UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO

IGOR MARTINS SILVA
13/0028258

CRIPTOGRAFIA NO PROCESSO JUDICIAL ELETRÔNICO E NA ANÁLISE DE PROVAS DIGITAIS

Brasília
Junho de 2017

IGOR MARTINS SILVA
13/0028258

CRIPTOGRAFIA NO PROCESSO JUDICIAL ELETRÔNICO E NA ANÁLISE DE PROVAS DIGITAIS

Monografia apresentada como requisito parcial à obtenção do título de Bacharel em Direito pela Faculdade de Direito da Universidade de Brasília – UnB.

Orientador(a): Alexandre Kehrig Veronese Aguiar

Brasília
Junho de 2017

TERMO DE APROVAÇÃO

IGOR MARTINS SILVA

CRIPTOGRAFIA NO PROCESSO JUDICIAL ELETRÔNICO E NA ANÁLISE DE PROVAS DIGITAIS

Monografia apresentada como requisito parcial à obtenção do título de Bacharel em Direito pela Faculdade de Direito da Universidade de Brasília – UnB.

BANCA EXAMINADORA

_____
Prof. Dr. Alexandre Kehrig Veronese Aguiar
Orientador

_____
Prof. Dr. Henrique Araújo Costa
Membro

_____
Profª. Drª. Daniela Marques de Moraes
Membro

Brasília, 29 de junho de 2017.

DEDICATÓRIA

À minha amada esposa Nathalia, por toda a luz que traz ao meu caminho.

AGRADECIMENTOS

Antes de tudo, agradeço a Deus pela benção da vida.

Agradeço à minha família, pois suportaram com amor os momentos de ausência e dedicação aos estudos.

Agradeço aos professores da Faculdade de Direito da Universidade de Brasília por terem compartilhado seus conhecimentos de forma tão abnegada com estes que ainda dão os primeiros trôpegos passos na vida acadêmica.

Por fim, agradeço aos meus companheiros de trabalho. Vocês viabilizaram esse projeto com paciência e compreensão.

"Uma criptografia robusta é capaz de resistir a uma aplicação ilimitada de violência. Nenhuma força repressora poderá resolver uma equação de matemática."

Julian Assange

RESUMO

O presente trabalho tem por propósito abordar as contribuições da criptografia para o Processo Judicial Eletrônico (PJe) e para a valoração de provas digitais. Para alcançar esse objetivo, apresenta, inicialmente, aspectos técnicos da criptografia de forma a estabelecer as bases sobre as quais são construídas suas relações com o mundo do Direito. Em seguida, descreve o papel da criptografia como pilar da segurança jurídica do PJe, enumerando os dispositivos normativos que confiam à assinatura eletrônica e ao certificado digital premissa de validade dos atos eletrônicos no âmbito do procedimento judicial digital. Ainda, em uma terceira fase, mostra como o ordenamento jurídico tem valorado os documentos eletrônicos e as provas digitais em sentido amplo com auxílio da criptografia para garantir a autenticidade, integridade e não-repúdio dos dados digitais. Por fim, conclui-se que os operadores do Direito conhecedores dos mecanismos de funcionamento criptográficos e acerca das suas contribuições para o mundo do Direito estão em melhores condições argumentativas para questionar ou reforçar a validade jurídica de dados digitais no âmbito dos procedimentos judiciais. Trata-se de estudo hipotético-dedutivo, com análise qualitativa de documentos e materiais bibliográficos.

Palavras-chaves: Criptografia, Processo Judicial Eletrônico, Prova digital.

ABSTRACT

The purpose of this paper is to address the contributions of cryptography to the Electronic Judicial Process (PJe) and to valuation of digital evidence. In order to reach this objective, it presents, initially, technical aspects of cryptography in order to establish the bases on which its relations with the world of Law are built. Next, it describes the role of cryptography as a pillar of legal security for PJe, listing the normative devices that entrust the electronic signature and the digital certificate with the premise of the validity of electronic acts in the context of digital court proceedings. In a third phase, it shows how the legal system has valued electronic documents and digital proofs in a broad sense with the aid of cryptography to guarantee the authenticity, integrity and non-repudiation of digital data. Finally, it is concluded that law professionals who have knowledge about cryptographic mechanisms of operation and about their contributions to the legal world are better able to question or reinforce the legal validity of digital data in judicial proceedings. This is a hypothetical-deductive study, with a qualitative analysis of documents and bibliographic materials.

Keywords: Cryptography, Eletronic Judicial Process, Digital evidence.

SUMÁRIO

1 – Introdução 9
2 – Segurança da informação no procedimento judicial 12
3 – Aspectos técnicos da criptografia 16
3.1 Princípios da criptografia 17
3.2 Criptografia de chave simétrica 19
3.3 Criptografia de chave pública 19
3.4 Funções de resumo criptográfico 21
3.5 Assinatura digital 23
3.6 Certificado digital 25
3.7 Requisitos de segurança da informação com criptografia 26
3.6.1 Confidencialidade 27
3.6.2 Integridade 27
3.6.3 Autenticidade 28
3.6.4 Não-repúdio 28
4 – Processo judicial eletrônico 30
4.1 Criptografia no PJe 31
4.2 Infraestrutura de Chaves Públicas Brasileira 34
5 – Provas digitais 38
5.1 Prova 38
5.2 Documento eletrônico e prova digital em sentido amplo 39
5.3 Jurisprudência 45
6 – Considerações finais 48
Referências bibliográficas 50

1 – Introdução

O desenvolvimento da tecnologia da informação trouxe mudanças significativas às relações sociais. A produção industrial, as telecomunicações, a eficiência dos meios de transporte, a exploração agrícola, o mercado financeiro, a política, tudo isso foi afetado diretamente pela capacidade de processamento de dados implementada por cérebros de gênios da informática, muitos deles anônimos, ao longo do século XX e nestes primeiros anos do século XXI.

O Direito, como não poderia ser diferente, também se viu compelido a incorporar mudanças impostas pelas novas formas de se fazer comércio e de se relacionar. Situações inéditas foram abarcadas pelo Direito por meio de adaptações hermenêuticas da legislação existente, enquanto outras precisaram de marco legal específico para sua regulamentação. Ao longo do tempo, a convivência entre tecnologia e direito, que no começo até suscitava nos mais céticos sinais de incompatibilidade, mostrou-se muito profícua para o progresso da sociedade.

Notadamente nos procedimentos judiciais, a revolução imposta pela tecnologia da informação trouxe simplicidade e celeridade ao trâmite de atos processuais, mas ainda desperta desconfianças quanto à validade e segurança dos dados digitais. Estariam os documentos agora virtuais tão seguros quanto as antigas cópias físicas guardadas nos fóruns de justiça? Qual a confiabilidade de uma prova digital anexada aos autos? O que permite assegurar que um documento digital foi assinado pela pessoa que alega tê-lo feito?

É para responder a essas e outras perguntas que a criptografia vem sendo empregada no âmbito da segurança da informação em larga escala na prática jurídica brasileira. Uma vez que o algoritmo criptográfico consegue implementar autenticidade, integridade, confidencialidade e não-repúdio, muitas das inseguranças próprias do ambiente digital são mitigadas e, portanto, o uso de tecnologia da informação no direito processual torna-se algo viável e aceitável.

Ora, se a criptografia viabiliza o uso da tecnologia da informação no âmbito do procedimento judicial, torna-se imprescindível que os operadores do Direito compreendam seus fundamentos e princípios de validade a fim de desenvolverem senso crítico sobre o tema. Hodiernamente, é possível observar que o uso da

criptografia se encontra disseminado na prática jurídica, contudo seu funcionamento e implementação ainda são incompreensíveis para boa parte dos operadores do Direito.

Destarte, o presente trabalho foi motivado por **problema** identificado no cotidiano da experiência jurídica: apesar do crescente uso da criptografia para a prática de atos processuais, como, por exemplo, quando assinam digitalmente uma petição inicial, os operadores do Direito não compreendem de fato o que está por trás dessas ações. Esse desconhecimento se alia à baixa produção acadêmica acerca das contribuições que a criptografia tem trazido para o mundo do Direito.

Portanto, o esforço aqui empreendido **justifica-se** em razão da necessidade de aproximar o profissional jurídico do conhecimento indispensável para compreender e questionar a legalidade dos atos processuais que tenham como base de validade o uso da criptografia, ou até mesmo questionar a admissibilidade de provas digitais que estejam em desconformidade com os requisitos mínimos para a segurança jurídica. À medida que cresce o uso de tecnologias da informação nos tribunais por meio do uso de processos judiciais eletrônicos, destaca-se o profissional capaz de entender as peculiaridades do trâmite digital dos autos. Da mesma forma, maior capacidade retórica terá para reforçar ou refutar evidências digitais anexadas aos autos como meios de prova.

A fim de colaborar para a mitigação do problema supracitado, o **objetivo geral** dessa obra constitui-se em identificar as contribuições da criptografia para o processo judicial eletrônico e para a valoração da prova digital no contexto da prática jurídica brasileira. Para atingi-lo, os seguintes **objetivos específicos** serão trabalhados:

- Conhecer os aspectos técnicos da criptografia que lhe permitem implementar os princípios de segurança da informação – integridade, confidencialidade, autenticidade e não-repúdio – no procedimento judicial;
- Descrever o papel da criptografia como pilar da segurança jurídica no âmbito do Sistema Processo Judicial Eletrônico (PJe) ao conferir integridade e autenticidade aos documentos eletrônicos;
- Explicar como a criptografia pode auxiliar na valoração das provas digitais ao garantir integridade e autenticidade aos dados digitais.

Para isso, o **paradigma metodológico** aplicado ao presente estudo foi o hipotético-dedutivo, tendo como **fontes de pesquisas** documentos e materiais bibliográficos que abordam os aspectos técnicos da criptografia, segurança da informação e direito processual.

Assim, a primeira parte do trabalho possui caráter mais estranho ao Direito – todavia, nem por isso deixa de ser importante – e explica o funcionamento dos processos criptográficos com o propósito de sedimentar as bases para a compreensão de como é possível utilizá-los a fim de garantir as funcionalidades que serão apresentadas nos capítulos seguintes.

Em um segundo momento, o presente trabalho se propõe a mostrar que o PJe somente se tornou realidade em razão do uso amplo da criptografia para implementar o certificado digital. Apenas assim foi possível assegurar a segurança jurídica que esse tipo de procedimento legal exige.

O tópico subsequente cuida de mostrar como a criptografia permite avaliar a autenticidade e a integridade de provas digitais colacionadas aos autos. Assim, serão trabalhados conceitos próprios do direito processual e da valoração de provas digitais e como esse ramo incorporou os aspectos técnicos dos algoritmos criptográficos em seu favor.

Por fim, a conclusão encerra o presente trabalho fazendo um apanhado geral do caminho percorrido pelas pesquisas realizadas e ratificando a importância que a criptografia desempenha atualmente na prática jurídica brasileira ao viabilizar segurança jurídica na análise de validade das provas digitais e no funcionamento dos PJe.

2 – Segurança da informação no procedimento judicial

A UNESCO, por ocasião da sua carta em favor da preservação da herança cultural digital[1], faz referência à "era da sociedade digital" na qual cidadãos e organizações, públicas e privadas, produzem e transformam cada vez mais informações em formato digital. As tecnologias da informação e comunicação envolvidas na produção, armazenamento, processamento e difusão de dados têm viabilizado reduções significativas nos custos, bem como ganhos de eficácia, em todos os processos de geração de riqueza.

Nesse sentido, o avanço constante nas tecnologias computacionais altera também a dinâmica das relações sociais. Exemplo dessa transformação pode ser observado nos suportes sobre os quais as relações jurídicas modernas são representadas. Se antigamente eram quase que exclusivamente estabelecidas sobre suportes físicos (papéis), recentemente é comum que sejam registradas em meios digitais (documentos eletrônicos). Desse modo, relações jurídicas comerciais e contratuais (*e-commerce* ou *internet banking*, por exemplo), bem como as relações jurídicas processuais em busca da solução de conflitos (processo judicial eletrônico) estão definitivamente fincando bases firmes no espaço cibernético.

Encontra-se no processo judicial eletrônico uma experiência altamente positiva nesse movimento em direção ao mundo digital. Isso porque sua lógica guarda perfeita sintonia com o conceito de "sistema de informação" – e os computadores foram criados para revolucionar essa área do conhecimento. Para comprovar as semelhanças entre procedimento judicial e sistema de informação, passa-se a uma breve explicação sobre esses institutos.

Inicialmente, é importante apresentar a posição majoritária da doutrina processual brasileira no que se refere à diferença entre processo e procedimento. Para Theodoro Júnior (2012, p. 61), notório processualista brasileiro, "é o procedimento, de tal sorte, que dá exterioridade ao processo, ou à relação processual, revelando-lhe o *modus faciendi* com que vai atingir o escopo da tutela jurisdicional". Assim, o processo seria o método para composição da lide, enquanto o procedimento seria a forma material com que o processo se realiza em cada caso concreto.

---

[1] Disponível em: http://www.unesco.org/new/en/communication-and-information/access-to-knowledge/preservation-of-documentary-heritage/digital-heritage/background/

Por isso que, informado por esse espírito, o presente trabalho aborda especificamente as colaborações da criptografia para o “procedimento” judicial dentro do ordenamento jurídico brasileiro.

Conforme Turban, Rainer Jr. e Potter (2007, p. 1), os sistemas de informação são responsáveis por coletar, processar, armazenar, analisar e disseminar informações com um propósito específico. Desse modo, sua finalidade é a obtenção de informações precisas para as pessoas certas, no momento certo, na quantidade certa e no formato certo. Logo, os sistemas de informação funcionam como uma máquina que por um lado recebe *inputs* (dados) e, no outro lado, entrega um *output* (informação) ao decisor.

É nítido, portanto, que os procedimentos judiciais que tomam lugar nos tribunais funcionam sob a lógica de um sistema de informação. Isso porque, em apertada síntese, a marcha processual serve para inserir dados válidos sob o prisma legal no processo a fim de que sejam submetidos a escrutínio e processamento pelos magistrados e, por fim, seja produzida a decisão judicial.

Acontece que os sistemas de informações estão vulneráveis a diversos perigos e ameaças, como nos lembra Turban, Rainer Jr. e Potter (2007, p. 60). A figura a seguir, nos mostra como são variadas essas ameaças.

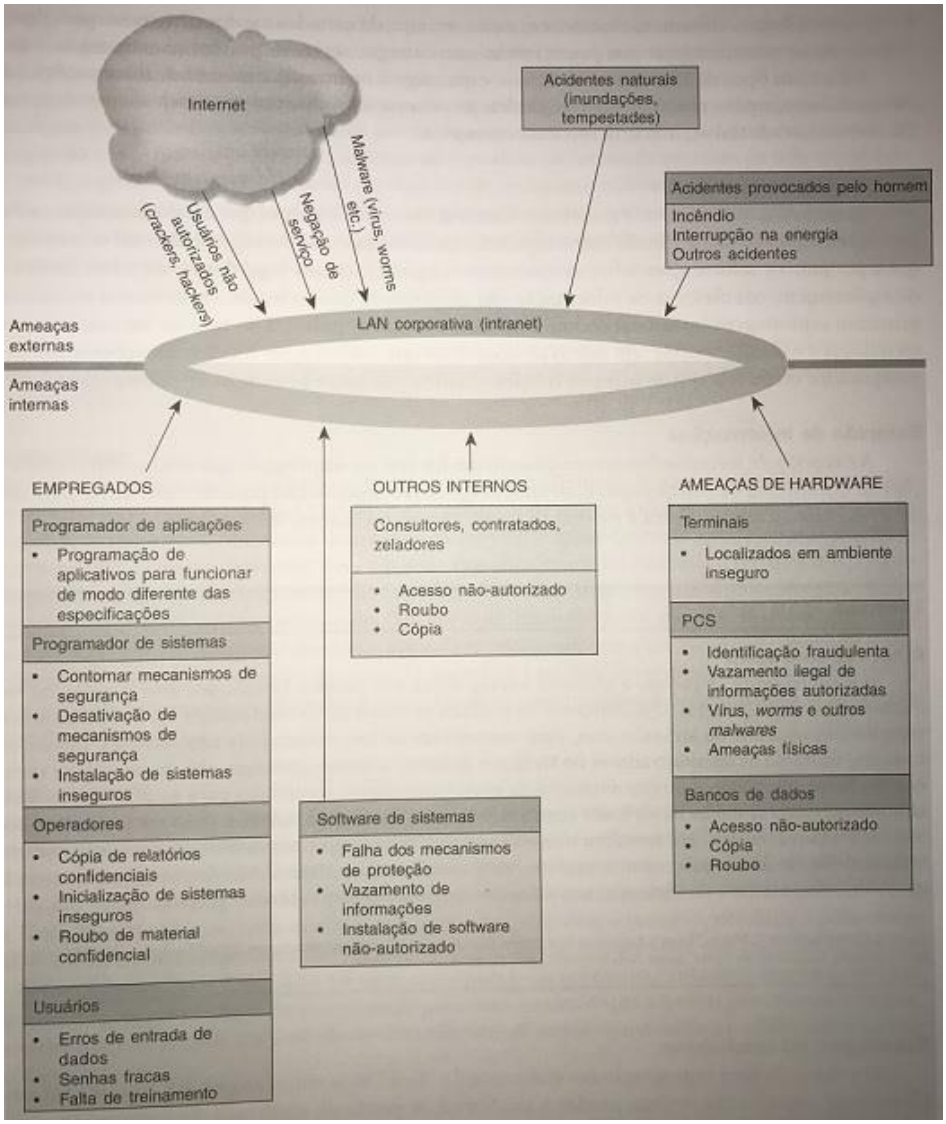

Figura 1 - Ameaças aos sistemas de informações
Fonte: TURBAN, RAINER JR. E POTTER (2007, p. 61)

Levando em consideração o paralelo traçado entre sistemas de informações e procedimentos judiciais, as mencionadas ameaças também podem ser opostas ao âmbito destes últimos.

Qualquer ameaça que recaia sobre os dados a serem processados no contexto de um procedimento judicial deve ser necessariamente interpretada como um risco à própria segurança jurídica do sistema normativo. À guisa de exemplo, eventual fraude em documento contendo sentença judicial, aqui vista como produto deste sistema de informação, pode vir a subverter por completo o sentido de uma decisão e, em última análise, o próprio sentido de justiça.

Ora, traçados os paralelos entre os procedimentos judiciais e os sistemas de informações e também entre a segurança jurídica e a segurança da

informação, a criptografia emerge como ferramenta adequada na estratégia de combate às ameaças que rondam um procedimento judicial cada vez mais digitalizado. Inspirados pela busca do ideal de justiça, o qual somente é alcançável dentro de condições de segurança jurídica, passa-se a discutir os aspectos técnicos da criptografia na sua tarefa de viabilizar segurança da informação na prática jurídica brasileira.

3 – Aspectos técnicos da criptografia

A criptografia, conforme apresenta Schneier (1996, p. 1), é a ciência e arte de manter uma comunicação segura. Por muito tempo esteve voltada para uma operação sobre a linguagem com propósito predominantemente militar.

Recentemente, a lógica computacional, transformadora da linguagem escrita e falada em números, levou ao surgimento da criptografia moderna. Os algoritmos criptográficos são atualmente operações lógico-matemáticas sobre blocos de bits (0 e 1) e têm sido utilizados extensivamente para implementar segurança da informação nesse novo paradigma.

Tal realidade tem promovido a aproximação entre o direito e a criptografia. À medida que os procedimentos judiciais se integram ao mundo digital, aumenta-se a demanda por um ambiente em que os dados estejam seguros, prestigiando, em última instância, o princípio da segurança jurídica no processo.

Para que o trâmite dos autos ocorra de modo seguro, é necessária a implementação dos seguintes requisitos, segundo nos apresenta Forouzan (2006, p. 711-713):

a) Confidencialidade: também conhecida como privacidade, este requisito impõe que apenas os envolvidos na comunicação sejam capazes de compreender o significado da mensagem transmitida. Normalmente é a característica mais atrelada ao termo criptografia.

b) Integridade: garante que nenhum dado foi alterado ao longo do seu percurso e chegou ao destinatário tal como fora produzido pelo remetente.

c) Autenticação: exigência que se faz de que a outra parte com quem se comunica seja realmente quem alega ser. No dia-a-dia, a autenticação é realizada seja pelo contato visual, seja pelo reconhecimento da voz. Nas comunicações digitais, a criptografia precisa se utilizar de estratégias matemáticas para trazer essa confirmação.

d) Não repúdio: significa dizer que, atendidos alguns requisitos dos protocolos criptográficos, os envolvidos na comunicação não podem negar a autoria das mensagens que produziram.

e) Disponibilidade e controle de acesso: por esse requisito, os dados da comunicação só podem ser acessados por pessoas autorizadas para tanto (controle de acesso) e no instante em que se fizer necessário (disponibilidade).

Passa-se adiante a discutir as estratégias utilizadas pela criptografia no sentido de obter os referidos requisitos de segurança da informação.

3.1 Princípios da criptografia

Inicialmente, é preciso esclarecer alguns conceitos que eventualmente possam confundir os não iniciados no assunto. Schneier (1996, p. 1) apresenta esses conceitos e define a criptografia como a ciência e arte de manter uma comunicação segura. Seus praticantes são chamados de criptógrafos. Por outro lado, os estudiosos que se dedicam à quebra do sigilo dessas comunicações são habitualmente chamados de criptoanalistas, uma vez que praticam a criptoanálise. Já a criptologia é um ramo específico da matemática especializada nos algoritmos que estão por trás da criptografia. Dentro da criptologia estão abarcadas a criptografia e a criptoanálise.

Outros termos são recorrentemente empregados nessa área. O **texto em claro** significa a mensagem em sua expressão compreensível e costuma ser representada pela letra **M**. Antigamente, essa mensagem costumava ser um texto escrito ou impresso. Com a evolução tecnológica, passou a ser, por exemplo, um arquivo de texto, um arquivo de áudio, um fluxo de bits ou qualquer dado que seja representado por dados binários e faça sentido para o destinatário (pessoa ou programa).

A **mensagem criptografada**, por outro lado, são os dados em seu estado incompreensível e costuma ser representada pela letra **C**. Para a transformação de texto claro em texto criptografado ocorre uma transformação operada pelo **algoritmo criptográfico**, normalmente chamado de **E**. Já a operação inversa para seu estado original e compreensível é realizada pelo **algoritmo de decriptação**, representado por **D**.

Em busca da manutenção da confidencialidade da comunicação, faz-se necessário o uso de **chaves** nas operações de transformação da mensagem. Estas costumam ser representadas pela letra **K**. Quando a chave utilizada para embaralhar os dados é a mesma que desembaralha, tem-se o sistema de algoritmo de chave secreta; mas quando as chaves são distintas, chama-se de sistema de algoritmo de chave pública. Ambos os casos serão apresentados em maiores detalhes mais à frente.

Em síntese, portanto, o texto em claro é transformado por um algoritmo de criptografia, utilizando-se uma chave, em uma mensagem criptografada:

$$E_K(M)=C$$

No outro sentido, a mensagem criptografada é transformada pelo algoritmo de decriptação, utilizando-se de uma chave, em texto em claro.

$$D_K(C)=M$$

A representação gráfica dessas operações pode ser vista na figura a seguir:

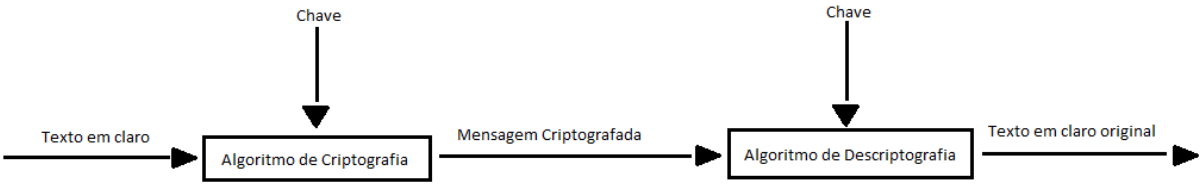

Figura 2- Criptografia e decriptação com chaves
Inspirado em SCHNEIER (1996, p. 3)

A soma de todos os textos em claro possíveis, das chaves, dos algoritmos e das mensagens criptografadas correspondentes compõe o que é chamado de **criptosistema**.

O esforço dos criptoanalistas em decifrar as mensagens criptografadas pode se concentrar sobre a lógica dos algoritmos ou sobre o conhecimento das chaves. Contudo, Schneier (1996, p. 7) nos traz a advertência do princípio de Kerckhoff segundo o qual um criptosistema que dependa do desconhecimento da lógica dos algoritmos para ser seguro será uma criptografia vulnerável. O ideal é que a força da criptografia dependa exclusivamente do segredo das chaves. Melhor seria manter os algoritmos sob escrutínio permanente dos acadêmicos. Por isso, aquele autor afirma: “Os melhores algoritmos que nós temos são aqueles que se tornaram

públicos, foram atacados pelos melhores criptoanalistas do mundo por anos e permanecem inquebráveis” (SCHNEIER, 1996, p.7, tradução nossa).

No que diz respeito às chaves, há duas formas de implementá-las: a primeira é pelo uso de uma chave em comum nas duas operações, conformando o sistema conhecido como criptografia de chave simétrica; e a segunda forma de implementação é pelo uso de chaves distintas nas operações de cifração e decifração, conformando o sistema conhecido como criptografia de chave pública.

3.2 Criptografia de chave simétrica

No tipo de criptografia de chave simétrica, exige-se que remetente e destinatário compartilhem uma chave antes de estabelecerem a comunicação. Desse modo, a segurança recai sobre o segredo da chave.

Para Schneier (1996, p. 4), as chaves não precisam ser necessariamente iguais, basta que sejam dedutíveis matematicamente a partir da outra:

> Symmetric algorithms, sometimes called conventional algorithms, are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms, the encryption key and the decryption key are the same.

Qualquer eventual comprometimento da chave nesse sistema expõe toda as comunicações que foram realizadas utilizando-a. Por isso, afirma Stallings (2003) que o gerenciamento da chave simétrica é um desafio em ambientes com muitas pessoas. Sempre que alguém sai desse grupo, a chave deve ser alterada em tempo razoável, o que frequentemente é inviável.

Por outro lado, ainda nos lembra Stallings (2003), os algoritmos criptográficos utilizados para implementar esse sistema costumam ser menos pesados para os sistemas computacionais modernos quando comparados com os algoritmos do sistema de chave pública.

3.3 Criptografia de chave pública

Na criptografia de chave pública o algoritmo é projetado de maneira tal que a chave utilizada para criptografar não seja dedutível matematicamente a partir daquela utilizada na operação de decriptação (SCHNEIER, 1996, p. 4).

Kurose e Ross (2006, p. 521) afirmam que a dificuldade inicial de entrar em acordo quanto a uma chave levou à criação da criptografia de chave pública. Em virtude do modo como funciona a rede mundial de computadores, é muito provável que os interlocutores não tenham tido a oportunidade prévia de combinarem uma chave em comum. A solução para essa dificuldade surgiu pelos estudos de Whitfield Difffie e Martin Hellman no ano de 1976, o que foi seguido pelo trabalho de três pesquisadores em 1978: Rivest, Shamir e Adleman. Seu produto levou as iniciais de seus criadores e ainda hoje é reconhecido pelo nome de RSA.

O funcionamento se dá nos seguintes termos, consoantes explica Kurose e Ross (2006, p. 521): Alice quer comunicar um segredo a Bob, mas não tiveram a oportunidade de combinar uma chave secreta previamente. Nesse caso, cada um deles deve possuir seu próprio par de chaves; uma será a chave pública, enquanto a outra será a chave privada. Como o próprio nome sugere, não há que se esconder a chave pública; pelo contrário, ela deve ser divulgada de tal forma que seja acessível a qualquer um que queira se comunicar com seu dono em sigilo. Assim, Alice obtém a chave pública de Bob e a utiliza na operação de criptografia, tornando a mensagem ininteligível.

A partir desse instante, apenas a chave privada de Bob será capaz de operar a decriptação e expor a mensagem original. Por isso, espera-se que Bob seja bastante prudente com o sigilo da sua chave privada.

No sentido oposto, a estória se repete. Bob consegue a chave pública de Alice em um repositório de fácil acesso e a utiliza na criptografia. Quando ela receber, somente com o uso da sua chave (Alice) privada será possível ler a resposta de Bob. Logo, percebe-se que se trata de um conceito simples, mas bastante funcional para o ambiente de redes em que vivemos atualmente.

A título de ilustração, a figura a seguir mostra as operações realizadas:

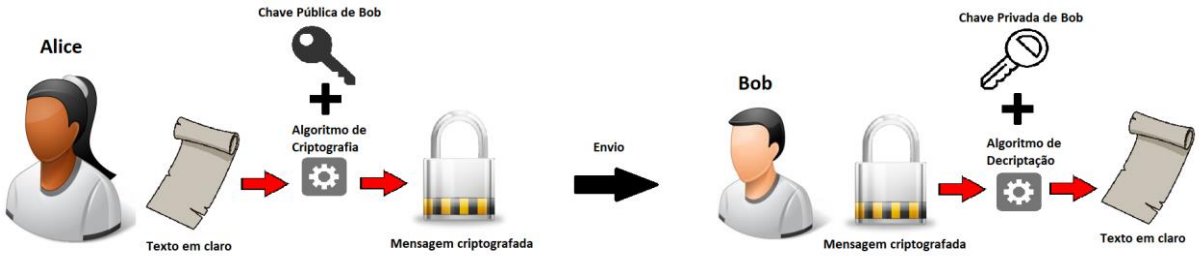

Figura 3 - Criptografia de chave pública
Fonte: elaborada pelo autor

3.4 Funções de resumo criptográfico

As funções de sentido único desempenham um papel central na segurança das comunicações. Por definição, elas são extremamente fáceis de calcular em um sentido, mas quase impossíveis de serem calculadas no sentido oposto (SCHNEIER, 1996, p. 30). Essa via de mão única não se presta às operações de confidencialidade citadas até aqui em que uma mensagem era inicialmente embaralhada e, na outra ponta, tornava-se novamente inteligível. No entanto, são de extrema valia quando utilizadas como funções de resumo criptográfico para a análise de possível adulteração dos dados durante o seu trânsito, conforme se passa a demonstrar.

As funções de resumo criptográfico utilizam como entrada uma quantidade de dados de tamanho variável e os converte em expressão de tamanho fixo, tal como se observa na figura abaixo:

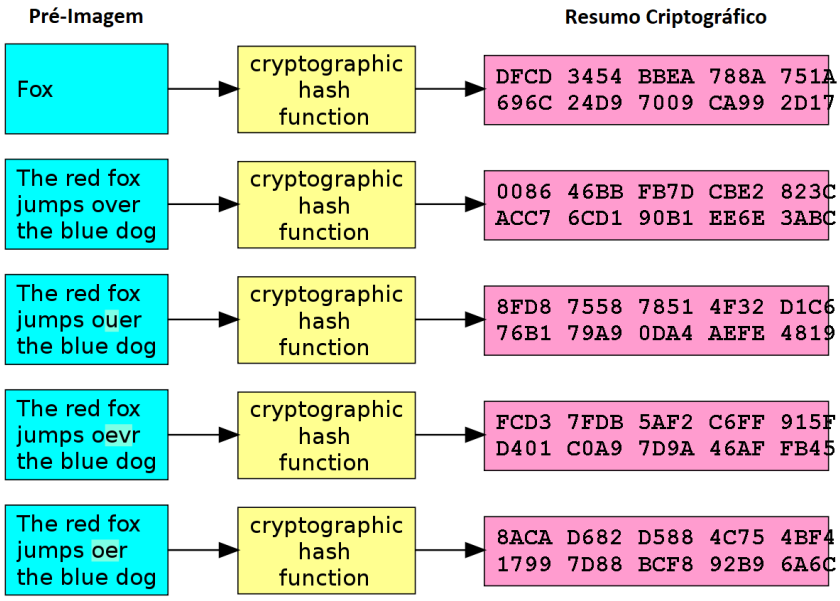

Figura 4 - Exemplo de função de resumo criptográfico
Fonte: https://en.wikipedia.org/wiki/Cryptographic_hash_function

É habitual chamar os dados de entrada na função de “pré-imagem”, enquanto os dados de saída são nomeados “resumos criptográficos” ou “*hashes”* (SCHNEIER, p. 30).

Como o tamanho da saída é sempre o mesmo em contraposição às possibilidades teoricamente ilimitadas da entrada, é lógico que haverá repetição de resultado para *inputs* diferentes. Contudo, um bom algoritmo de resumo criptográfico precisa tornar essa possibilidade significativamente remota.

Seguindo a lógica das funções de sentido único, as funções *hash*, como também são chamadas, transformam com facilidade a pré-imagem em um resumo criptográfico, mas é matematicamente impossível obter a pré-imagem a partir do *hash*. Outra característica desejável é que seja resistente a colisões: significa dizer que será extremamente difícil que duas pré-imagens produzam o mesmo resumo criptográfico (STALLINGS, 2003).

Conforme foi citado anteriormente, o *hash* não guarda nenhuma relação com a confidencialidade da comunicação. Sua contribuição à segurança da informação se presta ao requisito de integridade. Isso porque um único bit alterado na mensagem original produzirá um resumo criptográfico completamente diferente, o que viabiliza a análise de adulteração do conteúdo durante o seu trânsito.

3.5 Assinatura digital

A assinatura de documentos digitais utilizando-se da criptografia de chave pública foi a opção que obteve o maior sucesso até o momento na garantia de autenticidade exigida pela legislação. Logo, é importante conhecer suas características.

Kurose e Ross (2006, p. 531) descrevem os passos necessários para a assinatura digital. Suponha que Alice queira assinar um contrato de aluguel em formato digital que esteja celebrando com Bob a distância. O passo inicial é usar a chave privada de Alice para criptografar o documento preservando uma cópia em texto claro, afinal não se pretende obter confidencialidade sobre o negócio. O arquivo resultado da criptografia com a chave privada somente tornará a ser uma cópia exata do documento original caso venha a ser descriptografado com a chave pública de Alice. Qualquer outra chave que venha a ser utilizada resultará em um documento completamente diferente daquele celebrado pelas partes.

Ora, se o documento obtido confere com o original, é perfeitamente possível deduzir que somente Alice poderia ter criptografado o contrato. Nesse contexto, não só Bob pode se certificar da autenticidade da assinatura, mas qualquer pessoa em posse da chave pública de Alice tem essa capacidade.

Os referidos procedimentos tomam a seguinte forma:

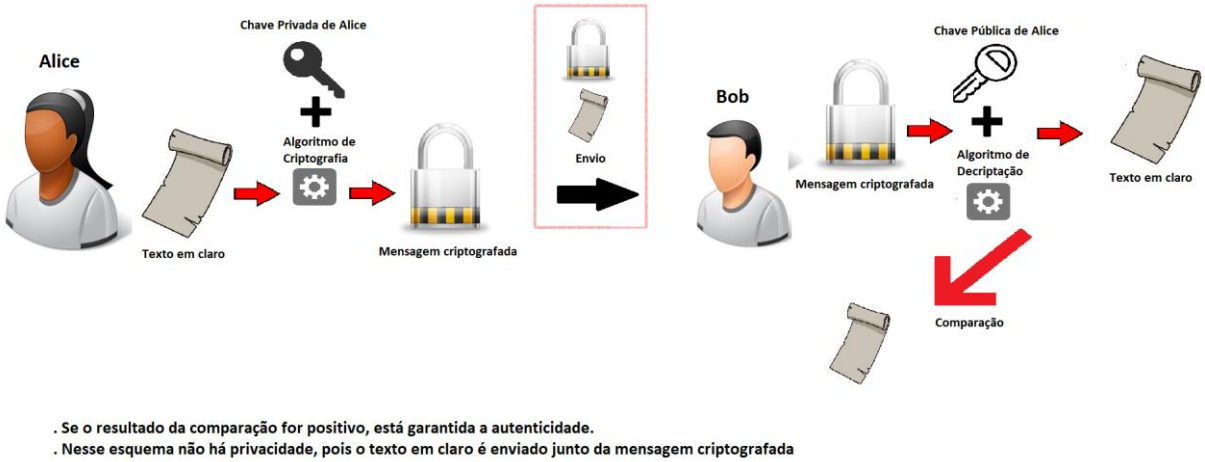

Figura 5 - Assinatura digital sem confidencialidade
Fonte: elaborada pelo autor

O processo pode se tornar ainda mais seguro se a função *hash* for utilizada. Isso porque além da garantia da autenticidade na origem, será possível

checar se houve qualquer modificação no seu conteúdo durante o envio (KUROSE; ROSS, 2006, p. 532).

Para tanto, Alice deve inicialmente aplicar a função de resumo criptográfico sobre o contrato, produzindo um *hash*. A partir de então, ela criptografa com sua chave privada somente este *hash* e o envia com o original para o destinatário.

Na outra ponta, Bob começa usando a chave pública de Alice sobre o *hash* criptografado a fim de obter o *hash* em claro. Agora é a vez de Bob usar o contrato original e aplicar sobre ele a mesma função de resumo criptográfico com o fito de compará-lo com *hash* obtido na operação anterior. Se a comparação for positiva, a integridade não foi violada.

Dessa maneira, encerra-se o processo de comunicação com Bob tendo a certeza de que o documento foi assinado mesmo por Alice e também que se trata de uma cópia exata do que ela tinha em mãos quando “assinou”.

A figura a seguir representa os procedimentos narrados:

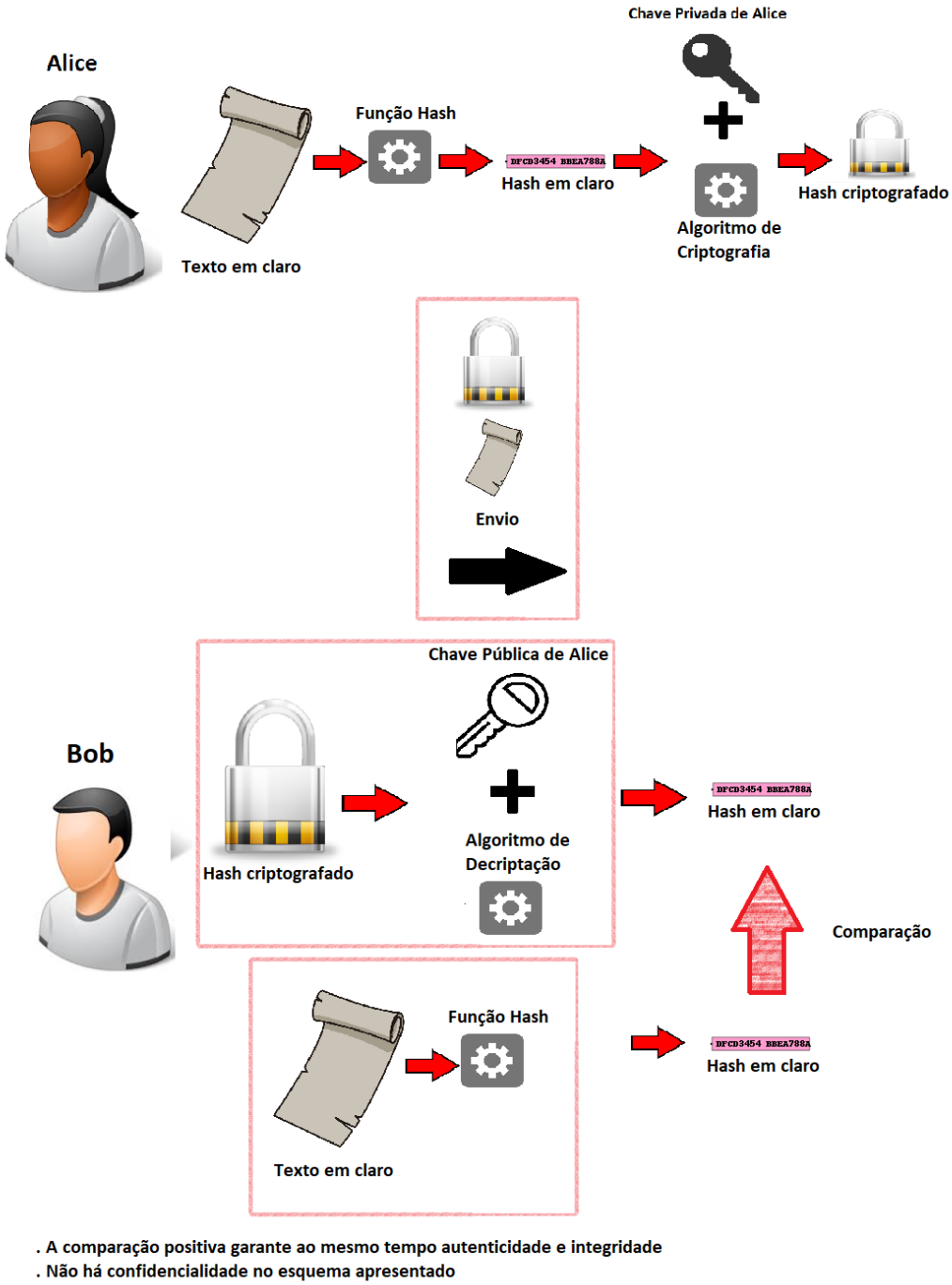

Figura 6 - Assinatura digital
Fonte: elaborada pelo autor

3.6 Certificado digital

A criptografia de chave assimétrica enfrenta um desafio, conforme relata Forouzan (2006, p. 724): como distribuir de forma segura as chaves públicas que serão utilizadas tanto para a verificação da autenticidade da assinatura digital quanto

para a confidencialidade de eventual comunicação? Afinal, alguém mal-intencionado poderia disponibilizar sua própria chave pública como se de outro fosse. A resposta está no sistema de certificação digital.

O sistema de certificação digital presume a existência de uma entidade na qual as partes confiam na chamada **Autoridade Certificadora** (AC). Essa instituição tem a responsabilidade de emitir e guardar certificados digitais que vinculem a chave pública à sua verdadeira origem. Para isso, usa chave privada da própria AC. Funciona de modo semelhante à identidade tradicional, em que há um órgão emissor atestando o vínculo entre a pessoa e o documento impresso (FOROUZAN, 2006, p. 724).

A título de exemplo, se Alice quer um certificado digital, deve enviar sua chave pública para a AC e comprovar com documentos sua identidade. Após estar certa de que realmente é Alice apresentando a chave pública, a AC usa sua própria chave privada para criptografar um certificado contendo a chave pública de Alice, gerando um *hash*. O próximo passo é disponibilizar ao mundo o par certificado-*hash* gerado para quem precisar se comunicar com Alice.

Continuando o exemplo, caso Bob queira lhe enviar uma mensagem secreta, antes de confiar cegamente na chave pública de Alice, Bob realizará algumas operações. Inicialmente irá obter no repositório da AC o certificado de Alice por se tratar de um lugar em que todos confiam. Em seguida, utilizará a chave pública da AC para decriptação do *hash* que veio junto ao certificado. Se o resultado desta última operação for exatamente igual ao certificado contendo a chave pública de Alice, é possível crer que realmente está em posse da chave autêntica. Agora Bob estaria seguro para criptografar uma mensagem privada ou para checar uma assinatura digital de Alice.

3.7 Requisitos de segurança da informação com criptografia

Compreendidas as características principais da criptografia pertinentes ao presente trabalho, passa-se a explicação de como elas são implementadas de modo a garantir os requisitos de segurança da informação apontados no início deste capítulo.

3.6.1 Confidencialidade

No mundo digital, os interlocutores que pretendem não expor o conteúdo de suas mensagens que trafegam pela rede mundial de computadores utilizam-se frequentemente da criptografia a fim de obter confidencialidade. O que possibilita sua implementação é a sequência de operações lógico-matemáticas realizadas pelos algoritmos utilizando-se de chaves para tanto.

É possível obter sigilo na comunicação pelo uso da criptografia de chave simétrica ou de chave assimétrica. Segundo nos apresenta Forouzan (2006, p.963), o emprego da primeira – chave simétrica – enfrenta grave desafio no mundo atual onde há dificuldade para a combinação prévia da chave e exige-se frequentemente que esse compartilhamento se dê entre diversas pessoas. Por outro lado, goza da vantagem de ser bastante eficiente do ponto de vista computacional.

Já o emprego de chave assimétrica facilita a conversa entre pessoas que não tiveram a oportunidade de estabelecer uma chave em comum e pode ser aplicada em ocasiões envolvendo um número grande de pessoas. Contudo, a sua desvantagem é o custo computacional elevado de operação.

Por isso, Forouzan (2006, p. 963) afirma que a resposta ideal, levando em consideração as vantagens e desvantagens de cada uma das estratégias, é utilizar as chaves assimétricas apenas no contato inicial com o propósito específico de compartilhar uma chave de sessão do tipo simétrica a qual servirá durante toda a comunicação. A partir desse momento, as trocas ocorrem ainda em sigilo, mas com maior eficiência em razão do baixo custo computacional.

3.6.2 Integridade

Em algumas ocasiões o objetivo dos interlocutores pode não ser o sigilo, mas sim a certeza de que nada foi alterado na mensagem ao longo do seu percurso. À guisa de exemplo, a solicitação do cliente para seu banco de uma transferência bancária com determinado valor deve estar protegida pelo requisito da integridade.

Consoante apresentado em tópico anterior, as funções de resumo criptográfico constituem ótima solução para apontar a existência de qualquer tipo de

alteração, ainda que seja ínfima, em arquivos. Por conseguinte, no contexto da segurança das informações, as funções de resumo criptográfico são amplamente utilizadas para atribuir uma “identidade” aos documentos passíveis de serem analisadas e comparadas posteriormente (KUROSE; ROSS, 2006, p. 513).

3.6.3 Autenticidade

Um dos requisitos para a segurança da informação é a garantia de que a comunicação de fato acontece com a pessoa que se acredita estar na outra ponta. E as funcionalidades até aqui apresentadas de sigilo e integridade não garantem *per se* essa autenticidade.

A tecnologia utilizada para atender a esse requisito é a assinatura digital e ela tem sido implementada com o emprego da criptografia assimétrica associada à função de resumo criptográfico (KUROSE; ROSS, 2006, p. 513). Os seus detalhes foram descritos no tópico anterior.

Portanto, conclui-se que a criptografia garante autenticidade por meio da assinatura digital.

3.6.4 Não-repúdio

O último requisito a ser abordado sobre segurança da informação vai um passo além de garantir a autenticidade das pontas de uma comunicação. O ideal é que haja uma forma de impedir o sujeito mal-intencionado de repudiar a assinatura que apôs em documento digital de maneira legítima. Nessa hipótese, fosse possível alegar que outra pessoa se fez passar por si para criptografar o hash de documento, toda a confiança do sistema ruiria, inviabilizando efeito jurídico aos atos realizados por meio do espaço cibernético (FOROUZAN, 2006, p. 724).

É com o emprego da estrutura por trás dos certificados digitais que o requisito de não-repúdio ganha vida. Uma organização que goza de credibilidade usa sua chave privada para assegurar ser verdadeiro o vínculo entre chave pública e o seu dono. Em caso de comprometimento da chave privada, seu dono deve informar

imediatamente à AC para que o seu certificado seja revogado e as pessoas não o utilizem mais nas verificações de autenticidade.

Logo, a criptografia garante o não-repúdio por meio da infraestrutura de certificados digitais.

4 – Processo judicial eletrônico

Em seu livro “Direito e informática: uma abordagem jurídica sobre a criptografia”, Marcacini (2002, p. 154) avaliava que as condições tecnológicas para a mudança em direção ao trâmite processual eletrônico já estariam estabelecidas. No entanto, o autor percebia que a maior dificuldade nesse movimento se daria em razão do fator cultural, pois:

> Ensinar os milhares de juízes, advogados, promotores e auxiliares de justiça a operar a criptografia adequadamente, e de forma segura, é, sem sombra de dúvida, a mais difícil e custosa tarefa a cumprir em direção à total informatização do Judiciário, que será culminada com a eliminação drástica do volume de papel utilizado.

A mudança no fator cultura tomou novos contornos com a publicação da Lei nº 11.419, de 19 de dezembro de 2006, dispondo sobre a informatização do processo judicial. Ficava estabelecida, a partir de então, autorização legal para o uso de meios eletrônicos na tramitação de processos judiciais, na comunicação de atos e na transmissão de peças processuais.

Iniciativas isoladas foram adotadas em diferentes regiões do país em busca de *softwares* que implementassem as funcionalidades da referida Lei. Contudo, a aplicação de recursos na compra desses programas enfrentou desafios que foram abordados no Acórdão TCU 1094 (BRASIL, 2012). Esse documento trouxe a recomendação de que fossem adotadas medidas pelos Órgãos da Justiça do Trabalho no sentido de evitar o desperdício de recursos no desenvolvimento de soluções a serem descartadas quando da implantação dos projetos nacionais, bem como que se abstivessem da prática de contratações cujo objeto viria a ser precocemente descartado, resultando em atos de gestão antieconômicos e ineficientes.

Dentre os esforços iniciais de transformação do processo eletrônico, a iniciativa de maior sucesso aconteceu no Tribunal Regional Federal da 5ª Região (TRF5). Após uma visita do Conselho Nacional da Justiça (CNJ) e de outros tribunais, entendeu-se que:

> Aquele era o projeto que atendia às restrições mais críticas com grande potencial de sucesso, atentando especialmente para a necessidade de uso de software aberto, para a conveniência de o conhecimento ficar dentro do

> Judiciário e para o fato de se observar as demandas dos tribunais. (BRASIL, 2010)[2]

Nesse diapasão, o projeto iniciado em setembro de 2009 no CNJ recebeu o nome de Processo Judicial Eletrônico (PJe). Cumprindo determinação expressa na Lei nº 11.419/2006, a qual atribui no art. 18 ao Poder Judiciário a responsabilidade de sua regulamentação, o CNJ editou a Resolução 185, de 18 de dezembro de 2013. Este documento, por sua vez, instituiu o Sistema Processo Judicial Eletrônico como um sistema de processo de informações e prática de atos processuais, estabelecendo os parâmetros para sua implementação e funcionamento.

Diante desse cenário, os tribunais passaram a ter bases mais sólidas para a adoção do PJe e começaram a publicar suas Portarias detalhando as fases de implantação e regulação no plano interno. A título de exemplo, o Tribunal de Justiça do Distrito Federal e Territórios (TJDFT) editou a Portaria Conjunta nº 53, de 23 de julho de 2014, mostrando o esforço desse tribunal em modernizar sua estrutura judiciária para prestar um melhor serviço jurisdicional aos cidadãos do Distrito Federal.

São muitos os benefícios decorrentes da utilização do processo eletrônico. Às partes da relação jurídica é possível a prática e acompanhamento dos atos processuais independentemente de o processo tramitar na Justiça Federal, Justiça Estadual, Justiça Militar dos Estados ou na Justiça do Trabalho. Configura-se, portanto, como uma solução única, gratuita para os próprios tribunais e atenta para os requisitos importantes de segurança e interoperabilidade. Há, ademais, ganhos notáveis de celeridade e qualidade na prestação jurisdicional; adequação da justiça ao princípio de proteção ambiental ao reduzir a quantidade de papel utilizado; racionalização dos gastos permitindo uma alocação mais eficiente dos recursos na atividade fim; solução dos conflitos; simplificação no trâmite dos atos processuais que têm seus lançamentos de movimentação realizados de forma simultânea às ações que lhe dão origem; melhora no controle do sistema judicial; e facilidade para produzir estatísticas e responder aos pedidos de informação, permitindo atender à necessidade de transparência própria aos Estados Democráticos de Direito.

4.1 Criptografia no PJe

[2] Conselho Nacional de Justiça. *Processo judicial eletrônico.* 2010.

Os inúmeros benefícios experimentados por tribunais em todas as regiões do país só se tornaram realidade em virtude da utilização de criptografia. Os pontos de intersecção entre o PJe e a criptografia abrangem os seguintes aspectos:

a) necessidade de assinatura digital certificada para a prática de atos processuais por meio eletrônico;
b) não-repúdio nos atos processuais praticados com uso da assinatura digital;
c) exigência de assinatura digital no relatório de indisponibilidade; e
d) obrigatoriedade de uso do protocolo HTTPS e uso de certificados digitais para os sítios eletrônicos e servidores que hospedam os serviços do PJe.

4.1.1 Necessidade de assinatura digital certificada para a prática de atos processuais por meio eletrônico

Este primeiro ponto configura-se como pilar básico do PJe. Ainda no início da Lei nº 11.419/2006, estabelece-se:

> Art. 2º O envio de petições, de recursos e a prática de atos processuais em geral por meio eletrônico serão admitidos mediante uso de assinatura eletrônica, na forma do art. 1º desta Lei, sendo obrigatório o credenciamento prévio no Poder Judiciário, conforme disciplinado pelos órgãos respectivos. (BRASIL, 2006)

No mesmo sentido, o Conselho Nacional de Justiça, cumprindo o seu dever de regular a supracitada Lei, previu no art. 6º do Resolução nº 185, de 18/12/2013, que "é obrigatória a utilização de assinatura digital a que se refere o art. 4º, § 3º, desta Resolução, com exceção das situações previstas no § 4º deste artigo".

Esse dispositivo tem sido repetido nas Portarias Conjuntas dos Tribunais com o CNJ para implantação do PJe. Particularmente o Tribunal de Justiça do Distrito Federal e Territórios reproduziu literalmente o dispositivo no mesmo art. 6º da sua Portaria Conjunta nº 53, de 23 de julho de 2014.

Diante da relevância alcançada pelo instituto da assinatura digital, é preciso citar como o ordenamento jurídico a define. A Lei nº 11.419/2006 utiliza o

termo assinatura eletrônica como sendo a “assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica”. Atualmente, o dispositivo normativo que rege não só o funcionamento das Autoridades Certificadoras, mas de toda a Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil), é a Medida Provisória nº 2.200-2 de 24, de agosto de 2001 (maiores comentários sobre este ato normativo serão abordados em tópico específico).

A Resolução nº 185 do CNJ, de 18/12/2013, no art. 3º, I, define:

> Assinatura digital: resumo matemático computacionalmente calculado a partir do uso de chave privada e que pode ser verificado com o uso de chave pública, estando o detentor do par de chaves certificado dentro da Infraestrutura de Chaves Públicas Brasileira (ICP-Br), na forma da legislação específica. (BRASIL, 2013)

Tecnicamente, há uma imprecisão nessa definição. Consoante apresentado no capítulo anterior, o resumo matemático é produto da função *hash*, a qual, por sua vez, não se utiliza de nenhum tipo de chave porque nunca será possível a operação inversa. Na verdade, a criptografia emprega a chave privada de quem assina para “embaralhar” o resumo matemático que só retornará ao seu valor original com o uso da chave pública de quem assinou.

4.1.2 Não-repúdio nos atos processuais praticados com uso da assinatura digital

Além da assinatura digital, outra colaboração da criptografia para o PJe está no requisito de segurança da informação chamado de não-repúdio. Essa contribuição ganha corpo no texto da Resolução nº 185 do CNJ, de 18/12/2013, e na Portaria Conjunta nº 53 do TJDFT, de 23/07/2014, com a mesma redação:

> O usuário é responsável pela exatidão das informações prestadas, quando de seu credenciamento, assim como pela guarda, sigilo e utilização da assinatura digital, **não sendo oponível, em qualquer hipótese, alegação de uso indevido**, nos termos da Medida Provisória n. 2.200-2, de 24 de agosto de 2001. (BRASIL, 2014, destaque nosso)

Houvesse a possibilidade de alegar não ser o autor de ato processual ao qual se conferiu assinatura eletrônica, todo o sistema ruiria diante da insegurança jurídica. Por isso, tão séria é a responsabilidade sobre a guarda do sigilo da chave privada nesse contexto.

4.1.3 Exigência de assinatura digital no relatório de indisponibilidade

Além da exigência de assinatura sobre os atos processuais desempenhados pelas partes, previu a Resolução nº 185 do CNJ no art. 10, § 3º, que o relatório de indisponibilidade do sistema PJe também fosse assinado digitalmente com efeito de certidão. Isso porque o referido documento tem efeito de, em algumas ocasiões e a depender do período de indisponibilidade, estender prazos processuais.

4.1.4 Protocolo HTTPS e uso de certificados digitais para os sítios eletrônicos e servidores do PJe

Os recursos oferecidos pelo PJe estão disponíveis na rede mundial de computadores. São reconhecidas as ameaças existentes nesse ambiente e, por isso, a criptografia também contribui para trazer segurança jurídica.

O protocolo HTTPS emprega a criptografia nas requisições web com o fito de obter confidencialidade e autenticidade nas comunicações entre o navegador do usuário e o servidor de páginas do PJe. A lógica é a mesma da relatada no capítulo anterior, com a diferença que os interlocutores são na verdade aplicações.

Desse modo, qualquer interceptação do fluxo de informações em trânsito entre o usuário do sistema PJe e seus servidores será incompreensível para os olhos de curiosos, protegendo senhas, informações pessoais e demais dados (confidencialidade). Ademais, é preciso estar certo de que o servidor na outra ponta atendendo às requisições é realmente administrado pelo tribunal (autenticidade).

4.2 Infraestrutura de Chaves Públicas Brasileira

Foi apresentada no tópico anterior a exigência da lei de que as assinaturas digitais estejam certificadas pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Trata-se de um modelo estabelecido pela Medida Provisória nº 2.200-2, de 24 de agosto de 2001. O seu art. 1º deixa claro o seu propósito e envolvimento com os requisitos de segurança da informação:

> Art. 1º Fica instituída a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir **a autenticidade, a integridade** e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. (BRASIL, 2001, destaque nosso)

Portanto, a estratégia normativa foi estabelecer uma estrutura hierárquica cuja Autoridade Certificadora Raiz é uma autarquia federal, o Instituto Nacional de Tecnologia da Informação (ITI), com sede e foro no Distrito Federal.

Mesmo tendo em seu topo um órgão da Administração Pública Federal, a cadeia pode ser composta tanto por pessoas jurídicas de direito público quanto por pessoas jurídicas de direito privado, desde que, claro, atendam aos requisitos legais e técnicos.

Outro dispositivo da Medida Provisória que merece comentário é o art. 10, § 2º, segundo o qual é possível utilizar certificados não provenientes da ICP-Brasil nas relações jurídicas desde que admitido pelas partes como válidas ou aceitas pelas pessoas a quem for oposto o documento. Não é o caso, sem embargo, da utilização de chaves dentro do sistema PJe, que estabelece de forma expressa a exigência de utilização de chaves da ICP-Brasil. Essa posição legislativa recebeu críticas severas por parte da Ordem dos Advogados do Brasil (OAB), consoante será discutido no próximo tópico.

As chaves certificadas empregadas pelos membros internos da justiça (desembargadores, juízes, servidores, etc.) têm sido distribuídas pelo CNJ. Advogados e demais cidadãos podem obter seus certificados em qualquer uma das Autoridades Certificadoras relacionadas no sítio eletrônico do ITI: http://www.iti.gov.br/icp-brasil/estrutura.

4.2 Críticas da Ordem dos Advogados do Brasil à infraestrutura IPC-Brasil

No seu artigo “A política de certificação digital: processos eletrônicos e a informatização”, Veronese (2007) apresenta as discussões e críticas despertadas por ocasião da origem da ICP-Brasil com a edição dos Decretos nº 3.587, de 05 set. 2000, 3.396, de 05 nov. 2001, e, finalmente, pela Medida Provisória 2.200-2, de 24 ago. 2001.

Afirma o autor que o projeto inicial foi pensado para ter sua validade restrita aos órgãos do Executivo da Administração Pública Federal. Contudo, a Medida Provisória (MP) revisou esse posicionamento e estendeu sua validade para todos os poderes e esferas da República, bem como aos cidadãos comuns. Dessa forma, somente gozariam de validade jurídica os certificados produzidos por Autoridades Certificadoras subordinadas à Autoridade-Raiz (ITI).

As críticas que surgiram, portanto, apontavam um viés autoritário da legislação. Primeiro, em razão da sua forma, pois as MP usualmente têm sua legitimidade questionada em razão do trâmite que seguem para sua conformação. Há nesse argumento fundada razão, vez que a MP que deu vida à ICP-Brasil ainda hoje não passou pelo escrutínio dos legisladores e continua produzindo efeitos apenas pela chancela presidencial.

Em segundo lugar, a estrutura piramidal que tomou a ICP-Brasil é condizente com a tradição administrativa dos Estados modernos, mas pode ser encarada como uma forma de controle e autoritarismo por parte do governo. Nesse diapasão, a OAB criticou a necessidade de que os cidadãos em seus negócios privados se sujeitassem à estrutura ICP-Brasil, negando-lhes liberdade contratual. Essa exigência foi vista até mesmo como uma ameaça à privacidade dos cidadãos diante da adoção de um certificado único.

Entretanto, as críticas mais graves da OAB estavam concentradas à emissão de certificados para os advogados. Como os atos processuais demandavam certificado digital, essa instituição entendia ter competência exclusiva para controlar a emissão de certificados para os profissionais da classe. Somente ela seria capaz de dizer quem seria ou não advogado em gozo de capacidade postulatória.

Quanto à estrutura pretendida pela OAB, Veronese (2007, p. 28) afirma:

> O modelo proposto pela OAB é distinto. Ele resulta da ausência de um único vértice. Assim, existiriam órgãos com competência para gerir os vários sistemas de certificação. Um exemplo deste modelo é o caso americano, onde cada Estado possui uma entidade raiz. Neste modelo, a interoperabilidade é um ponto central, com a formação de certificações cruzadas (“bridges”). A competência é compartilhada e atribuída conforme o uso social dos certificados. [...] O modelo é policêntrico, ou seja, baseado em uma lógica de rede.

O ITI, por seu turno, alega que a AC-Raiz não tem em sua guarda a chave privada dos usuários da infraestrutura, de forma que não há autoritarismo. Ela nem mesmo emite os certificados, mas apenas credencia aqueles que desejam ser reconhecidos como autoridade certificadora segundo padrões estabelecidos pelo Comitê Gestor da ICP-Brasil.

5 – Provas digitais

A criptografia prestou-se ao papel de pilar da segurança jurídica no processo eletrônico ao viabilizar integridade e autenticidade aos documentos eletrônicos. Sem ela, o PJe ruiria. Mas os seus benefícios não estão delimitados apenas aos trâmites processuais: é, ademais, ferramenta poderosa nas mãos dos juízes por ocasião da análise de admissibilidade e valoração das provas digitais.

5.1 Prova

As pretensões apresentadas em juízo sempre são alegadas com base em fatos, pois são estes que, em última análise, produzem o direito subjetivo supostamente violado. Para tanto, ambas as partes do litígio apresentam os fatos que suportam suas versões na ação, seja o autor, seja o réu.

Mas a mera alegação não tem força suficiente para convencer o juiz da pretensão. Por isso, são necessárias as provas. Para Theodoro Júnior (2012, p. 437) são dois os sentidos possíveis para o conceito de prova no processo. Sob um aspecto objetivo, prova seria o “instrumento ou meio hábil para demonstrar a existência de um fato”. Na dimensão subjetiva, prova é a “certeza originada quanto ao fato, em virtude da produção do instrumento probatório”.

Durante o processo de formação da sua convicção, o juiz não pode agir arbitrariamente. O ordenamento jurídico brasileiro privilegiou, como nos lembra Alvim (2009, p. 278), o sistema da *persuasão racional*, segundo o qual o juiz deve formar livremente sua convicção pela livre apreciação das provas, desde que fundamentada e respeitando os limites legais. Esse sistema superou o *positivo* que atribuía a cada prova um valor fixo, reduzindo o juiz a um mero autômato durante o julgamento; e também o sistema da *íntima convicção* que prevaleceu nos julgamentos da inquisição, emprestando ampla margem de liberdade ao julgador que podia, até mesmo, concluir contrariamente às provas dos autos.

A Lei nº 13.105, de 16 de março de 2015, também conhecida como Novo Código de Processo Civil, adotou o critério da atipicidade da prova, o que significa dizer que são aceitos quaisquer meios de prova não proibidos pelo ordenamento

jurídico nacional (art. 369 do CPC). Está aí o corte legal que serve de baliza para o juiz na construção da sua convicção. Não sendo a prova ilícita, o juiz tem liberdade para sopesar sua relevância para a definição da sentença. Neste momento, a criptografia desempenha importante papel ao fornecer condições para um julgamento mais preciso e seguro sobre as provas digitais.

5.2 Documento eletrônico e prova digital em sentido amplo

A despeito do princípio da persuasão racional do juiz consagrado no art. 371 do Código de Processo Civil, alguns dispositivos normativos desse mesmo instrumento estabelecem, *a priori*, um prestígio diferenciado a alguns meios de prova, a exemplo da prova documental.

Ora, essa opção legislativa é uma consequência lógica da credibilidade emanada da sua própria essência como prova pré-constituída, tendo por propósito perenizar atos e fatos jurídicos. Em um mundo no qual os eventos estão sendo abundantemente registrados em meios eletrônicos, as provas digitais hão de ser um meio relevante nos processos judiciais. Por isso, é tão necessário ao magistrado conhecer os requisitos de segurança da informação emprestados pela criptografia para a constituição da prova digital como meio de prova, permitindo-lhe uma avaliação mais acurada do peso e da relevância que de fato merecem por ocasião da livre formação do convencimento.

Interessante notar que as provas digitais nem sempre serão documentos eletrônicos que comprovam alguma relação jurídica explícita. Por isso, sugere-se uma distinção entre documento eletrônico e prova digital em sentido amplo. Esta última engloba os diversos tipos de dados armazenados em mídias digitais sujeitos à análise posterior da sua integridade e dos seus metadados e podem vir a ser anexadas aos autos de um processo como mera prova documentada. Dessa forma, um arquivo de áudio produto de uma escuta ambiental não poderia, a rigor, ser chamado de documento eletrônico, mas sim de prova digital em sentido amplo. Por outro lado, um documento confeccionado em editor de texto, por exemplo Word Office, conformado como um contrato de aluguel, deve ser classificado como um documento eletrônico e, caso subscrito por assinatura digital, seria uma prova documental.

Outra forma possível de distinguir documento eletrônico de prova digital em sentido amplo é fazer um paralelo com os conceitos de documento e instrumento apresentados por Theodoro Júnior (2012, p. 471). Para esse autor “documento é gênero a que pertencem todos os registros materiais de fatos jurídicos”. Por outro lado, “instrumento é, apenas, aquela espécie de documento adrede preparado pelas partes, no momento em que o ato jurídico é praticado, com a finalidade específica de produzir prova futura do acontecimento”. Nesse caso, o conceito de documento se aproximaria da ideia de prova digital em sentido amplo, enquanto o instrumento se aproximaria da ideia de documento eletrônico.

Em virtude da distinção supracitada, e em face da criptografia, esses dois tipos de prova merecem análises separadas.

5.2.1 Documento tradicional, documento eletrônico e assinatura digital

Os documentos são constituídos por dois elementos: o conteúdo e o suporte. O primeiro está relacionado à sua semântica, à ideia que encerra; enquanto o segundo é composto pela sua manifestação concreta e sensível, sendo seu elemento material.

No que tange ao conteúdo, o documento pode conter a transcrição de um fato, a manifestação de vontade ou de pensamento. É possível também falar de uma manifestação de ciência.

Contudo, a discussão mais relevante ao presente trabalho é sobre o suporte em que estão contidos os documentos. O documento tradicional sempre foi vinculado a um suporte físico que o materializasse. Chiovenda (1969, vol. 3, p. 127, destaque nosso) entende que o “documento, em sentido amplo, é toda **representação material** destinada a reproduzir determinada manifestação do pensamento, como uma voz fixada duradouramente”. Para Pontes de Miranda (1996, tomo IV, p.357, destaque nosso) “o documento, como meio de prova, é toda **coisa** em que se expressa por meio de sinais, o pensamento”. Ambas as expressões destacadas remetem à materialidade física do documento, abrindo a possibilidade de uma discussão sobre a materialidade dos documentos eletrônicos.

Sobre isso, Marinoni, Arenhart e Mitidiero (2015, p. 296) afirmam:

> Vale ressaltar que é frequente equiparar o suporte da prova documental à escritura. Imagina-se, nesta perspectiva, que somente haverá prova documental nas situações de prova escrita. Todavia, como já foi dito, o suporte do documento não se limita à via do papel escrito. Ao contrário, o que caracteriza o suporte é o fato de tratar-se de elemento real, pouco importando sua específica natureza. Dessa forma, o suporte pode ser uma folha de papel, mas também o papel holográfico, a fita cassete, o disquete de computador etc.

Não obstante a posição dos respeitados autores, fica clara a impossibilidade atual de atrelar o documento a uma materialidade física. Os documentos eletrônicos nada mais são do que sequências de bits passíveis de serem transferidas livremente entre memórias sem prejuízo algum do conteúdo.

Por óbvio, essa imaterialidade traz consigo desafios. O principal é a dificuldade de atribuir autenticidade e integridade aos dados representados por essa sequência de bits, seja qual for o suporte ao qual esteja vinculada. É o que se passa a discutir.

Para que um documento eletrônico seja entendido como tal, será necessário que tenha sido criado por alguma pessoa identificável com propósito definido. Ao seu criador, ou em nome de quem se fez o documento, dá-se o nome de autor, tal qual consta no art. 410 do Código de Processo Civil. Via de regra, a autoria de um documento será constatada pela subscrição, ou seja, pela assinatura aposta pelo autor no corpo do documento. A verificação dessa assinatura é o que confere autenticidade ao documento, vez que torna certa sua autoria.

Quando Marinoni, Arenhart e Mitidiero (2015, p. 297-298) discutem o tema da autenticidade, os ilustrem autores não abordam a Medida Provisória 2.200-2/2001. Por isso, consideram que o tema da autenticidade em documentos eletrônicos foi enfrentado de modo superficial no nosso ordenamento jurídico tendo como parâmetro apenas a Lei nº 11.419/2006. Realmente, o propósito desse diploma legal é tratar da informatização do processo judicial, enquanto a autenticidade de documentos eletrônicos recebeu tratamento acessório.

É na Medida Provisória 2.200-2/2001 que se encontram pilares mais firmes para a validade jurídica dos documentos eletrônicos assinados por chaves certificadas sob as normas da Infraestrutura de Chaves Públicas Brasileira. Isso

porque no art. 1º dessa norma garante-se a validade jurídica dos documentos em formato eletrônico que utilizem certificados digitais.

O Código de Processo Civil promulgado recentemente também não se esquiva de enfrentar o assunto. No seu art. 441, afirma serem aceitos os documentos eletrônicos produzidos com a “observância da legislação específica” (atualmente a MP 2.200-2/2001). Já no art. 439, o CPC aduz que os documentos eletrônicos somente poderão ser utilizados em processos convencionais se forem impressos e tiverem sua autenticidade verificada. Por fim, esse mesmo diploma no seu art. 440 atribui ao juiz a responsabilidade de apreciar o valor probante do documento eletrônico não convertido.

Encerrando a discussão sobre a autenticidade, o art. 411, II, do CPC, ademais, deixa claro que nosso ordenamento jurídico considera autêntico o documento que “estiver identificado por qualquer outro meio legal de certificação, inclusive eletrônico, nos termos da lei”.

No que diz respeito à integridade, é preciso que se diga da sua necessária vinculação à autenticidade no caso dos documentos eletrônicos. Uma assinatura aposta sobre conteúdo adulterado tem sua significação esvaziada, por óbvio. Assim o documento tradicional, de materialidade física, está mais vulnerável a alterações no seu conteúdo do que o documento eletrônico com assinatura digital.

É claro que existem exames periciais capazes de identificar fraudes que contaminam a integridade de um documento tradicional, mas isso requer exame detalhado e de profissional qualificado. No caso dos documentos eletrônicos, a descrição trazida neste trabalho no capítulo de criptografia mostrou que faz parte de toda assinatura com certificado digital a análise de integridade. Ao comparar o resumo criptográfico gerado pelo destinatário com o outro produzido pelo uso da criptografia com chave privada da origem, é possível obter segurança jurídica quanto à inalterabilidade do seu conteúdo. Essa comparação é feita automaticamente pelos algoritmos de análise de assinatura digital de maneira extremamente veloz e simples ao usuário, tornando viável a todos analisar a integridade de um documento.

Toda a confiança depositada nesse processo depende essencialmente de dois fatores: primeiro, que a chave privada do responsável pela assinatura não seja comprometida; segundo, que a chave pública realmente esteja vinculada à pessoa a que se refere.

Para tratar do primeiro problema, o titular da chave deve tomar cautelas para sua proteção. A Medida Provisória 2.220-2/2001, no parágrafo único do art. 6º, atribuiu ao titular a responsabilidade de gerar seu par de chaves pública e privada, de modo que ninguém tivesse contato com o conteúdo da chave privada. À Autoridade Certificadora (AC) somente será apresentada a chave pública. Logo, a AC não pode gerar a chave privada para o solicitante do certificado digital.

É a característica de não-repúdio que o obriga a ser diligente na guarda dessa chave privada. Ainda a MP 2.200-2/2001, no parágrafo 1º do art.10, afirma que "declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiras em relação aos signatários" (BRASIL, 2001). Trata-se de presunção relativa, uma vez que é possível apresentar meios de prova robustos de comprometimento da chave privada com o fito de afastar a responsabilidade pelo uso ilegítimo da assinatura digital.

No âmbito do Processo Judicial Eletrônico, a regulamentação da Lei nº 11.419/2006 editada pelo CNJ parece ser mais rigorosa na sua redação. Isso porque no parágrafo 2º do art. 4º da Resolução 185 do CNJ, já comentada anteriormente, consta a afirmação de não ser oponível, **em qualquer hipótese**, alegação de uso indevido.

Sobre o segundo problema, a estratégia utilizada para garantir que a chave pública realmente pertence àquele que se alega foi a utilização dos certificados digitais, assunto abordado anteriormente sob o tópico 4.2.

5.2.2 Prova digital em sentido amplo e a integridade

Retomando a diferença proposta entre documentos eletrônicos e provas digitais em sentido amplo, lembra-se que estes seriam semelhantes ao que Theodoro Júnior (2012, p.471) citou como documento em sentido amplo. Portanto, seriam registros a respeito de algum fato ou, de outro modo, qualquer arquivo digital que remete a fato sem necessariamente estar assinado por seu autor. Assim, por ocasião de sua produção, a prova digital em sentido amplo não se propunha a constituir prova prévia de algum ato ou fato jurídico.

Os arquivos digitais de toda espécie, sem embargo, ainda que não subscritos, estão sujeitos a produzir valor probatório no sistema processual brasileiro. Durante a valoração da prova digital em sentido amplo por parte do magistrado, um aspecto a ser considerado é a integridade dos dados apresentados.

Nesse sentido, a fim de trazer mais segurança aos procedimentos judiciais, e mesmo administrativos, que a Administração Pública Federal (APF) editou por meio do Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional (GSI-PR) a Norma Complementar Nº 21/IN01/DSIC/GSIPR, de 08 de outubro de 2014. Esse documento estabelece diretrizes para o registro, coleta e preservação de evidências a partir da análise de dados digitais nos órgãos e entidades da APF.

Não obstante cuidar especificamente sobre incidentes nas redes de computadores no âmbito da APF, essa norma serve como referência para a análise da relevância da integridade quando lidando com dados digitais passíveis de serem apresentados como provas digitais em procedimentos judiciais.

No item 7.5, alínea a, consta que devem ser preservados os resumos criptográficos de todos os arquivos coletados como evidências de ilícitos. Essa lista deve compor um único arquivo que também deverá produzir um resumo criptográfico. Depois da reunião dos arquivos e respectivos *hashes*, essas informações devem ser preservadas junto com um Termo de Custódia dos Ativos de Informação.

Percebe-se, pelas exigências descritas, que o DSIC reconheceu a importância de aplicar a criptografia, notadamente as funções unidirecionais de produção de resumo criptográfico, com o fito de garantir a inalterabilidade das provas produzidas.

Outro órgão da APF, a Secretaria Nacional de Segurança Pública do Ministério da Justiça (Senasp), preocupado com a qualidade da produção de provas técnicas pelos órgãos de perícia das polícias investigativas, publicou em 2013 documento nomeado “Procedimento Operacional Padrão: Perícia Criminal”. Tal dispositivo visava a padronizar os procedimentos operacionais relacionados às principais atividades periciais. O documento aborda sete grandes áreas periciais prioritárias, sendo uma delas a Informática Forense.

Na seção de procedimentos operacionais padrão para Informática Forense, são sugeridos procedimentos para o exame pericial de mídias de armazenamento computacional, de equipamento computacional portátil, local de

informática e local de internet. Em todos esses casos existe a indicação para que a integridade dos dados recolhidos seja garantida por meio da utilização de uma função de resumo criptográfico, especificamente por meio do emprego do algoritmo SHA-512. Os produtos dessa função, os *hashes*, devem constar no documento científico elaborado pelo perito. Desse modo, a força probatória dessas evidências impede a alegação por parte do acusado de que os dados constantes dos autos não correspondem aos dados originais.

Portanto, colocados lado a lado, tanto a Norma Complementar Nº 21/IN01/DSIC/GSIPR do DSIC quanto o "Procedimento Operacional Padrão: Perícia Criminal" do Senasp reforçam a validade das provas digitais em sentido amplo dentro dos processos judiciais como meios de provas, mormente quando aplicadas funções criptográficas unidirecionais para a garantia da integridade dos dados.

5.3 Jurisprudência

Por se tratar de um tema relativamente recente, a questão das provas digitais ainda não foi enfrentada de forma significativa nos nossos tribunais superiores. Assim como há pouca produção acadêmica sobre o assunto, também pouca jurisprudência veio à lume até o momento.

Quanto à assinatura em documentos digitais, o acórdão do Agravo de Instrumento 564.765, do Supremo Tribunal Federal, entendeu não ser aceitável a digitalização de assinatura manual como forma de comprovação de subscrição, uma vez que não possui qualquer certificado digital capaz de provar a sua originalidade. Admitir a simples digitalização abriria ampla avenida às fraudes em documentos digitais, ampliando a insegurança jurídica[3].

Em acórdão da Sentença Estrangeira Contestada 9.853, do Superior Tribunal de Justiça, ficou reforçado que os documentos digitalizados possuem a

[3] EMENTA: Ato processual: recurso: chancela eletrônica: exigência de regulamentação do seu uso para resguardo da segurança jurídica. 1. Assente o entendimento do Supremo Tribunal de que apenas a petição em que o advogado tenha firmado originalmente sua assinatura tem validade reconhecida. Precedentes. 2. No caso dos autos, não se trata de certificado digital ou versão impressa de documento digital protegido por certificado digital; trata-se de mera chancela eletrônica sem qualquer regulamentação e cuja originalidade não é possível afirmar sem o auxílio de perícia técnica. 3. A necessidade de regulamentação para a utilização da assinatura digitalizada não é mero formalismo processual, mas, exigência razoável que visa impedir a prática de atos cuja responsabilização não seria possível.
(AI 564765, Relator(a): Min. SEPÚLVEDA PERTENCE, Primeira Turma, julgado em 14/02/2006, DJ 17-03-2006).

mesma força probatória dos seus originais físicos e documentos com assinatura digital, nos termos do art. 11, da Lei 11.419/2006[4].

Ainda, o Agravo Regimental no Recurso Especial 1.335.192, do Superior Tribunal de Justiça, negou provimento ao recurso por ele não possuir certidão comprovando a assinatura eletrônica. Somente havia referência à expressão "documento eletrônico recebido na origem" na lateral do documento, o que, nas palavras da relatora, apenas significa que o documento foi peticionado eletronicamente, mas não que sua autoria tenha sido certificada[5].

Encerrando, o Agravo Regimental no Recurso Especial 249.395, do Superior Tribunal de Justiça, deu provimento ao agravo reformando o acórdão recorrido que não aceitou comprovante retirado da internet, sendo exigida a apresentação da via física. O amplo uso das tecnologias de informação na vida moderna ensejou a reforma do julgamento[6].

---

4 HOMOLOGAÇÃO DE SENTENÇA ESTRANGEIRA PROFERIDA NOS ESTADOS UNIDOS DA AMÉRICA. DIVÓRCIO CONSENSUAL. AUTENTICIDADE DOS DOCUMENTOS ELETRÔNICOS. CITAÇÃO POR EDITAL. AUSÊNCIA DE NULIDADE. VIOLÊNCIA DOMÉSTICA. 1. A sentença estrangeira, proferida pela autoridade competente, transitou em julgado, está autenticada pelo cônsul brasileiro e traduzida por tradutor juramentado no Brasil. Houve regular citação no processo alienígena (fl. 50), ademais a sentença estrangeira não ofende a soberania ou a ordem pública. 2. É tranquila a jurisprudência desta Corte no sentido da impossibilidade de se questionar a autenticidade dos documentos que são enviados eletronicamente ou digitalizados, ambos em obediência à forma prevista na Lei 11.419/2006. 3. No caso, trata-se de ação de divórcio em que a requerente relata já não ter nenhum contato com o réu há sete anos, valendo salientar a circunstância segundo a qual, havendo ela sido vítima de violência doméstica, a Corte americana expediu ordens proibindo o requerido "de abusar da requerente", de "entrar em contato com a requerente", bem como de "sair e permanecer fora da residência da requerente" (fls. 64-65). Não há, assim, razão alguma que justifique venha a autora a saber do paradeiro de seu ex-cônjuge, afigurando-se correta a citação por edital. 4. Homologação da sentença estrangeira deferida (SEC 9.853/EX, Rel. Ministro LUIS FELIPE SALOMÃO, CORTE ESPECIAL, julgado em 01/10/2014, DJe 28/10/2014).

5 AGRAVO REGIMENTAL NO RECURSO ESPECIAL. PROCESSUAL PENAL. PETIÇÃO DE RECURSO ESPECIAL APÓCRIFA. RECURSO INEXISTENTE. VÍCIO INSANÁVEL. PRECEDENTES. AGRAVO REGIMENTAL DESPROVIDO. 1. A expressão "Documento eletrônico recebido na origem" indica, literalmente, que a peça foi recebida já na forma eletrônica (sem que tenha sido digitalizada pelo Tribunal), não tendo o condão de confirmar a autenticidade da peça ou a existência de assinatura digital. 2. A jurisprudência desta Corte e do Pretório Excelso é pacífica no sentido de que os recursos sem assinatura, dirigidos às instâncias extraordinárias, são considerados inexistentes. Vício insanável, não sendo possível a abertura de prazo para a regularização do feito. Precedentes. 3. Decisão que se mantém por seus próprios fundamentos. 4. Agravo regimental desprovido (AgRg no REsp 1335192/PR, Rel. Ministra LAURITA VAZ, QUINTA TURMA, julgado em 03/12/2013, DJe 19/12/2013).

6 PROCESSUAL CIVIL. AGRAVO REGIMENTAL. AGRAVO EM RECURSO ESPECIAL NÃO CONHECIDO. DESERÇÃO. COMPROVAÇÃO DE PAGAMENTO DE CONTA/TRIBUTO. NÃO ACEITAÇÃO DO COMPROVANTE EXTRAÍDO DA INTERNET. ENTENDIMENTO SUPERADO EM RAZÃO DA AMPLA UTILIZAÇÃO DE MEIO ELETRÔNICO NA VIDA MODERNA. POSSIBILIDADE DE CONFERÊNCIA DOS DADOS LANÇADOS NO DOCUMENTO. NECESSIDADE DE SUPERAÇÃO DO ÓBICE. ÔNUS EXCESSIVO. AGRAVO PROVIDO. 1. Não é razoável impor à parte condições mais rigorosas para a comprovação do pagamento de conta ou tributo (taxas, inclusive) do que aquelas exigidas pelo mercado ou instituições públicas. 2. Para comprovação do preparo, deve ser considerado o uso de meios eletrônicos já incorporados ao cotidiano dos brasileiros, reputando-se válido o comprovante extraído da internet, tendo em vista a possibilidade de aferir se os dados nele lançados referem-se a pagamento relativo a processo específico. 3. Agravo regimental provido (AgRg no AREsp 249.395/SC, Rel. Ministro PAULO DE TARSO SANSEVERINO, Rel. p/ Acórdão Ministro JOÃO OTÁVIO DE NORONHA, TERCEIRA TURMA, julgado em 12/11/2013, DJe 25/02/2014).

Portanto, são poucas as decisões abordando o assunto provas digitais. Há a expectativa de que o uso mais extensivo do Sistema Processo Judicial Eletrônico e o aumento das relações jurídicas estabelecidas em meio digital assinadas eletronicamente venham a aumentar o número de ações que tenham o tema como objeto principal ou acessório. Mas não podemos dizer que nosso ordenamento jurídico esteja despreparado para enfrentar as questões que virão. As leis existentes são suficientes. Talvez nosso maior obstáculo seja o conhecimento dos operadores do Direito sobre as diversas possibilidades argumentativas que surgem diante do uso de provas digitais.

6 – Considerações finais

O presente trabalho debruçou-se sobre as contribuições da criptografia para o PJe e para a valoração da prova digital. Para cumprir o seu propósito, iniciou traçando um paralelo entre os sistemas de informação e os procedimentos judiciais. Ambos recebem *inputs*, processam os dados e entregam *outputs.* Nesse sentido, a criptografia surge como opção para implementar segurança da informação nos procedimentos jurídicos, garantindo, em última análise, segurança jurídica.

Passou-se, portanto, à explicação dos aspectos técnicos da criptografia fundamentais para a compreensão de como ela viabiliza os requisitos de segurança da informação, quais sejam, confidencialidade, integridade, autenticidade e não-repúdio. Nesse esforço, o primeiro objetivo específico foi alcançado.

Em seguida, foi descrito o papel da criptografia como pilar do PJe, pois, sem ela, o caminho para fraudes informáticas negaria qualquer efeito jurídico aos atos processuais praticados por meio da rede mundial de computadores.

Por fim, foram apresentados argumentos no sentido de reconhecer a validade jurídica de documentos eletrônicos e de provas digitais em sentido amplo como meios de prova admitidos em direito. Mais uma vez, isso só se tornou realidade em virtude da garantia de autenticidade e integridade emprestadas pela criptografia.

Quanto às limitações deste trabalho, nota-se que não se buscou enfrentar dados quantitativos para análise dos efeitos de implantação do PJe como de economia gerada nas Comarcas em que já foi implementado e de efeitos sobre a duração dos processos. Também não foi discutida a segurança dos algoritmos criptográficos utilizados para a produção de certificados eletrônicos, assinaturas digitais e resumos criptográficos. Outra questão não abordada foi o número de ações judiciais que tenham como objeto principal ou secundário as questões de autenticidade e integridade.

Portanto, deixa-se em aberto para futuros estudos análises quantitativas sobre os efeitos da implantação do PJe e sobre as ações judiciais discutindo autenticidade e integridade de dados digitais. Para a área mais atinente à criptologia, percebe-se boa oportunidade de discutir com maior profundidade a força dos algoritmos criptográficos empregados pelas Autoridades Certificadoras da ICP-Brasil,

bem como dos algoritmos de resumos criptográficos, notadamente o SHA-512 citado como referência pelo estudo do Senasp.

Sob o ponto de vista sociológico, foi possível perceber o obstáculo que as novas tecnologias enfrentam para serem implementadas na vida política de uma comunidade. Christiana e Veronese (2007) sintetizaram bem essa observação no artigo “Segredo e democracia: certificação digital e software livre”, como é possível observar no seguinte trecho:

> O tempo da tecnologia não é o tempo da política, ou seja, a implementação de uma solução técnica tem muitos empecilhos que não são de natureza tecnológica. Os artefatos tecnológicos, além de socialmente construídos, são aplicados mediante a execução de políticas específicas visando à sua utilização pela sociedade civil. Uma vez pronta, a tecnologia conhece, além do espaço técnico de sua produção, o espaço jurídico-institucional da implementação. [...] o processo de incorporação do espaço técnico da criptografia ao cenário político nacional [...] abrange mudanças, alterações e estratégias do espaço jurídico-institucional, sem o qual o artefato não integra o domínio público e nem adquire, consequentemente, visibilidade pública.

Não obstante esses desafios, conclui-se que o presente trabalho logrou êxito em apresentar aos operadores do Direito os aspectos da criptografia envolvendo o PJe e as provas digitais de modo a lhes entregar recursos argumentativos, seja qual for o seu papel nos procedimentos judiciais, na busca pelo ideal de justiça sustentado pelo princípio da segurança jurídica.

●

Referências bibliográficas

ALMEIDA FILHO, José Carlos de Araújo. **Processo Eletrônico e Teoria Geral do Processo Eletrônico: A Informatização Judicial no Brasil.** Rio de Janeiro. Forense, 2007.

ALVIM, José Eduardo Carreira; CABRAL JUNIOR, Silvério Luiz Nery. **Processo Judicial Eletrônico – Comentários à Lei 11.419/06**. Curitiba: Juruá, 2007.

BRASIL. Conselho Nacional de Justiça. Resolução nº 185, 18 dez. 2013. Institui o Sistema Processo Judicial Eletrônico - PJe como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento. Disponível em: <http://www.cnj.jus.br/busca-atos-adm?documento=2492>. Acesso em: 04 jun. 2017.

_____. Departamento de Segurança da Informação e Comunicações. Gabinete de Segurança Institucional da Presidência da República. Norma Complementar nº 21/IN01/DSIC/GSIPR, de 08 out. 2017. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf>. Acesso em: 02 jun. 2017.

_____. Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. **Diário Oficial da União**: Brasília, 18 dez. 2006.

_____. Lei nº 13.105, de 16 mar. 2015. Código de Processo Civil. **Diário Oficial da União**: Brasília, 17 mar. 2015.

_____. Medida Provisória Nº 2.200-2, de 24 ago. 2001. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm>. Acesso em: 30 maio 2017.

_____. Tribunal de Contas da União. **Acórdão nº 1.094/2012** – Segunda Câmara. Brasília: Tribunal de Contas da União, 2012. Disponível em: < https://contas.tcu.gov.br/pesquisaJurisprudencia/#/detalhamento/11/%252a/NUMACORDAO%253A1094/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/false/18 >. Acesso em 10 jun. 2017.

_____. Tribunal de Justiça do Distrito Federal e Territórios. **Portaria Conjunta nº 53**, de 23 jul. 2017. Disponível em: <http://www.tjdft.jus.br/publicacoes/publicacoes-oficiais/portarias-conjuntas-gpr-e-cg/2011/00053.html>. Acesso em: 03 jun. 2017.

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

CHIOVENDA, Giuseppe. **Instituições de direito processual civil.** Trad. da 2ª edição italiana por J. Guimarães Menegale. 3ª ed. São Paulo: Saraiva, 1969.

CLEMENTINO, Edilberto Barbosa **Processo Judicial Eletrônico – Em Conformidade com a Lei 11.419, de 19.12.2006**. Curitiba: Juruá, 2007

CONSELHO NACIONAL DE JUSTIÇA. **Certificação digital: você já tem a sua?** Disponível em: <http://www.cnj.jus.br/tecnologia-da-informacao/processo-judicial-eletronico-pje/certificacao-digital>. Acesso em 03 jun. 2017.

_____. **Processo judicial eletrônico.** Disponível em: <http://www.cjf.jus.br/observatorio/arq/cartilha_pje.pdf>. Acesso em: 05 jun. 2017.

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores.** Tradução de Glaydson Eduardo de Figueiredo. 3. ed. Porto Alegre: Bookman, 2006.

FREITAS, Christiana Soares; VERONESE, Alexandre. **Segredo e democracia: certificação digital e software livre.** Informática pública. v. 8 (2). p. 9-26. Belo Horizonte: Prodabel. 2007.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Benefícios.** Disponível em: <http://www.iti.gov.br/index.php/certificacao-digital/beneficios>. Acesso em: 03 jun. 2017.

KUROSE, James F.; ROSS, Keith W. **Rede de computadores e a internet: uma abordagem top-down**. Tradução de Arlete Simille Marques; revisão técnica de Wagner Luiz Zucchi. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

MARCACINI, Augusto Tavares Rosa. **Direito e informática: uma abordagem jurídica sobre a criptografia.** 1. ed. Rio de Janeiro: Forense, 2002.

MARCACINI, Augusto Tavares Rosa. **Direito e informática: uma abordagem jurídica sobre a criptografia**. Rio de Janeiro: Forense, 2002.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. **O novo processo civil.** São Paulo: Editora Revista dos Tribunais, 2015.

MIRANDA, Francisco C. Pontes de. **Comentários ao Código de Processo Civil.** 3ª ed. Rio de Janeiro: Forense, 1996.

PINHEIRO, Patricia Peck. **Direito digital.** 4. ed. São Paulo: Saraiva, 2011

SCHNEIER, Bruce. **Applied Cryptography – Protocols, Algorithms, and Source Code in C**. 2 ed. New York: John Wiley & Sons, Inc., 1996.

SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA. **Procedimento operacional padrão: perícia criminal**. Disponível em: < http://www.justica.gov.br/sua-seguranca/seguranca-publica/analise-e-pesquisa/download/pop/procedimento_operacional_padrao-pericia_criminal.pdf>. Acesso em: 05 jun. 2017.

STALLINGS, William. **Cryptography and Network Security – Principles and Practices.** 3 ed. New Jersey, EUA: Prentice Hall, 2003.

THEODORO JÚNIOR, Humberto. **Curso de Direito Processual Civil.** v. 1. 53ª ed. Rio de Janeiro: Forense, 2012.

TURBAN, Efraim; RAINER JR., R. Kelly; POTTER, Richard E**. Introdução a Sistemas de Informação**. 4. ed. Rio de Janeiro: Elsevier. 2007.

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION. **Digital heritage.** Diponível em: <http://www.unesco.org/new/en/communication-and-information/access-to-knowledge/preservation-of-documentary-heritage/digital-heritage/background/>. Acesso em 28 maio 2017.

VERONESE, Alexandre. **A política de certificação digital: processos eletrônicos e a informatização judiciária.** Revista de Direito de Informática e Telecomunicações – RDIT. v. 1. n.1, jul./dez. 2006. Belo Horizonte: Fórum, 2006.