendo presunção legal. Um documento assinado digitalmente não é um documento com firma reconhecida por tabelião, capaz de inverter o ônus para que o impugnante tenha que provar que não subscreveu o documento. Há um descompasso entre os pressupostos da legislação e a técnica de subscrição mediante assinatura digital, justamente pela legislação estar fundada na possibilidade das assinaturas autógrafas serem periciáveis grafotecnicamente, fato impossível no caso da assinatura digital. Uma das possíveis soluções seria uma nova norma para criar a presunção legal de recondução do uso da assinatura digital pelo seu titular.

PALAVRAS-CHAVE: Assinatura digital. Contestação de assinatura. Incidente de verificação. Presunção legal. Ônus probatório.

Introdução

O presente artigo pretende trazer uma reflexão sobre a possibilidade jurídica da contestação da assinatura digital dentro da Infraestrutura de Chaves Públicas (ICP-Brasil).

A propriedade de não repúdio, que impede que o emissor de uma mensagem negue a sua autenticidade, parece ter resolvido definitivamente a questão de transações à distância entre partes que não se conhecem. O não repúdio evitaria que uma das pessoas, após a transação, afirmasse que não a tinha celebrado. Portanto, o não repúdio é utilizado para se estabelecer uma presunção absoluta ou relativa em desfavor do titular do par de chaves pública/privada. Para aqueles que defendem que o não repúdio gera uma presunção absoluta, tal entendimento impossibilitaria a contestação das assinaturas digitais. Por outro lado, há aqueles que defendem que o não repúdio significaria uma presunção relativa, estabelecendo ônus para o titular do par de chaves pública/privada provar que não subscreveu o documento assinado digitalmente (uso abusivo da chave privada).

Porém, nenhuma das soluções se harmoniza com a ordem jurídica brasileira à luz da equivalência funcional. O não repúdio, sendo conceito técnico de criptografia, é apenas uma presunção *hominis*, não é presunção legal. Presunções decorrem da lei, e não de propriedades técnicas. Aceitar que o não repúdio gera um ônus para o titular do par de chaves pública/privada seria conceder ao documento assinado digitalmente o mesmo tratamento jurídico de um documento com firma reconhecida por tabelião.

* Enviado em 27/9, aprovado em 19/11, aceito em 16/12/2013.

** Mestrando em Direito e Políticas Públicas – UNIRIO; Pós-Graduado em Direito da Tecnologia da Informação – UCAM; Pós-Graduado em Direito Público – UGF. Faculdade de Direito, Pós-Graduação. Rio de Janeiro, Rio de Janeiro, Brasil. E-mail: cfamnunez@gmail.com.

Atualmente, podemos constatar um descompasso entre os pressupostos da legislação e a técnica de subscrição mediante assinatura digital, justamente pela lei processual estar fundada na possibilidade fática de as assinaturas autógrafas serem periciáveis grafotecnicamente, fato impossível no caso das assinaturas digitais.

Mas se o não repúdio não impede que uma assinatura digital possa ser contestada, possibilitando a contestação da assinatura digital, qual seria o regime jurídico aplicável? Como se daria a distribuição do ônus probatório na contestação da assinatura digital? São estas questões que iremos discorrer no presente artigo.

1 Autoria, subscrição, autenticidade e o documento eletrônico

O documento tem três elementos que o formam: autoria, conteúdo e suporte (DIDIER JR.; BRAGA; OLIVEIRA, 2009, p. 147-153). Quando tratamos de documentos eletrônicos, o elemento suporte nem sempre se manifestará da mesma forma, sendo substituído por um conceito lógico cujo objetivo é manter a integridade do documento.

O autor de um documento é aquela pessoa a quem se atribui a formação do documento. A autoria de um documento pode ser subdividida em autoria material e autoria intelectual. Autoria material é atribuída àquela pessoa que criou o meio ou suporte do fato que está sendo representado. Já a autoria intelectual é atribuída à pessoa a mando de quem essa criação foi feita. Assim, se eu redijo e datilografo a carta, ou se faço que a carta seja redigida e datilografada por meu secretário, eu serei o autor intelectual em ambos os casos. Porém, não basta que a autoria esteja indicada no documento. É necessário que a autoria seja provada. E a forma de se provar a autoria de um documento é uma questão de previsão legal. A lei deve estabelecer como se prova a autoria de um documento (DIDIER JR.; BRAGA; OLIVEIRA, 2009, p. 147).

A subscrição é a aposição de um sinal exclusivo que identifica o autor do documento (DIDIER JR.; BRAGA; OLIVEIRA, 2009, p. 149). A forma mais comum de subscrição é a aposição da assinatura autógrafa ao pé de um documento, ou seja, assinar de forma manuscrita um documento em papel. A subscrição é importante porque não só indica o autor do documento como também torna presumível que a declaração contida no documento foi desejada pelo autor. Apesar de praticamente se considerar subscrição como sinônimo de assinatura, a subscrição mediante assinatura autógrafa não é a única forma de identificação da autoria de um documento. Por exemplo, pode-se considerar como subscrição a autenticação mecânica lançada pelas instituições bancárias ao pé do boleto representativo da dívida, e que corresponde à sua declaração de recebimento, na data indicada, do valor ali informado (DIDIER JR.; BRAGA; OLIVEIRA, 2009, p. 149).

A subscrição tem dupla função: indicativa e declarativa. A função indicativa tem a ver com o fato de ser a subscrição que aponta o autor do documento, enquanto a função declarativa consiste no fato de que quem subscreve um documento assume sua paternidade e seu conteúdo (MARINONI; ARENHART, 2005, p. 371-372). Há autores, como Francesco Carnelutti, que entendem que a subscrição é elemento essencial à própria existência do documento (DIDIER JR.; BRAGA; OLIVEIRA, 2009, p. 150). Há, na doutrina estrangeira, entendimento de que há impossibilidade de se conceder efeitos jurídicos

aos documentos eletrônicos pelo simples fato de estes não poderem ser assinados de forma manuscrita:

> Por outro lado, mesmo sendo possível considerar um documento eletrônico como um documento escrito, não se pode nunca presumir o valor de "escritura privada". Requisito essencial da escritura privada é a assinatura, isto é, a imposição do nome e sobrenome por parte da pessoa de quem prove as declarações que formam o texto escrito. [...] Devemos, portanto, distinguir claramente entre o valor jurídico do documento escrito da do valor jurídico da "escritura privada" e reconhecer ao documento eletrônico o sentido estrito de valor de documento escrito e não de uma escritura privada justamente pela impossibilidade do ato de subscrição pessoal. (GIANNANTONIO, 1991, p. 113 apud MARCACINI, 2010, p. 79, tradução nossa)[1]

Nesse entendimento, os documentos eletrônicos não poderiam ser considerados documentos simplesmente pelo fato de não poderem ser subscritos. Mas este não é o entendimento da doutrina nacional, tampouco de nossa legislação. A lei reconhece como documentos, ainda que não assinados, aqueles que pela experiência comum não se costumam assinar como os livros comerciais e assentos domésticos (art. 371, III, CPC), o testamento militar (art. 1.893, CC) e a nota escrita pelo credor, ainda que não assinada, no corpo do documento representativo da obrigação (DIDIER JR.; BRAGA; OLIVEIRA, 2009, p. 150).

Importa observar que, nos casos de documentos não assinados, outras formas de se comprovar a autoria do documento devem ser realizadas para que se empreste eficácia jurídica ao documento: prova testemunhal, admissão ou confissão da obrigação pelo devedor e perícia grafotécnica nos casos de manuscritos.

Portanto, concluímos que a autoria é elemento essencial do documento, ou seja, não existe documento sem autor. A subscrição é apenas uma técnica para se atribuir a autoria do documento e que, em regra no direito brasileiro, concederá eficácia jurídica ao documento: sem assinatura autógrafa, em regra, o documento existe, mas não tem eficácia probatória. Logo, os documentos eletrônicos têm existência jurídica, e sua eficácia probatória dependerá da técnica a ser utilizada para a atribuição de autoria. Ademais, como afirmado anteriormente, é a lei que estabelece a forma de se comprovar a autoria. No caso dos documentos eletrônicos, é a Medida Provisória nº 2.200-2/2001 que regula a matéria, que, veremos em seguida, acaba por remeter ao regime geral das provas documentais do CPC.

Outro ponto importante é o conceito de autenticidade. A autenticidade de um documento diz respeito à coincidência entre o autor aparente do documento e o seu autor real. Ou seja, se a técnica utilizada para identificar o autor indica, de fato, o autor real do documento analisado (DIDIER JR.; BRAGA; OLIVEIRA, 2009, p. 150). Essa prova de coincidência entre autoria aparente e autoria verdadeira, o que tornará o documento autêntico, é realizada nos termos da lei e depende de alguns fatores, como a natureza do documento (particular ou pública) e a técnica utilizada para indicação de autoria (subscrição ou documentos não assinados). O ônus probatório, como veremos, é definido em lei. Também será o tipo de prova requerida, especialmente nos casos de assinatura autógrafa em que se exige perícia grafotécnica.

2 Conceitos de criptografia, assinatura eletrônica e assinatura digital

Criptografia é uma ciência que se dedica a proteger uma mensagem tornando seu conteúdo ininteligível (COUTINHO, 2011, p.1). A criptografia divide-se em dois grandes grupos: códigos e cifras. As cifras, por sua vez, podem caracterizar-se em dois tipos básicos de transformação: transposição e substituição (TKOTZ, 2005, p. 21). As cifras de transposição apenas trocam as posições originais dos caracteres; enquanto as cifras de substituição alteram os caracteres originais (TKOTZ, 2005, p. 22). Cada cifra é formada por um algoritmo e uma chave. Um algoritmo é um método geral de codificação, sendo que a chave especifica os detalhes exatos de uma codificação em particular (SINGH, 2003, p. 27). Cifrar uma mensagem é usar um algoritmo (método geral) juntamente com uma chave (informações específicas) para tornar uma mensagem ininteligível.

Usualmente, diz-se que a criptografia pode ser simétrica (convencional) ou assimétrica. A criptografia se diz simétrica quando o emissor e o receptor de uma mensagem cifrada utilizam da mesma chave para cifrar e decifrar uma mensagem. Durante séculos, a humanidade empregou unicamente essa técnica, em que as partes legítimas envolvidas na transmissão de uma mensagem secreta deveriam compartilhar da mesma chave secreta para poderem ter acesso à mensagem criptografada (VOLPI, 2001, p. 8). Assim, num sistema de criptografia simétrica, o processo de decifragem é simplesmente o oposto da cifragem (SINGH, 2003, p. 294).

A criptografia simétrica apresenta algumas desvantagens: a) os interlocutores precisam encontrar um canal seguro antes do início da comunicação, já que há a necessidade de troca da chave secreta entre o emissor e receptor; b) para cada par de emissor-receptor, há necessidade de uma chave secreta para que se garanta a confidencialidade, de forma com que cada pessoa precise gerenciar um número enorme de chaves; c) o uso da chave secreta, comum ao emissor-receptor, não consegue garantir a autoria da mensagem.

Já na criptografia assimétrica, a chave de cifragem e a chave de decifragem são diferentes (SINGH, 2003, p. 294). O importante é observar que há uma relação de complementaridade entre as chaves privada e pública, de forma que, cifrando uma mensagem com uma das chaves, só se consegue decifrar uma mensagem com a outra. Assim, se é cifrada uma mensagem com a chave pública, somente a sua chave privada será capaz de decifrar a mensagem. Esse é o procedimento que normalmente ocorre quando se quer criptografar uma mensagem.

O processo de assinatura digital utiliza-se dessa propriedade das chaves assimétricas. Assim, quando o remetente cifra a mensagem com a sua chave privada, o destinatário deve utilizar a chave pública do remetente para decifrá-la. Como, em tese, somente o titular da chave privada tem o conhecimento dela, o destinatário da mensagem pode ter certeza de que a mensagem foi enviada por quem tem posse da chave privada, uma vez que ela foi conferida com a chave pública do remetente.

Na prática, não é a mensagem inteira que é cifrada com a chave privada. É que a criptografia assimétrica apresenta uma desvantagem: a sua complexidade faz com que

os computadores demorem em cifrar a mensagem. Dessa forma, utiliza-se um algoritmo, denominado *hash*, para se obter um resumo (*message digest*) da mensagem a ser enviada. Logo, o que realmente é cifrado pela chave privada é o resultado do *hash* (resumo), e não o inteiro teor da mensagem (VOLPI, 2001, p. 22). Portanto, podemos afirmar que assinar digitalmente um documento consiste em cifrar o *message digest* com a chave privada (MENKE, 2005, p.47).

Há de se distinguir a assinatura digital da assinatura eletrônica: a relação é de espécie e gênero. Ou seja, qualquer mecanismo eletrônico utilizado para a identificação de um autor é considerado como assinatura eletrônica. O mecanismo mais comum é simplesmente atribuir um nome de usuário único (*login*) e uma senha (*pin*) pessoal, intransferível e que deve permanecer em sigilo absoluto para ser eficaz. A assinatura eletrônica não se utiliza necessariamente da criptografia assimétrica (que, nesse caso, seria a espécie assinatura digital) e, portanto, é mais insegura em termos tecnológicos (PINHEIRO, 2008, p. 17-18; ATHENIENSE, 2010, p. 111; MENKE, 2005, p. 42-43). Lembremos que o uso de cartão de crédito ou débito com senhas é um exemplo corriqueiro de utilização de assinatura eletrônica. No presente artigo, daremos maior atenção à assinatura digital justamente por ser tida como a mais confiável. Sendo juridicamente possível a contestação da assinatura digital, também será possível contestar qualquer assinatura eletrônica.

3 Assinatura autógrafa e assinatura digital: similitudes, diferenças e equivalência funcional

Vejamos as similitudes e diferenças das assinaturas autógrafa e digital para, em seguida, entendermos o conceito de equivalência funcional.

Todos estão bem familiarizados com a assinatura manuscrita (também conhecida como autógrafa, quirógrafa ou halógrafa), uma vez que é do cotidiano assinar documentos dos mais variados tipos. Mas bem poucos estão conscientes do que realmente uma assinatura autógrafa representa: no ato da subscrição autógrafa, registra-se uma informação que cria um elo personalíssimo entre o registro gráfico e a pessoa que a lançou no documento em papel. Portanto, a assinatura autógrafa é sempre individualizada, mas não há necessidade de que seja legível, ou seja: que se possa ler o nome inteiro da pessoa que assina. Assim, o que realmente particulariza uma assinatura e torna possível identificar seu titular é a forma de grafar os caracteres (morfologia) e outros dados característicos como gênese, pressão e remates, sendo irrelevante se a assinatura contém o nome completo da pessoa (MARINONI; ARENHART, 2005, p. 371).

Foge ao escopo deste trabalho apresentar as técnicas pelas quais os peritos grafotécnicos conseguem identificar o titular de uma assinatura autógrafa, mas iremos apresentar alguns conceitos básicos sob os quais se assentam esta ciência. A grafoscopia é uma ciência que trata do exame minucioso e do reconhecimento do grafismo, objetivando a busca da autenticidade e autoria do registro gráfico aposto nos documentos. Assenta-se em dois postulados gerais: a) "O grafismo é individual e inconfundível" e b) "As leis da escrita são independentes dos alfabetos utilizados" (FALAT, 2010, p. 91-92). Edmond Solange Pellat, perito francês, foi responsável por estabelecer as quatro leis do grafismo (MONTEIRO, 2008, p. 19). Com base nessas leis, é possível fazer a análise do grafismo

registrado no documento pelo estudo de certos elementos como a imagem (forma do grafismo), espontaneidade (naturalidade na execução do lançamento da escrita), dinâmica (registros de pressão e velocidade) e outras informações complementares como ataques e remates (início e término da escrita), tendência do punho (traços curvos ou angulosos) e fechamento dos gramas circulares. Dessa forma, assim como as pessoas podem ser reconhecidas pela sua maneira de andar, falar e gesticular, elas também podem ser identificadas pelo seu registro gráfico (FALAT, 2010, p. 92-99).

Assim, ao subscrever com assinatura autógrafa um documento em papel, estamos registrando, no próprio corpo do documento, informações biométricas comportamentais do seu autor, estabelecendo um liame personalíssimo entre o ato de subscrição e o próprio documento. A assinatura autógrafa é um meio de identificação biométrica, uma vez que registra características comportamentais únicas (singulares) de um indivíduo (PINHEIRO, 2008, p. 61).

Já na subscrição por meio da assinatura digital, não há esse liame subjetivo no ato de subscrição: basta conhecer a chave privada para que se assine digitalmente. Portanto, qualquer um que esteja de posse da chave privada pode assinar em nome de outra pessoa, sem que isso deixe vestígios. A assinatura digital não registra informações biométricas de quem subscreve o documento eletrônico. É nesse fato que reside a maior diferença entre a assinatura autógrafa e assinatura digital.

É aqui que surge o conceito de equivalência funcional. Apesar de as assinaturas digital e autógrafa serem distintas de fato, a lei as equipara como se fossem iguais. Assim, pela equivalência funcional, atribuem-se dois efeitos à assinatura digital: a) cumprir os mesmos requisitos formais da assinatura manuscrita; b) torná-la admissível como meio de prova com os mesmos efeitos processuais da assinatura autógrafa (MENKE, 2005, p. 142). No Brasil, também se adotou a equivalência funcional (art. 10, § 1º, da Medida Provisória nº 2.200-2/2001), de maneira que as assinaturas digitais e autógrafas, ainda que distintas de fato, sejam equivalentes para todos os efeitos jurídicos.

4 O conceito de não repúdio

Devemos analisar o conceito de não repúdio. Dependendo dos efeitos jurídicos que se queira dar ao conceito de não repúdio, será sempre impossível a impugnação da assinatura digital. Mas será que isso é realmente verdadeiro e possível no Direito brasileiro?

Segundo a definição de Silva (2004, p. 39) "o não repúdio evita que um dos participantes da comunicação negue que esta tenha ocorrido". Portanto, o autor apresenta um conceito técnico referente ao não repúdio. Só que, mais adiante em seu texto, o mesmo autor traz à baila uma consequência jurídica desse conceito:

> O não repúdio acontece quando uma determinada mensagem eletrônica, seja de que teor for, adquire força de "aceitação" e efeitos jurídicos concretos, sem possibilidade de uma das partes alegar que não participou do negócio. Isto quer dizer que o não repúdio é uma cláusula que, inserida no contrato, desde que esteja cercado da devida segurança, *torna impossível anular um contrato alegando a insegurança dos meios de comunicação [...] O que o não repúdio traz de novo é quase*

> *um seguro contra a alegação de que o negócio não foi feito e a certeza de que se houver uma disputa judicial, a cláusula será uma garantia para as partes* (SILVA, 2004, p. 39-40, grifo nosso)

Em suma, o autor apresenta o não repúdio como um conceito técnico, mas com uma consequência jurídica: uma cláusula contratual para evitar a impugnação de um negócio jurídico eletrônico. Assim, a questão realmente se torna confusa, porque o conceito de não repúdio nasceu como uma propriedade técnica da criptografia, e, por aparente influência lobista de empresas norte-americanas, procurou-se conceder um significado jurídico à expressão técnica: "Isto é importante principalmente por causa do termo 'não repúdio'. Tal como o termo 'confiável', este termo é tomado a partir da literatura acadêmica sobre criptografia. Significa algo muito específico: que o algoritmo de assinatura digital não pode ser quebrado. Portanto, um terceiro não pode forjar sua assinatura" (ELLISON; SCHNEIER, 2000, p. 2, tradução nossa).[2]

Portanto, o conceito de não repúdio nasceu como um conceito puramente técnico da área de criptografia, significando apenas que um algoritmo criptográfico é inquebrável, o que impossibilita que um terceiro (estranho ao processo de comunicação segura) seja capaz de forjar uma assinatura digital falsa.

No entanto, como os próprios autores acrescentam, a indústria da Infraestrutura de Chaves Públicas conseguiu estender esse conceito para a esfera jurídica, inclusive através de *lobby*, no sentido de se criarem leis que garantam que um documento assinado digitalmente jamais possa ser juridicamente impugnado:

> Foram os fornecedores de ICP que blindaram o termo não repúdio, emprestando um sentido legal, mediante *lobby* para que se aprovassem leis com intuito de que se alguém usar a sua chave privada de assinatura, então não terá como repudiar a assinatura. Em outras palavras, em algumas leis de assinatura digital (por exemplo, Utah e Washington), se a sua chave de assinatura foi certificada por uma Autoridade Certificadora (AC), então você é responsável por tudo o que a chave privada faz. Não importa quem estava no teclado do computador ou se um vírus utilizou a sua assinatura digital: você será legalmente responsável (ELLISON; SCHNEIER, 2000, p. 2).[3]

No mesmo sentido de reconhecer o não repúdio apenas como um conceito técnico e não jurídico:

> Os termos não repúdio e repúdio, a princípio, são estranhos ao direito contratual dos países de tradição romano-germânica. [...] Warwick Ford e Michael S. Baum, na obra *Secure Electronic Commerce – Building the Infrastructure for Digital Signatures and Encryption* observam que nos países da *common law* o termo *repudiation* está associado ao direito contratual. [...] Por outro lado, o termo *non-repudiation* já faz parte de decisões judiciais nas cortes norte-americanas há mais de 15 anos, apenas com o significado de que uma parte não negou ou não tem a intenção de negar os termos de um contrato ou de uma declaração de vontade. Até hoje, segundo afirmam, o termo *non-repudiation* jamais foi empregado pela jurisprudência norte-americana no sentido que lhe empresta a área de segurança da informação, qual seja, o de atributo de um meio de comunicação específico ou de um mecanismo de segurança da informação, que serve para impedir que a parte negue que uma mensagem específica foi recebida ou enviada. Os autores dividem

> as espécies de não repúdio em não repúdio de origem (que protege o receptor da mensagem, indicando que a mensagem efetivamente se originou do declarante), não repúdio de envio (que protege o declarante, comprovando que a mensagem foi efetivamente transmitida) e não repúdio de recebimento (que também protege o declarante, comprovando que a mensagem foi efetivamente recebida pelo destinatário). (MENKE, 2011, p. 13)

Marcos da Costa também fala do não repúdio como um conceito técnico, inclusive criticando o seu uso como um conceito jurídico:

> Prova maior da tendência de se pretender transferir ao titular do certificado emitido no âmbito da ICP-Brasil os riscos de sua emissão, está na afirmação comum de que referidos certificados gerariam o efeito de não repúdio, ou seja, aquele titular não poderia negar ter uma assinatura digital que lhe fosse atribuída. Não repúdio, porém, é uma expressão técnica, que diz respeito à vinculação do par de chaves criptográficas. Bruce Schneier já alertava para a apropriação indevida que a indústria da PKI fez da expressão, para dar a seus produtos algum significado jurídico, por mais absurdo que fosse. (COSTA, 2003, p. 7)

Por fim, apresentamos o conceito de Augusto Marcacini:

> No entanto, é comum repetir-se, sem qualquer reflexão, que assinaturas digitais contariam com a propriedade do "não repúdio", algo como um pó mágico capaz de impedir toda e qualquer discussão acerca da veracidade do documento ou da assinatura digital. Esta expressão, na verdade, era utilizada no jargão técnico-científico para expressar que as operações matemáticas, insistentemente testadas pela comunidade científica, se mostravam inquebráveis; isto é, que a correta decodificação com a chave pública permite irrefutavelmente concluir que esta codificação foi feita por quem tinha a chave privada. Esta é a única verdade matemática que pode ser concluída, não sendo adequado estendê-la a todos os demais fatos que rondam o documento eletrônico. A tentativa de atribuir algum significado jurídico a "não repúdio", patrocinada por quem evidentemente tinha interesse nisso, é um dos grandes mitos que encobrem a certificação eletrônica, e que, corretamente analisado, se mostra um verdadeiro absurdo em uma sociedade democrática, em que não se pode impedir o julgador de valorar as provas acerca dos fatos controvertidos. (MARCACINI, 2003, p. 5)

Portanto, o conceito de não repúdio é uma propriedade de natureza técnica da área de criptografia, significando apenas que o algoritmo da assinatura digital é inquebrável, não havendo possibilidade (matemática) de que um terceiro possa forjar a assinatura digital.

Há, porém, de se lembrar que não há nada que impossibilite, no plano dos fatos, que alguém ou um vírus de computador use a chave privada para assinar um documento digitalmente. Nesse ponto, é sempre bom lembrar que a segurança da informação pode ser comparada a uma corrente formada por quatro elos: infraestrutura, tecnologia, aplicações e pessoas. Além disso, a força dessa corrente será medida pelo seu elo mais fraco que é normalmente o próprio ser humano, haja vista a importância que se atribui à "Engenharia Social", técnica de obtenção de informações através da manipulação dos usuários (pessoas) de um sistema de informação (PINHEIRO, 2008, p. 28-33). Em relação à chave privada, não podemos esquecer que parte desse elo fraco é o armazenamento

e também a senha de acesso à chave privada. Se minha chave privada está armazena no disco rígido (HD) de meu computador, é possível que um vírus possa danificá-la ou entregá-la a terceiros. A escolha de uma senha fraca para o acesso à chave privada, como uma data de aniversário, também pode ser um problema, pois pode ser facilmente descoberta. Nesses casos, de nada adiantará o uso da criptografia assimétrica, pois a força da minha segurança será dada por esses elos fracos. Esses e outros aspectos são abordados pelo Instituto de Tecnologia da Informação, autarquia responsável pela ICP-Brasil, em sítio eletrônico na internet (ITI, 2012).

Concluindo, o não repúdio não apresenta um significado jurídico a ponto de determinar que um documento eletrônico assinado digitalmente seja impossível de impugnação. Mas é possível impugnar um documento eletrônico assinado digitalmente?

5 Possibilidade jurídica de impugnação: contestação de assinatura digital

Em primeiro lugar, a questão poderia ser deslocada para a presunção de autenticidade do documento eletrônico assinado digitalmente. Se considerarmos que um documento eletrônico assinado digitalmente apresente presunção absoluta quanto à sua autoria, nossa resposta seria que é impossível contestar a assinatura digital de um documento eletrônico. Portanto, é importante saber se um documento eletrônico assinado digitalmente contenha presunção absoluta (*juris et de jure*) ou relativa (*juris tantum*).

Atualmente, a Medida Provisória nº 2.200-2/2001 é a norma jurídica nacional que regula a matéria dos documentos eletrônicos, assinaturas digitais e a infraestrutura de chaves públicas no Brasil. Assim reza o § 1º do art. 10: "§ 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" (BRASIL, 2001).

A Medida Provisória faz remissão ao antigo Código Civil de 1916, que, no art. 131, tinha a mesma redação que o art. 219 do atual Código Civil (CC):

> Art. 131. As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários. (BRASIL, 1916)
>
> Art. 219. As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários. (BRASIL, 2002)

Em relação ao Código de Processo Civil (CPC), encontramos a seguinte disposição legal em relação ao tema: "Art. 368. As declarações constantes do documento particular, escrito e assinado, ou somente assinado, presumem-se verdadeiras em relação ao signatário" (BRASIL, 1973).

Portanto, o documento eletrônico assinado digitalmente está juridicamente regulado pelas mesmas disposições dos documentos particulares, tanto no Código Civil quanto no Código de Processo Civil.

Chegamos aqui à resposta para uma das perguntas iniciais: qual o regime jurídico dos documentos eletrônicos assinados digitalmente? É exatamente o mesmo

regime jurídico dispensado aos documentos particulares subscritos mediante assinatura autógrafa (assinatura manuscrita).

Mas ainda resta a seguinte pergunta: o documento eletrônico assinado digitalmente teria presunção absoluta ou relativa? A resposta encontra-se no próprio CPC:

> 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.
>
> Art. 389. Incumbe o ônus da prova quando:
> I - se tratar de falsidade de documento, à parte que a arguir;
> II - se tratar de contestação de assinatura, à parte que produziu o documento. (BRASIL, 1973)

Ou seja, se o documento eletrônico segue o mesmo regime jurídico do documento tradicional, com a possibilidade de se contestar da assinatura autógrafa, também será possível a contestação da assinatura digital. Portanto, trata-se de presunção relativa, já que a fé do documento particular cessa quando lhe é contestada a assinatura, tendo o CPC estabelecido o ônus da prova em cada caso. Podemos afirmar que se trata de presunção relativa (*juris tantum*) justamente porque regula um ônus probatório:

> As presunções legais constituem técnicas para garantir determinados valores em situações específicas. [...] Não se pode deixar de ressaltar, no entanto, que as normas jurídicas estatuidoras das presunções legais se distinguem das demais normas, na medida em que asseguram esses valores mediante a regulação do ônus da prova. Instauram, assim, uma "regra de julgamento", a indicar ao magistrado qual deve ser o conteúdo material da sentença, em determinadas situações específicas. Nesse contexto, o desfavorecido pela presunção suporta o ônus de provar em contrário. E isso de forma totalmente independente de sua posição processual, nada importando o fato de ser autor ou réu. (OLIVEIRA, 2011, p. 14)

Há autores que entendem se tratar de uma presunção relativa no caso das assinaturas digitais:

> O Código estabelece aí uma presunção *juris tantum*, que admite prova em contrário. Enquanto, porém, essa prova não é feita, o documento assinado, seja público ou particular, desde que apresente a forma e a aparência exterior de autenticidade, vale como prova de que, em relação ao signatário. Existe uma declaração de vontade capaz de produzir efeitos jurídicos. (MENKE, 2005, p. 138)
>
> Impedir alguém de negar uma assinatura, digital ou não, é a negação do Estado de Direito. Pode-se regular ônus de prova de quem negar uma assinatura, mas jamais retirar de alguém o direito de impugná-la (COSTA, 2003, p. 7).

Portanto, pela análise da legislação brasileira, chegamos à conclusão de que é possível a contestação da assinatura digital lançada em um documento eletrônico,

uma vez que a Medida Provisória nº 2.200-2, que regula a matéria, remete diretamente para o mesmo e tradicional regime jurídico da presunção de veracidade dos documentos particulares subscritos mediante a assinatura autógrafa. Sendo possível contestar a assinatura autógrafa no documento em papel, também é juridicamente possível contestar a assinatura digital aposta em documento eletrônico.

6 Contestação da assinatura autógrafa: incidente de verificação e *onus probandi*

Como vimos anteriormente, o regime jurídico que regula as assinaturas digitais é exatamente o mesmo das tradicionais assinaturas autógrafas. Portanto, antes de passarmos para o estudo específico das assinaturas digitais, relembremos a doutrina e a jurisprudência sobre a questão do incidente de verificação e da questão do ônus da prova quando da contestação da assinatura autógrafa.

Em primeiro lugar, vejamos o que disciplina o art. 372 do CPC:

> 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.
> Parágrafo único. Cessa, todavia, a eficácia da admissão expressa ou tácita, se o documento houver sido obtido por erro, dolo ou coação. (BRASIL, 1973)

Esse artigo do CPC disciplina o que é chamado na doutrina estrangeira de "reconhecimento de escritura privada", que, no Direito brasileiro, com base na lição de Egas Moniz de Aragão, se chama de "incidente de verificação" (MARINONI; ARENHART, 2005, p. 309). O incidente de verificação trata da impugnação da autenticidade (autoria) e do contexto. Não se deve confundir esse incidente com o incidente de falsidade, uma vez que o conceito de falsidade na esfera processual civil não se confunde com o de falsidade na esfera penal. No Direito Penal, o questionamento sobre a autenticidade ou não de uma assinatura firmada em um documento pertence à seara da falsidade. Já no processo civil, há uma dualidade de institutos, com regimes diversos de instrumentos para arguir se um documento é inautêntico (incidente de verificação) ou falso (incidente de falsidade documental). Assim:

> É forçoso, portanto, concluir que os campos de aplicação do incidente de verificação e o de falsidade documental são distintos (embora possam ambos os incidentes ser oferecidos concomitantemente), sendo inviável o uso de um para a veiculação da matéria relativa ao outro. [...] De toda sorte, pode-se concluir que a função do incidente [de verificação] estudado não é o de arguir qualquer espécie de falsidade do documento impugnado. Ao revés, o objetivo específico desta figura [incidente de verificação] é o de permitir à parte o questionamento da autenticidade da assinatura aposta no documento trazido aos autos, bem assim a veracidade do contexto apresentado pelo mesmo. (MARINONI; ARENHART, 2005, p. 371-372)

Portanto, há distinção entre os dois incidentes: um visa à comprovação da autenticidade (comprovar autoria do documento) e outro, à veracidade (ou falsidade) do documento. É por esse motivo que há uma aparente contradição entre os artigos 387 e 388 do CPC:

> Art. 387. Cessa a fé do documento, público ou particular, sendo-lhe declarada judicialmente a falsidade.
> .....
> Art. 388. Cessa a fé do documento particular quando:
> I - lhe for contestada a assinatura e enquanto não se lhe comprovar a veracidade. (BRASIL, 1973)

Quando cessaria a fé do documento particular impugnado? Somente quando declarada judicialmente a sua falsidade (art. 387) ou no momento da contestação da assinatura (art. 388, I)? Pelo art. 387, o documento particular seria válido enquanto não houvesse uma decisão judicial declarando-o falso. Já pela leitura do inciso I do art. 388, bastaria a impugnação (contestar a assinatura) para negar fé ao documento particular. Para um, a mera impugnação retira a fé do documento; para o outro, é preciso aguardar decisão judicial. Como conciliar essa contradição? A única opção possível é entender o art. 387 do CPC como uma regra geral, em relação à falsidade documental, quando a fé do documento particular só cessa após a declaração judicial de falsidade. Já o inciso I do art. 388 do CPC seria um caso particular, uma regra específica, que contempla apenas os casos de contestação de assinatura; caso no qual a mera impugnação cessa – imediatamente – a fé do documento particular (MARINONI; ARENHART, 2005, p. 395). Dessa forma, conclui-se que o incidente de falsidade se dá quando há adulteração, supressão ou confecção de assinatura no documento.

Em resumo, contestando a assinatura de documento particular, imediatamente cessa a sua fé, até que seja provada a sua autenticidade (sua autoria). Mas de quem é o ônus de provar a autoria do documento cuja assinatura foi contestada? A resposta está inscrita no inciso II do art. 389 do CPC: "Art. 389. Incumbe o ônus da prova quando: [...] II - se tratar de contestação de assinatura, à parte que produziu o documento" (BRASIL, 1973).

Portanto, o *onus probandi* da autoria cabe "à parte que produziu o documento", regra prevista no inciso II do art. 389. Ou seja, quem contestou a assinatura nada precisa provar, pois o documento impugnado não terá força probante até que a parte contrária demonstre a sua autoria real: "Como se tem do inciso I deste artigo, em relação aos documentos particulares, estes perderão a fé se for contestada a assinatura, ficando sua eficácia probante em suspenso até que se lhe comprove a veracidade" (MARINONI; ARENHART, 2005, p. 395).

Porém, ainda pode surgir uma dúvida quanto à redação do inciso II: o que significa "produziu" o documento? Produzir o documento em juízo ou confeccionar o documento? A doutrina nacional entende que o legislador utilizou a expressão "produziu o documento" no seu sentido técnico-jurídico, ou seja: produzir o documento em juízo como uma fase da instrução processual.[4] Há uma razão lógica para o uso técnico da expressão "produziu": o juiz não tem como saber quem realmente confeccionou o documento, podendo ser qualquer uma das partes, até mesmo um terceiro. Portanto, o CPC só pode estar se referindo àquele que produziu o documento em juízo, ou seja, quem apresentou a prova e dela quer se beneficiar (MARINONI; ARENHART, 2005, p. 305).

A jurisprudência do STJ também entende que a expressão "produziu o documento" é usada no sentido técnico, conforme os Embargos de Declaração no Agravo

Regimental no Agravo em Recurso Especial nº 151.216/SP, o Recurso Especial nº 302.469-MG e o Agravo Regimental no Agravo nº 604.033/RJ. Vejamos a ementa dos embargos de declaração mencionados (no Recurso Especial nº 151.216-SP):

> EMBARGOS DE DECLARAÇÃO. AGRAVO REGIMENTAL. AGRAVO EM RECURSO ESPECIAL. EXISTÊNCIA DE OMISSÃO NO ACÓRDÃO EMBARGADO. SANEAMENTO DO VÍCIO QUE IMPLICA ATRIBUIÇÃO DE EFEITOS INFRINGENTES. EMBARGOS À EXECUÇÃO. IMPUGNAÇÃO À AUTENTICIDADE DA FIRMA APOSTA NO TÍTULO EXECUTADO. ÔNUS DA PROVA DA AUTENTICIDADE PERTENCENTE AO EMBARGADO-EXEQUENTE, QUE TROUXE O DOCUMENTO
> 1. A atribuição de efeitos infringentes aos embargos declaratórios é possível nas excepcionais situações em que, sanada a omissão, contradição, obscuridade ou erro material, a alteração da decisão surja como consequência necessária.
> *2. Tratando-se de contestação de assinatura, o ônus da prova da sua veracidade cabe à parte que produziu o documento. A fé do documento particular cessa com a impugnação do pretenso assinante, e a eficácia probatória do documento não se manifestará enquanto não comprovada a sua veracidade.*
> 3. Embargos de declaração acolhidos com efeitos infringentes. Agravo conhecido para se conhecer do recurso especial e dar-lhe provimento (BRASIL, 2013, grifo nosso)

Portanto, podemos concluir que, na contestação da assinatura, a simples impugnação imediatamente cessa a fé do documento particular, e que o ônus da prova da sua autenticidade (isto é, a prova da autoria do documento impugnado) cabe à parte que produziu o documento em juízo como fase da instrução. Por outro lado, a contestação de assinatura não inicia o procedimento de falsidade documental, mas o incidente de verificação de assinatura.

7 Contestação da assinatura digital e processo judicial eletrônico

Após se estudar a questão do ônus probatório no caso de contestação da assinatura autógrafa, discorre-se sobre a contestação da assinatura digital. Sobre o tema, não temos ainda uma vasta discussão doutrinária específica.

Menke, quando trata da questão do ônus probatório e da contestação da assinatura digital, assim leciona:

> Na prática, quando se recebe uma mensagem assinada digitalmente, ela estará acompanhada do certificado digital do remetente, onde constará, entre outros dados, a sua chave pública. Um programa de computador do destinatário aplicará a chave pública do emissor da mensagem e confirmará a autoria e a integridade do documento eletrônico, a partir de uma rápida consulta ao repositório de chaves públicas do terceiro de confiança – Autoridade Certificadora – onde será verificado: 1) se a chave pública realmente existe e se está associada àquela pessoa; 2) se o respectivo certificado digital é válido, ou seja, se não foi por algum motivo (perda, comprometimento ou roubo de chave privada) revogado. *Com a confirmação positiva, tem-se a presunção de que o documento eletrônico provém da pessoa que o assinou (autoria)*, e que ele não foi alterado no seu percurso virtual (integridade). *À presunção de autoria – e como decorrência dessa propriedade – agrega-se ainda outro elemento constantemente enfatizado no jargão técnico das assinaturas digitais: é o chamado não repúdio, que, a princípio, impedirá ao autor da declaração de vontade assinada digitalmente obter sucesso em eventual tentativa de negar*

> *a sua vinculação com o conteúdo do documento. A presunção aqui tratada não é absoluta, mas sim* juris tantum*, admitindo prova em contrário, caso em que o titular da chave de assinatura, para negar a autoria de determinada manifestação de vontade, terá o ônus de comprovar a utilização indevida de sua chave privada por outra pessoa mal-intencionada, como por exemplo, nos casos de coação ou de furto* (MENKE, 2011, p. 4, grifo nosso)

Como podemos observar, o autor empresta efeitos jurídicos ao conceito de não repúdio, ao afirmar a existência de uma presunção relativa. Quando tratamos da questão da chave pública válida, estamos indiretamente tentando demonstrar a autoria do documento, ou seja, provar a autenticidade do documento eletrônico. Provar a autenticidade de um documento é demonstrar que o autor aparente coincide com o autor real. Por outro lado, "contestar a assinatura" significa negar a autoria do documento, uma vez que a autoria de um documento é provada pela sua subscrição, não importando se o conteúdo do documento foi efetivamente elaborado pelo subscritor.

Usar a chave pública para provar a autoria do documento eletrônico assinado digitalmente é recorrer à propriedade do não repúdio que se trata apenas de um conceito técnico, e não jurídico. A conferência da chave pública com a chave privada não gera evidência de que o seu titular, de fato, subscreveu o documento eletrônico. Trata-se de simples indício, uma vez que a chave privada usada na assinatura digital confere com a chave pública do titular do par de chaves, parecendo indicar que ele a utilizou. Há nesse raciocínio uma presunção *hominis* de que somente o titular poderia ter acesso àquela chave privada. A questão é sutil, mas muito importante. Não é uma presunção legal, apenas uma presunção do homem. Presunções legais precisam estar previstas em lei, e não decorrem de propriedades matemáticas.

Devemos observar que, quando o suposto autor do documento contesta a assinatura lançada no documento, ele afirma que não o subscreveu. Ou seja, no tradicional documento em papel, a contestação de assinatura autógrafa significa o não reconhecimento da sua autoria, alega-se que não se subscreveu aquele documento. Quando tratamos da assinatura digital, o ato de subscrição de um documento eletrônico se dá pelo uso da *message digest* (resumo do documento eletrônico a ser assinado) e da chave privada do subscritor. Portanto, o ato de subscrever digitalmente está associado ao uso da chave privada, e não à manipulação da chave pública.

Assim, podemos concluir que, quando o suposto autor contesta a assinatura digital aposta em um documento eletrônico, ele afirma que não subscreveu o documento eletrônico, ou seja: alega que não usou pessoalmente sua chave privada para assinar o *mesage digest* do documento eletrônico. É possível que alguém se apodere da chave privada e a utilize como se fosse o seu proprietário: "De qualquer modo, é importante lembrar que se terceiros tiverem acesso à chave privada, poderão subscrever documentos como se fossem o seu verdadeiro titular, sem que isto deixe qualquer vestígio" (MARCACINI, 1999, p. 12).

Tentar usar a operação de conferência da chave pública com a chave privada para afastar a alegação de contestação de assinatura é recorrer à propriedade do não repúdio. Não se pode usar dessa propriedade técnica para se conceder efeitos jurídicos,

pois a conferência do par de chaves públicas e privadas não significa que o suposto autor efetivamente tenha subscrito o documento eletrônico, tratando-se de mero indício. Ou seja, a conferência da chave pública com a chave privada não é evidência de que a chave privada tenha sido utilizada pelo seu titular para assinar o *message digest* do documento eletrônico: apenas significa que alguém utilizou a chave privada para assinar o *message digest* do documento eletrônico.

Se, por um lado, autores criticam a legislação norte-americana por tentar se utilizar do conceito técnico de não repúdio para gerar efeitos jurídicos, criando uma presunção absoluta de que o documento eletrônico foi efetivamente assinado pelo titular do par de chaves privada e pública, tornando juridicamente impossível a contestação da assinatura; por outro lado, o não repúdio não pode ser utilizado para criar uma presunção relativa e, consequentemente, criar uma regra de distribuição do ônus da prova. O não repúdio é apenas indício de autoria; não é evidência. Portanto, o não repúdio, por ser propriedade técnica, não pode gerar nem presunção absoluta (inadmissão de prova em contrário), tampouco presunção relativa. Criar presunções é matéria reservada ao legislador. A distribuição do ônus probatório é uma questão legislativa, e não a decorrência de uma propriedade matemática. Portanto, também não é possível se utilizar de um conceito matemático, que liga a chave privada à sua correspondente chave pública, para provar o fato de que alguém efetivamente subscreveu digitalmente um documento eletrônico.

Para se provar que uma pessoa subscreveu um documento digital, deve-se provar que o titular do par de chaves usou sua chave privada para assinar o *message digest* do documento eletrônico. Aceitar que, mediante a conferência da chave pública com a chave privada, se prova que o suposto autor subscreveu digitalmente o documento, é recorrer a uma presunção que não está prevista no ordenamento jurídico brasileiro.

De fato, essa suposta presunção legal relativa, que não existe no ordenamento brasileiro, está presente na lei italiana, que criou a "presunção legal de recondução da assinatura digital ao seu titular" (SANDEI, 2008, p. 77)[5] – isto é: uma presunção relativa de utilização da chave privada pelo seu verdadeiro titular. Tal presunção legal hoje tem assento no § 2º do art. 21 do Código de Administração Digital (CAD) italiano:

> 2. O documento eletrônico assinado com uma assinatura eletrônica avançada, formato qualificado ou digital, em conformidade com as normas técnicas estabelecidas no artigo 20, § 3º, que garantem a possibilidade de identificar o autor, a integridade e a imutabilidade do documento, concede a eficácia prevista no artigo 2.702 do Código Civil. *Em relação à utilização do dispositivo de assinatura, presume-se a recondução ao uso pelo seu titular, a não ser que se prove em contrário*. (ITÁLIA, 2005, tradução nossa, grifo nosso)[6]

Assim, a lei italiana criou uma presunção legal relativa, regulando a distribuição do ônus probatório:

> O art. 21, § 2º, do CAD, esclarece que o documento eletrônico, subscrito com assinatura digital ou com outro tipo de assinatura eletrônica, tem o efeito previsto no artigo 2.702 do Código Civil e que, quanto ao uso do dispositivo de assinatura, presume-se ter sido feito pelo seu proprietário, exceto quando apresentada prova em contrário. (PATTI, 2008, p. 4, tradução nossa)[7]

Importante observar que na legislação italiana, antes do advento do CAD, havia o § 3º do art. 10 do Decreto nº 445/2000 que acabou por gerar discussão sobre a questão:

> 3. O documento eletrônico, quando é subscrito com assinatura digital ou com outro tipo de assinatura eletrônica avançada, e, sendo a assinatura baseada em um certificado qualificado e gerada mediante dispositivo para criação de uma assinatura segura, faz também prova plena, até o incidente de falsidade, da proveniência [autoria] da declaração subscrita (ITÁLIA, 2000, tradução nossa).[8]

Naquela época, a doutrina italiana se questionava muito quanto à ausência dessa presunção de utilização (*presunzione di utilizzo*), o que gerava uma discussão entre duas teses doutrinárias: uma, da "eficácia forte" do documento assinado digitalmente, não sendo possível desconhecer a assinatura digital, mas estando o documento sujeito ao incidente de falsidade; uma segunda, da "eficácia débil", atribuindo ao documento digital a eficácia de documento particular, podendo o titular da firma desconhecê-la:

> Um vivo debate precedeu e se seguiu ao processo legislativo. Neste debate surgiram duas teses. Uma, da eficácia forte do documento digital, segundo a qual a validação [da assinatura digital] equivaleria ao reconhecimento de firma, atribuindo-se ao documento uma eficácia probatória que persistia até o término do incidente de falsidade. Outra, da eficácia débil, atribuindo ao documento digital a eficácia probatória de escrito particular, sem reconhecimento de firma, permitindo ao titular da assinatura a faculdade de desconhecê-la. (BIANCA, 2008, p. 2, tradução nossa)[9]

Como sabemos, uma presunção relativa irá estabelecer uma distribuição do ônus probatório. Portanto, surge a questão: de quem é o ônus de provar a autoria do documento eletrônico que tenha sua assinatura digital contestada? Como vimos anteriormente, o regime jurídico que rege as assinaturas digitais no Direito brasileiro é o mesmo que regulamenta as tradicionais assinaturas autógrafas. Portanto, no caso da contestação da assinatura digital aposta em documento eletrônico, o ônus da prova está prescrito no inciso II do art. 389 do CPC. Portanto, contestada a assinatura digital de um documento eletrônico, cabe a quem produziu o documento – ou seja, quem quer conceder o efeito probante ao documento eletrônico – o ônus de provar que esse documento foi subscrito pela parte contrária.

Logo, quem contestou a assinatura digital não precisa provar que não utilizou sua chave privada para assinar o *message digest* do documento. Cabe à parte contrária, que quer valer-se do documento eletrônico, provar que o suposto autor – quem contestou a assinatura digital e é titular do par de chaves pública e privada –, de fato subscreveu digitalmente o documento eletrônico, ou seja, de fato utilizou sua chave privada para assinar o *message digest* do documento eletrônico. Esse é o ônus probatório que se pode extrair da redação do art. 389, II, do CPC: tanto no caso da assinatura autógrafa quanto no da assinatura digital. De fato, os casos citados por Menke (2011, p. 4), de "coação e furto", e por Marcacini (1999, p. 13), de "apropriação e uso indevido da chave privada verdadeira", não se enquadram nos casos de contestação de assinatura e no seu incidente de verificação.

Nos casos de coação, dolo e erro, assim regula o 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.
> Parágrafo único. Cessa, todavia, a eficácia da admissão expressa ou tácita, se o documento houver sido obtido por erro, dolo ou coação. (BRASIL, 1973)

Ou seja, basta a parte alegar, dentro do prazo legal, que não reconhece a autenticidade da assinatura para que a fé do documento particular cesse imediatamente (art. 388, I, CPC). Mesmo extrapolando-se o prazo, a parte ainda poderá impugnar o documento alegando os vícios de vontade como coação, dolo ou erro:

> O vocábulo documento empregado no parágrafo não está se referindo à res, mas ao meio de prova, visto em seu aspecto intrínseco, ou seja, à declaração, à letra e à assinatura, a cujo respeito versa a admissão de autenticidade ou veracidade. [...] Mesmo que a parte haja expressamente aceito o documento, ou tenha-o admitido pelo silêncio, fica-lhe livre, portanto, vir impugná-lo no futuro, se tiver sido levada a agir por erro, dolo, ou coação (hipóteses que autorizam a anulação da confissão), cabendo-lhe o ônus de provar a ocorrência dos apontados vícios da vontade, sem o que a presunção não será derrubada. (ARAGÃO, 1981, p. 246 apud DIDIER JR.; BRAGA; OLIVEIRA, 2009, p. 164)

Havendo impugnação posterior ao prazo estabelecido em lei, teremos caso de invalidação de confissão ou revisão da admissão tácita:

> Configurado o erro de fato ou a coação, caberá à parte que admitiu a autenticidade ou veracidade do conteúdo do documento buscar a invalidação desse ato jurídico. Vale observar que a admissão *expressa* equivale à confissão. Tendo havido, pois, confissão (admissão expressa da autenticidade ou veracidade do conteúdo), os meios de que dispõe a parte para buscar a invalidação do seu ato estão previstos no CPC, aplicando-se aqui, por analogia, o art. 352 [...]. Em se tratando de admissão *tácita*, que não se confunde com a confissão, poderá ela ser revista no próprio processo, independentemente de ação autônoma, desde que provados o erro de fato ou a coação" (DIDIER JR.; BRAGA; OLIVEIRA, 2009, p. 164-165, grifo dos autores).

Portanto, os exemplos de coação levantados por Fabiano Menke (2011), mais relacionam-se com o fato jurídico da admissão ou com o ato jurídico da confissão (e a possibilidade de sua invalidação) do que com a contestação da assinatura.

Já nas situações de "furto" ou "apropriação e uso indevido da chave privada", mencionadas por Marcacini (1999, p. 13) e Menke (2011, p. 4), estamos diante de casos de falsidade documental, uma vez que os documentos serão formados falsamente, ou seja, forjados por quem não é autor: "Não há dúvida de que a inserção de assinatura de outrem, em documento (seja público ou particular) implica uma forma de falsidade documental" (MARINONI; ARENHART, 2005, p. 395).

Assim, o furto e apropriação da chave privada verdadeira parecem ser caso de falsidade documental, e não de contestação de assinatura apurado pelo incidente de verificação.

A doutrina italiana chamava atenção, antes do advento do CAD, para o fato de se querer imputar ao titular da chave privada o ônus de provar que sua chave havia sido usada por um terceiro mal-intencionado, em termos idênticos como propõem Menke e Marcacini:

> A legislação anterior esta prevista no art. 10, § 3º, da T.U. 445/00, que, alterada e complementada pelo Decreto Legislativo de 23 de janeiro de 2003, estabelecia, no art. 10, que "o documento eletrônico quando assinado com uma assinatura digital ou outro tipo de assinatura eletrônica avançada [...] faz também prova plena, até o incidente de falsidade, da proveniência da declaração subscrita". A falha deste dispositivo, referente ao reconhecimento de assinaturas digitais, levou a doutrina a considerar a *assinatura digital, uma assinatura autenticada (de per si) e, consequentemente, a criticar a escolha do legislador em ter atribuído ao documento eletrônico assinado digitalmente o valor de prova legal com os mesmos efeitos do documento particular com firma reconhecida ou com firma autenticada, sem, porém, exigir os mesmos requisitos*. Dessa forma, observava-se que o legislador havia subvertido o sistema legal de provas, porque *vendo na assinatura digital uma assinatura reconhecida de per si, extirpou-se, pela raiz, a possibilidade de desconhecê-la. O titular da assinatura digital, para repudiar a paternidade do documento assinado digitalmente não podia mais se limitar a um mero desconhecimento da firma aposta, mas deveria seguir o procedimento adotado para o incidente de falsidade*. De outra parte, aquele que é o titular do dispositivo de assinatura [titular da chave] deveria provar no incidente de falsidade, não a falsidade da assinatura digital, que pela sua característica técnica não pode ser falsa, mas provar o fato de sua aposição [utilização] abusiva. (SANDEI, 2008, p. 74-75, grifo nosso, tradução nossa)[10]

De fato, ao "inverter esse ônus", estaríamos equiparando o documento assinado digitalmente ao documento particular com firma reconhecida por autenticidade nos termos do art. 369 do CPC: "Reputa-se autêntico o documento, quando o tabelião reconhecer a firma do signatário, declarando que foi aposta em sua presença" (BRASIL, 1973). Nesse caso, haverá uma inversão do ônus da prova, quer dizer: o ônus da prova ficará com quem contestou a assinatura que fora reconhecida por autenticidade pelo tabelião ou escrivão (MARINONI; ARENHART, 2005, p. 404).

Sandei (2008, p. 75) justamente critica a exigência de que caberia a quem contestou a assinatura digital o ônus de provar que ela foi utilizada por um terceiro mediante um incidente de falsidade, pois o que se deseja provar é a aposição abusiva da assinatura digital. Como bem anotou, é como se o documento assinado digitalmente fosse reconhecido *de per si*, e impossibilitasse a contestação da assinatura (*disconoscimento della firma*). É como afirmássemos que todo documento assinado digitalmente fosse um documento particular com firma reconhecida por tabelião. Aliás, é o que alguns autores nacionais acabam afirmando, pretendo equiparar as autoridades certificadoras da ICP-Brasil aos tabeliões: "Enquanto nos documentos em papel a autenticidade é comprovada por firma que eventualmente poderá ser reconhecida por um tabelião que atestará sua legitimidade, nos documentos eletrônicos, a assinatura digital emitida por meio de um certificado digital de uma Autoridade Certificadora é que atribuirá a autoria" (ATHENIENSE, 2010, p. 125).

Ainda temos uma última hipótese, levantada por Santos (1994, p. 171), que difere da contestação da assinatura: quando, no próprio ato da admissão (antes do término do prazo para contestar a assinatura), a parte reconhece a sua assinatura, mas alega que o documento foi obtido por erro, dolo ou coação (um caso particular das hipóteses levantadas por Menke e Marcacini). Nesse caso, o ônus da prova também caberá a quem reconheceu a assinatura, uma vez que será instaurado o incidente de falsidade. A diferença é que, de imediato, cessará a fé do documento impugnado. Nessa hipótese, a força probante do documento cessa imediatamente (igual como na contestação da assinatura), mas quem reconheceu a assinatura assume para si o ônus de provar o vício de vontade alegado.

Observemos que, na contestação da assinatura, a parte simplesmente alega que não subscreveu o documento eletrônico e, portanto, que não utilizou de sua chave privada para assinar o *message digest* do documento eletrônico apresentado em juízo.

Ocorre, então, um descompasso entre a legislação e a técnica, uma vez que a assinatura digital não confere um liame subjetivo igual ao da assinatura autógrafa. Foi essa a conclusão da doutrina italiana:

> [...] veio amadurecendo o convencimento de que deveria se abandonar o procedimento legado da natureza cartácea do documento, para se introduzir uma regra nova que simplesmente sancionasse a presunção legal de imputabilidade [do uso] da assinatura digital ao seu titular, salvo prova em contrário. A ideia, recebida pela Comissão [de reforma da lei de assinatura digital], da presunção de recondução da assinatura digital ao seu titular, recebeu acolhimento no Código de Administração Digital. (BIANCA, 2008, p. 3, tradução nossa)[11]

Dessa forma, não acreditamos que a propriedade matemática do não repúdio seja capaz de afastar a regra legal de distribuição do ônus probatório inserta no art. 389, II, do CPC, e muito menos extinguir o instituto da contestação da assinatura (ainda que digital) e inviabilizar o incidente de verificação de assinatura.

Por outro lado, a conferência de compatibilidade entre as chaves pública e privada é apenas indício – e não evidência – de que o seu titular tenha assinado digitalmente o documento eletrônico, haja vista que o que se deve provar (no incidente de verificação quando da contestação de assinatura) é que o titular de fato subscreveu o documento impugnado, ou seja, efetivamente utilizou sua chave privada para assinar o *message digest* do documento eletrônico.

Portanto, analisando-se a doutrina e legislação brasileira, no caso de contestação da assinatura digital, cabe a quem produziu o documento o ônus de provar que esse documento foi subscrito pelo suposto autor, isto é: provar que o suposto autor utilizou sua chave privada para assinar o *message digest* do documento eletrônico ao qual se quer conceder força probante.

E quanto a possibilidade de contestação da assinatura digital no âmbito dos processos judiciais eletrônicos? Entendemos que também é possível pelos mesmos motivos já expostos. A Lei nº 11.419/2006 rege o chamado processo eletrônico, do qual destacamos o art. 1º, que trata das assinaturas eletrônicas:

> Art. 1º O uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais será admitido nos termos desta Lei.
> .....
> § 2º Para o disposto nesta Lei, considera-se:
> .....
> III - assinatura eletrônica as seguintes formas de identificação inequívoca do signatário:
> a) assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica;
> b) mediante cadastro de usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos. (BRASIL, 2006)

Essa lei admite tanto a assinatura digital como também uma modalidade específica de assinatura eletrônica, mediante cadastro de usuário pelos órgãos do Poder Judiciário. Mas teria a lei criado uma presunção absoluta, impossibilitando a contestação no âmbito de processos judiciais eletrônicos? Aparentemente pode-se ter essa impressão ao se reportar ao inciso III do § 2º do art. 1º da Lei nº 11.419/06, pois é usada a expressão "formas de identificação inequívoca do signatário". Porém, a mesma lei, no art. 11 e §§ 1º e 2º, assim dispõe:

> Art. 11. Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.
> § 1º Os extratos digitais e os documentos digitalizados e juntados aos autos pelos órgãos da Justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pelas procuradorias, pelas autoridades policiais, pelas repartições públicas em geral e por advogados públicos e privados têm a mesma força probante dos originais, ressalvada a alegação motivada e fundamentada de adulteração antes ou durante o processo de digitalização.
> § 2º A arguição de falsidade do documento original será processada eletronicamente na forma da lei processual em vigor. (BRASIL, 2006)

Ou seja, ainda que considerados originais, os documentos eletrônicos podem ser impugnados, seguindo a lei processual comum (CPC). Conforme já exposto anteriormente, entendemos que há distinção entre a "falsidade" e o "incidente de verificação" (MARINONI; ARENHART, 2005, p. 309), mas o fato é que a lei em questão não veda nenhum caso, mas pelo contrário, prevê a possibilidade de impugnação de documentos produzidos no âmbito do processo judicial eletrônico:

> A arguição de falsidade mencionada no § 2º deve ser feita conforme a lei processual em vigor, ou seja, o CPC, nos arts. 390 a 395, podendo ser processado com relação ao documento original digitalizado, e quanto ao documento produzido eletronicamente, ainda que seja assinado digitalmente, *pois contra a assinatura digital também poderá ser oposta a arguição*. A arguição será processada por meio eletrônico e, seguramente, deverá ser dirimida consoante prova pericial técnica para apurar a falsidade do documento eletrônico questionado. (ATHENIENSE, 2010, p. 218, grifo nosso)

Portanto, no caso de contestação de assinatura digital desenvolvido no presente artigo, consideramos principalmente a hipótese de um documento eletrônico particular assinado digitalmente (por exemplo, uma transação eletrônica de compra e venda

realizada anteriormente ao processo judicial) e carreado como prova em processo judicial eletrônico. É o exato equivalente de um documento particular carreado como prova em autos de processo judicial físico, quando se poderá contestar a assinatura nos casos já vistos anteriormente. A lei do processo eletrônico não veda a hipótese de contestação da assinatura digital.

O caso tratado no art. 11 da Lei nº 11.419/06 versa mais sobre a falsidade, ou seja, a impugnação de uma peça processual eletrônica quando se prova, por exemplo, que não foi o advogado que usou a sua chave privada para assinar uma petição ou que há alguma irregularidade na integridade do documento. Situação similar é a impugnação da peça processual, por se alegar algum vício antes ou durante a digitalização do documento. Nesses casos, o ônus probatório é o do incidente de falsidade, cabendo a quem arguiu provar a falsidade (art. 389, I, CPC).

Ressalte-se, porém, que não há vedação legal para contestar a assinatura digital ou eletrônica em processo judicial eletrônico. E, portanto, deve-se seguir o ônus probatório estabelecido no art. 389, II, do CPC. Contestar é afirmar que não se subscreveu o documento. A outra parte, que quer valer-se do documento em juízo, terá o ônus de provar que quem contestou, de fato, assinou o documento digital ou eletronicamente.

Portanto, pode-se afirmar que é sempre possível impugnar a assinatura digital, tanto pela contestação no caso de documentos eletrônicos particulares assinados digitalmente, mesmo que juntados a processos judiciais eletrônicos, quanto nos casos de arguição de falsidade de documentos e peças processuais no âmbito dos processos judiciais eletrônicos. A assinatura digital não é algo que imuniza de forma permanente e absoluta um documento eletrônico, havendo sempre a possibilidade de impugnação pela contestação ou pela arguição de falsidade, cada qual com seu ônus probatório.

Conclusão

Quando se trata de documentos em papel, assinados de forma autógrafa, tendo sua assinatura contestada nos termos do art. 388, I, do CPC, compete à parte que produziu o documento em juízo provar a autenticidade da assinatura (art. 389, II) no incidente de verificação.

Conforme unanimidade na doutrina e na jurisprudência, o caso é de prova pericial grafotécnica, de forma a comprovar que a assinatura foi produzida pelo punho escritor do suposto autor. Porém, quando estamos diante da contestação da assinatura digital, não há perícia capaz de comprovar que o documento eletrônico foi subscrito pelo suposto autor. Isto é: não há como provar que o titular do par de chaves privada e pública efetivamente utilizou a sua chave privada para assinar o *message digest* do documento eletrônico impugnado. Isso porque não há um liame subjetivo no ato de subscrição digital do documento eletrônico assinado, tal como ocorre quando um documento em papel é subscrito mediante assinatura autógrafa. Qualquer pessoa poderia ter se apoderado da chave privada – diretamente ou por intermédio de um vírus de computador ou outro *malware* – e tê-la utilizado para subscrever o documento eletrônico.

A Lei nº 11.419/06 também não impede a possibilidade de impugnação de documento assinado digitalmente no âmbito do processo judicial eletrônico, conforme prevê o § 2º do art. 11.

Como sabemos, o punho escritor deixa registrado no papel uma informação biométrica comportamental. Essa informação é capaz de ser reconhecida pelo perito grafotécnico mediante a análise da peça questionada e a aplicação das quatro leis do grafismo enunciadas pelo francês Edmond Solange Pellat no início do século XX. Portanto, para que um documento eletrônico, que teve sua assinatura digital contestada, tenha sua eficácia probatória restituída, caberá a quem o produziu em juízo provar que o suposto autor efetivamente subscreveu o documento eletrônico mediante o uso de chave privada para assinar o *message digest* do referido documento eletrônico, utilizando-se dos meios ordinários de prova, mas ficando desguarnecido da prova pericial. Vimos, também, que o não repúdio não seria capaz de comprovar um liame subjetivo entre o titular do par de chaves pública e privada e a operação de subscrever o documento eletrônico mediante o uso efetivo da chave privada. Qualquer um, apoderando-se da chave privada, seria capaz de assinar o documento, passando-se por seu titular.

Como podemos observar, o atual regime jurídico da contestação da assinatura digital não traz tanta segurança jurídica como era de se esperar, já que nossa legislação baseia-se ainda na tradicional técnica de subscrição de documentos mediante assinatura autógrafa. E, fundado nessa técnica de subscrição, o Direito brasileiro distribui o ônus probatório entre as partes envolvidas em caso de contestação de assinatura de um documento particular, lastreada na possibilidade de perícia grafotécnica da assinatura questionada.

O problema não reside na assinatura digital em si mesma, mas num descompasso entre os pressupostos da legislação e a técnica de subscrição mediante assinatura digital. Conforme abordado anteriormente, não se pode utilizar da propriedade do não repúdio para criar presunções absolutas (como na legislação norte-americana) ou presunções relativas e, consequentemente, as regras de distribuição do ônus probatório. As presunções legais e o *ônus probandi* decorrem da lei, e não da técnica utilizada para subscrever um documento. O não repúdio, quando muito, serve como fundamento do indício de autoria.

Além disso, o atual regime de distribuição do ônus probatório, nos casos de contestação de assinatura, encontra-se muito bem estabelecido pela lei brasileira, tanto pelos dispositivos do Código de Processo Civil, quanto pelo art. 10, § 1º, da Medida Provisória nº 2.200-2. Não há distinção legal entre a tradicional assinatura autógrafa e a assinatura digital: são os efeitos da adoção da equivalência funcional.

Portanto, esse descompasso legislativo entre o atual regime jurídico do ônus probatório nos casos de contestação de assinatura e a técnica de subscrição mediante assinatura digital deve ser revisto de forma a garantir uma maior segurança jurídica ao documento eletrônico assinado digitalmente.

Uma das possíveis soluções seria uma nova norma de presunção legal (e novas regras de distribuição do ônus da prova) nos casos específicos da subscrição de documentos eletrônicos mediante assinatura digital. Esta é a proposta apresentada no art. 23 do Projeto de Lei da Câmara dos Deputados nº 1.589/1999 que criaria a presunção legal de recondução da assinatura digital ao seu titular.[12]

Portanto, apesar de a Medida Provisória nº 2.200-2 ter legalmente equiparado a assinatura digital à assinatura autógrafa – buscando justamente conceder uma maior confiabilidade aos documentos eletrônicos –, o regime jurídico atual da contestação da assinatura está em descompasso com a técnica de subscrição mediante assinatura digital, justamente pelo fato de a legislação estar fundada na possibilidade das assinaturas autógrafas serem periciáveis grafotecnicamente, fato impossível nos casos das assinaturas digitais.

LEGAL CHALLENGE OF DIGITAL SIGNATURE

ABSTRACT: This article studies the possibility of legal dispute of digital signature confirmation, as well the legal rules and the burden of proof related to repudiation of electronic document authorship. The non-repudiation, as a cryptographic technical concept, is just a *praesumptio hominis* (presumption of fact), not being a presumption of law. A digital signature is not a notarized signature, able to shift the burden of proof in order that who repudiate the signature has to prove he has not used his digital signature. There is a mismatch between the assumptions of legislation and underwriting technic through digital signature, because legislation is based on the possibility of handwritten signatures are subject to forensic document examiners, something impossible in the case of digital signature. One solution would be a new legal rule of burden of proof in order to create a presumption of law that presumes that digital signature is used by its holder.

KEYWORDS: Digital signature. Dispute signature. Authorship verification. Presumptions of law. Burden of proof.

Referências

ATHENIENSE, Alexandre. *Comentários à Lei 11.419/06 e as práticas processuais por meio eletrônico nos Tribunais brasileiros*. Curitiba: Juruá, 2010.

BIANCA, Cesare Massimo. Documento digitale e atto notarile. *Convengo La Sicurezza Giuridica Nella Società Dell'informazione*, Roma, 25-26 set 2008. Disponível em:<http://www.notariato.it/export/sites/default/it/primo-piano/congressi-convegni/convegno-sicurezza-giuridica-pdf/Bianca_Relazione.pdf>. Acesso em: 11 fev. 2013.

BRASIL. Projeto de Lei [da Câmara] nº 1.589, de 1999. Dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e dá outras providências. Diário da Câmara dos Deputados, Brasília, DF, 24 set. 1999, p. 44.338-44.344. Disponível em: <http://imagem.camara.gov.br/Imagem/d/pdf/DCD24SET1999.pdf#page=266>. Acesso em: 22 mar. 2013.

BRASIL. Superior Tribunal de Justiça. *Embargos de Declaração no Agravo Regimental no Agravo em Recurso Especial nº 151.216/SP*. Embargante: Joana Maria Viana da Mota Ynoue. Embargado: Joaquim de Jesus Morgado. Relator: Min. João Otávio de Noronha. Brasília, DF, 17 set. 2013.

COSTA, Marcos da. *Validade jurídica e valor probante de documentos eletrônicos*. 2003. Disponível em: <http://www.cic.unb.br/~pedro/trabs/validade.html>. Acesso em: 10 jan. 2013.

COUTINHO, Severino Collier. *Números inteiros e criptografia RSA.* Rio de Janeiro: IMPA, 2011.

DIDIER JR., Fredie; BRAGA, Paula Sarna; OLIVEIRA, Rafael. *Direito processual civil:* Teoria da prova, direito probatório, teoria do precedente, decisão judicial, coisa julgada e antecipação dos efeitos da tutela. 4. ed. Salvador: Juspodivm, 2008. V. 2.

ELLISON, Carl; SCHNEIER, Bruce. Tem risks of PKI: what you're not being told about public key infrastructure. *Computer Security Journal* [S.l], v. XVI, n. 1, p. 1-8, 2000. Disponível em: <http://www.schneier.com/paper-pki.pdf>. Acesso em: 3 fev. 2013.

FALAT, Luiz Roberto Ferreira; REBELLO FILHO, Hildebrando Magno. *Entendo o laudo pericial grafotécnico e a grafoscopia*. 1. ed. Curitiba: Juruá, 2010.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. *Sobre certificação digital*. Brasília: ITI, 2012. Disponível em: <http://www.iti.gov.br/perguntas-frequentes/1743-sobre-certificacao-digital#cuidadoscert>. Acesso em: 14 nov. 2013.

ITÁLIA. *Codice dell'Amministrazione Digitale*. Decreto Legislativo 7 marzo 2005, n. 82. Disponível em: <http://www.digitpa.gov.it/amministrazione-digitale/CAD-testo-vigente>. Acesso em: 22 dez. 2013.

_____. *Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445*. Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. Disponível em: <http://www.interlex.it/testi/dpr00445.htm#10>. Acesso em: 22 dez. 2012.

MONTEIRO, André Luís Pinheiro. *A grafoscopia a serviço da perícia judicial:* a importância do perito em assinaturas no combate às fraudes. Curitiba: Juruá, 2008.

MARCACINI, Augusto Tavares Rosa. *O documento eletrônico como meio de prova*. São Paulo, nov. 1999. Disponível em: <http://augustomarcacini.net/index.php/DireitoInformatica/DocumentoEletronico>. Acesso em: 5 jan. 2012.

_____. *Certificação eletrônica, sem mitos ou mistérios*. São Paulo, abr. 2003. Disponível em: <http://augustomarcacini.net/index.php/DireitoInformatica/CertiFicacaoEletronicaSemMitos>. Acesso em: 5 jan. 2012.

_____. *Direito e informática*: uma abordagem jurídica sobre a criptografia. São Paulo: [s.n.], 2010.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. *Comentários ao código de processo civil*. 2. ed. São Paulo: RT, 2005. V. 5: Do processo de conhecimento: arts. 332 a 341. T. 2.

McCULLAGH, Adrian; CAELLI, William. *Non-repudiation on digital environment*. Bridgman, v. 8. n. 8. 7 aug. 2000. Disponível em: <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/778/687>. Acesso em: 5 fev 2013.

MENKE, Fabiano. *Assinatura eletrônica no direito brasileiro.* São Paulo: RT, 2005.

_____. *Assinatura digitais, certificados digitais, infraestrutura de chaves públicas brasileira e a ICP alemã*. Busca Legis. Florianópolis, 4 mar. 2011. Disponível em: <http://www.buscalegis.ufsc.br/revistas/files/journals/2/articles/4429/public/4429-4422-1-PB.pdf>. Acesso em: 5 jan. 2013.

OLIVEIRA, Carlos Alberto Álvaro de. Presunções e ficções no direito probatório. *Revista de Processo*, São Paulo, n. 196, p. 13-20, jun. 2011.

PATTI, Salvatore. *La sottoscrizione del documento informatico:* la firma digitale. *Convengo la Sicurezza Giuridica nella Società Dell'informazione*. Roma, 25-26 set. 2008. Disponível em: <http://www.notariato.it/export/sites/default/it/primo-piano/congressi-convegni/convegno-sicurezza-giuridica-pdf/Patti_Relazione.pdf>. Acesso em: 10 fev. 2013.

PINHEIRO, José Maurício. *Biometria nos sistemas computacionais*: você é a senha. Rio de Janeiro: Ciência Moderna, 2008.

SANDEI, Claudia. *Il valore giuridico del documento informatico.* 2008. Tese (Doutorado em Direito). Università degli Studi di Ferrara, 2008. Disponível em:<http://eprints.unife.it/110/1/TESI_COPISTERIA_def..pdf>. Acesso em: 11 fev. 2013.

SANTOS, Moacyr Amaral. *Comentários ao Código de Processo Civil:* Lei nº 5.869, de 11 de janeiro de 1973. 6. ed. Rio de Janeiro: Forense, 1994. v.4.

SILVA, Lino Sarlo da. *Public key infrastructure – PKI:* conheça a infraestrutura de chaves públicas e a certificação digital. São Paulo: Novatec, 2004.

SINGH, Simon. *O livro dos códigos.* 3. ed. Rio de Janeiro: Record, 2003.

TKOTZ, Viktoria. *Criptografia:* segredos embalados para viagem. São Paulo: Novatec, 2005.

VOLPI, Marlon Marcelo. *Assinatura digital:* aspectos técnicos, práticos e legais. Rio de Janeiro: Axcel Books, 2001.

Notas

[1] No original: "Por otro lado, si bien cabe estimar que un documento electrónico puede ser considerado un documento escrito, no puede asumir nunca el valor de escritura privada. Requisito esencial de la escritura privada, en efecto, es la rúbrica, esto es, la imposición del nombre propio y apellido por parte de la persona de la cual resultan provenir las declaraciones que forman el texto de la escritura. [...] Debemos, por tanto, distinguir claramente el valor jurídico del documento escrito del valor de la escritura privada y reconocer al documento electrónico en sentido estricto valor de documento escrito, y no de escritura privada por la imposibilidad del acto de suscripción personal".

[2] No original: "This matters mostly because of the term 'non-repudiation'. Like 'trusted', this term is taken from the literature of academic cryptography. There it means something very specific: that the digital-signature algorithm is not breakable, so a third party cannot forge your signature".

[3] No original: "PKI vendors have latched onto the term and used it in a legal sense, lobbying for laws to the effect that if someone uses your private signing key, then you are not allowed to repudiate the signature. In other words, under some digital signature laws (e.g., Utah and Washington), if your signing key has been certified by an approved CA, then you are responsible for whatever that private key does. It does not matter who was at the computer keyboard or what virus did the signing: you are legally responsible".

[4] Somente encontrou-se um autor que entende que o CPC utilizou a expressão "produziu o documento" na sua acepção leiga: "Tratando-se de arguição de falsidade da assinatura, o ônus da prova é do suposto autor do documento, isto é, daquele que suscita dúvidas sobre sua assinatura, haja vista que a expressão 'produziu' inserida no inciso II do art. 389 refere-se à produção do documento e não da prova em juízo" (FUX, 2004, p. 711).

[5] No original: "Presunzione legale di riconducibilità della firma digitale al suo titolare".

[6] No original: "2. Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria".

[7] No original: "Svolgendo poi il rinvio, l'art. 21, comma 2 cit., dispone che 'il documento informático, sotoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile' e che 'l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia la prova contraria'".

[8] No original: "3. Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è

generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto".

[9] No original: "Um vivace dibatto há preceduto e seguito le varie tappe dell'iter legislativo. In quesito dibattito sono emerse due tesi: quella dell'efficacia forte del documento digitale, secondo la quale la validazione equivale al riconoscimento e attribuisce al documento eficacia probatoria fino a querela di falso. L'altra tesi, dell'efficacia debole, attribuirsce al documento digitale l'efficacia probatória della scrittura priva di riconoscimento, ammetttendo la facoltà del titolare della firma di disconoscerla liberamente".

[10] No original: "La disciplina previgente era conteúda nell'art. 10, comma 3, del t.u. 445/00 che, cosi come modificato ed integrato dal d.lgs. 23 gennaio2003, n. 10, stabilivia Che 'il documento informático, quando è sottoscritto com firma digitale o com um altro tipo di firma elettronica avanzata [...] fa inoltre pinea prova, fino a querela di falso, della provenienza delle dichiarazione da chi l'há sottoscritto'. La mancanza in detta dispozione de qualsiasi riferimento al riconoscimento della firma digitale, aveva indotto la dotrtrina a considerare la firma digitale una firma (già di per sé) riconosciuta e, consecuentemente, a criticare la scelta del legislatore di atribuiré al documento informatico con firma digitale il valore de prova legale con effetti pari a quella della scrittura privata con firma riconosciuta o autenticata, senza però che ne ricorressero i requisiti. In tal modo, si osservava, il legislatore aveva starvolto il sistema legale delle prove, perché vedendo nella firma digitale uma firma di per sé riconosciuta, si escludeva alla radice la possibilità di disconoscerla. Il titolare della firma digitale, cioè, per ripudiare la paternità del documento firmato digitalmente, non avrebbe potuto limitarse ad un mero disconoscimento della firma stessa, ma avrebbe dovuto seguire il procediemnto dettato per la querela di falso. D'altra parte, ciò che il titolare del dispositivo di firma doveva provare nel procedimento di querela di falso, non era la fasitá della firma digitale, che per le sue caratteristiche tecniche non può mai essere falsa, bensì il fatto della sua abusiva apposizione".

[11] No original: "[...] ero venuto maturando il convincimento che occorreva abbandonare le procedura legata alla natura cartácea del documento e introdurre una regola nuova che sancisse semplicemente la presunzione legale di imputabilità della firma digitale al suo titolare, salvo che sai data prova contraria. L'idea, accolta dal Comitato, della presunta riconducibilità della firma digitale al suo titolare, ha trovato accoglimento nel codice dell'amministrazione digitale".

[12] "Art. 23. Havendo impugnação do documento eletrônico, incumbe o ônus da prova: I – à parte que produziu o documento, quanto à autenticidade da chave pública e quanto à segurança do sistema criptográfico utilizado; II – à parte contrária à que produziu o documento, quando alegar apropriação e uso da chave privada por terceiro, ou revogação ou suspensão das chaves" (BRASIL, 1999).