FUNDAÇÃO DE ENSINO “EURÍPIDES SOARES DA ROCHA”
CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA - UNIVEM
CURSO DE DIREITO

RODRIGO DAL ROVERE GARBI

A INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA COMO FERRAMENTA PARA EFETIVAÇÃO DO PROCESSO ELETRÔNICO

MARÍLIA
2009

RODRIGO DAL ROVERE GARBI

A INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA COMO FERRAMENTA PARA EFETIVAÇÃO DO PROCESSO ELETRÔNICO

Trabalho de Curso apresentado ao Curso de Direito da Fundação de Ensino "Eurípides Soares da Rocha", mantenedora do Centro Universitário Eurípides de Marília – UNIVEM, como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador:
Prof. Dr. Mário Furlaneto Neto

MARÍLIA
2009

GARBI, Rodrigo Dal Rovere.

A Infra-Estrutura de Chaves Públicas brasileira como ferramenta para efetivação do Processo Eletrônico. / Rodrigo Dal Rovere Garbi; orientador: Mário Furlaneto Neto. Marília, SP: [s.n], 2009.

68 f.

Trabalho de Curso (Graduação em Direito) – Curso de Direito, Fundação de Ensino "Eurípides Soares da Rocha", mantenedora do Centro Universitário Eurípides de Marília – UNIVEM, Marília, 2009.

1. Direito 2. Informatização do Judiciário 3. Processo Eletrônico

CDD: 341.430285

FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"
MANTENEDORA DO CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA – UNIVEM
Curso de Direito

Rodrigo Dal Rovere Garbi
RA: 32052-8

A INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA COMO FERRAMENTA PARA EFETIVAÇÃO DO PROCESSO ELETRÔNICO

Banca examinadora do Trabalho de Conclusão de Curso apresentada ao Programa de Graduação em Direito da UNIVEM, F.E.E.S.R, para obtenção do Título de Bacharel em Direito.

Nota: 10,0

ORIENTADOR(A): _____
Mário Furlaneto Neto

1° EXAMINADOR(A): _____
José Eduardo Lourenço dos Santos

2° EXAMINADOR(A): _____
Christovam Castilho Junior

Marília, 24 de outubro de 2009.

Dedicatória

Primeiramente a Deus, criador de tudo e de todos, pois sem ele nada seria possível, aos meus pais que carrego sempre no coração, em especial a minha mãe que mesmo sem meu pai desde os meus 15 anos, perseverou e me tornou o que sou, e a minha linda e carinhosa esposa Lara que sempre me apóia e incentiva nesta jornada através do universo jurídico tão diferente do universo profissional onde atuo.

AGRADECIMENTOS

Aos professores que com seu trabalho, dedicação e insistência nos transmitiram seus conhecimentos, em especial ao professor Mário Furlaneto Neto que norteou este trabalho dentro de um mar de possibilidades me permitindo concluir mais esta etapa, a minha esposa Lara que me levou a universidade de direito e me motivou a levá-la até o final, aos familiares que por vezes sentiram minha falta enquanto me aprofundava nos estudos, aos amigos que nesta universidade conquistei e a todos aqueles, que de uma forma ou de outra, contribuíram para que esta jornada fosse concluída e mais um degrau superado.

Pode ser que um dia deixemos de nos falar...
Mas, enquanto houver amizade,
Faremos as pazes de novo.

Pode ser que um dia o tempo passe...
Mas, se a amizade permanecer,
Um de outro se há de lembrar.

Pode ser que um dia nos afastemos...
Mas, se formos amigos de verdade,
A amizade nos reaproximará.

Pode ser que um dia não mais existamos...
Mas, se ainda sobrar amizade,
Nasceremos de novo, um para o outro.

Pode ser que um dia tudo acabe...
Mas, com a amizade construiremos tudo novamente,
Cada vez de forma diferente.
Sendo único e inesquecível cada momento
Que juntos viveremos e nos lembraremos para sempre.

Há duas formas para viver a sua vida:
Uma é acreditar que não existe milagre.
A outra é acreditar que todas as coisas são um milagre.

Albert Einstein

GARBI, Rodrigo Dal Rovere. A Infra-Estrutura de Chaves Públicas brasileira como ferramenta para efetivação do Processo Eletrônico. 2009. 68 f. Trabalho de Curso (Bacharelado em Direito) – Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", Marília, 2009.

RESUMO

A evolução dos meios de comunicação, em especial a adoção da Internet como meio de comunicação em massa em escala planetária, está levando todas as áreas da sociedade a rever seus métodos e processos, com isso novas formas de interação surgem nesta seara afetando todos os indivíduos de forma direta ou indireta. No Poder Judiciário brasileiro não é diferente, acompanhando as novas tecnologias surgiu neste poder a figura do Processo Eletrônico, inserido em um projeto maior que é denominado informatização do judiciário, onde se busca a agilidade processual utilizando-se das novas tecnologias. Assim, por meio de uma revisão bibliográfica e jurisprudencial, a análise do processo eletrônico, dentro do contexto da informatização do Poder Judiciário, tem por objetivo verificar quais as diretrizes delimitadas pela lei de Informatização do Processo e as ferramentas que a informática disponibiliza para conferir segurança jurídica aos atos processuais. Conclui-se que o emprego da assinatura eletrônica, calcada no sistema de infra-estrutura de chaves públicas brasileira é capaz de conferir autenticidade ao documento jurídico e, via de conseqüência, segurança jurídica.

Palavras-chave: Direito. Informatização do Judiciário. Processo eletrônico.

LISTA DE ILUSTRAÇÕES

Figura 1 – Esboço da função HASH com aplicação de chave privada. 38
Figura 2 – Organograma da ICP-Brasil..... 46
Figura 3 – Cadeia Hierárquica da ICP-Brasil..... 47

LISTA DE ABREVIATURAS E SIGLAS

a.C.: Antes de Cristo

AC: Autoridade Certificadora

AC Raiz: Autoridade Certificadora Raiz

AR: Autoridade de Registro

ARPANET: Advanced Research Projects Agency Net. Rede da Agência de Projetos e Pesquisas Avançadas do EUA.

CEF: Caixa Econômica Federal

CF: Constituição Federal

CPC: Código de Processo Civil

d.C.: Depois de Cristo

DNS: Domain Name Service

DOU: Diário Oficial da União

e-governo: Governo Eletrônico

EUA: Estados Unidos da América

ICP: Infra-Estrutura de Chaves Públicas

ICP-Brasil: Infra-Estrutura de Chaves Públicas Brasileira

IMESP: Imprensa Oficial do Estado de São Paulo

MILNET: Military Network. Rede Militar dos EUA

NSA: National Security Agency. Agência de Segurança Nacional dos EUA

NSFNET: National Science Foundation Network. Rede da Fundação Nacional de Ciência dos EUA

OAB: Ordem dos Advogados do Brasil

RSA: Sistema de Criptografia Inventado por: Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman

SERPRO: Serviço Federal de Processamento de Dados

SRF: Secretaria da Receita Federal

TCP/IP: Transfer Control Protocol/Internet Protocol

TRF: Tribunal Regional Federal

UCLA: University of California, Los Angeles. Universidade da Califórnia, Los Angeles, EUA

UE: União Européia

WWW: World Wide Web. Grande rede mundial (de computadores) [tradução livre]

SUMÁRIO

INTRODUÇÃO 11

CAPÍTULO 1 – PROCESSO, DO ORAL AO ELETRÔNICO 14
1.1 O Processo Oral, Imediato 14
1.2 O Processo Reduzido a Termo, em Papel 14
1.3 O Processo Reduzido a Termo, em Meio Eletrônico 15
1.4 Direito da Informática ou Direito Eletrônico? 19
1.5 Processo Judicial Eletrônico 20
1.5.1 Tramitação de Processos Judiciais 22
1.5.2 Comunicação de Atos Processuais 22

CAPÍTULO 2 - PRINCÍPIOS JURÍDICOS E O PROCESSO ELETRÔNICO 25
2.1 Igualdade 25
2.2 Devido Processo Legal 27
2.3 Contraditório e Ampla Defesa 28
2.4 Oralidade 29
2.5 Publicidade 29
2.6 Instrumentalidade e da Economia Processual 30

CAPÍTULO 3 – SEGURANÇA NOS ATOS PRATICADOS ELETRONICAMENTE 33
3.1 Internet 33
3.2 Origem da Criptografia 35
3.3 Criptografia Simétrica 36
3.4 Hash 37
3.5 Criptografia Assimétrica 38
3.6 Criptografia Quântica 39
3.7 Chaves Públicas e Chaves Privadas 40
3.8 Assinatura Eletrônica e Assinatura Digital 41
3.9 Certificado Digital 42
3.10 Infra-Estrutura de Chaves Públicas em outros países 44
3.11 ICP-Brasil e a Infra-Estrutura de Chaves Públicas 45

CONSIDERAÇÕES FINAIS 51

REFERÊNCIAS 52

ANEXOS 54
A Method for Obtaining Digital Signatures and Public-Key Cryptosystems 54

INTRODUÇÃO

O computador é a grande invenção humana do século XX, no início apenas mais um aparelho eletro eletrônico com capacidade de efetuar cálculos numéricos inventado com o intuito bélico, que ao passar do tempo se tornou essa maravilhosa máquina com incontáveis utilidades. Essa nova máquina, que tanto nos fascina e auxilia, faz com que todos os homens, de forma direta ou indireta se tornem dependentes, pois, com elas houve um grande incremento na produção humana, seja em qualidade ou quantidade, assumindo uma posição definitiva na vida de todos.

A alta velocidade das transações feitas por computador pode ser presenciada em diversos ramos da sociedade, como as instituições bancárias, bolsas de valores, escritórios de contabilidade, escritórios de advocacia, pregões eletrônicos, lojas on-line, entre tantos outros. Hoje é inimaginável a vida sem essas máquinas, servindo a humanidade desde o controle de uma usina de energia nuclear até entretenimento e lazer.

Na esteira da revolução da informática foram criados novos métodos de comunicação, sendo o mais famoso a Internet, que hoje, pouco mais de duas décadas após sua criação, se tornou indispensável a diversos ramos da sociedade. A Internet possibilita a qualquer pessoa, em qualquer parte do mundo, ter contato ou estar virtualmente em outra localidade não importando a distância física que separa os interlocutores. Comunicação esta instantânea e agregando voz, dados e imagem numa única mídia.

Pensando nesse aumento de qualidade e quantidade, logo eficiência, o Poder Judiciário e outras esferas de poder, estão adotando a Internet como o novo meio para se praticar os atos processuais e administrativos. Atos estes, que antes necessitavam a presença física do advogado, juiz ou particular ao juízo ou órgão público onde o ato devesse ser praticado, e atualmente, podendo ser praticado do escritório ou de qualquer outro local onde se encontre, inclusive fora do país.

Essa adoção da Internet está sendo regulamentada em diversos dispositivos legais que estão em discussão desde a década de 1990 e outros já aprovados ou convertidos em lei, como a Lei nº 11.419/2006 e a MP nº 2.200-2/2001 que de forma incomum foi tornada permanente pela emenda constitucional nº 32/2001. Por se tratar de algo muito recente, para os padrões jurídicos, e de espantosa velocidade de mutação, a adoção destes novos métodos é gradual e sempre cercada de várias discussões, visto que há diversos projetos de lei em

tramitação nas duas casas do Congresso Nacional propondo diversas mudanças na atual forma prescrita pelos dispositivos retro mencionados.

Mas, para que essa nova forma de praticar os atos jurídicos seja possível é necessário que se garanta a identidade dos interlocutores e que ateste a validade do conteúdo enviado entre eles. Entra em cena então a certificação digital, a assinatura eletrônica em sua vertente assinatura digital e toda a criptografia por trás deste aparato tecnológico, garantindo a exata comunicação entre as partes. Será a certificação digital e a entidade certificadora por trás dela que atestarão a validade do ato jurídico praticado, dando a este ato autenticidade, integridade e validade jurídica.

Há no mundo, principalmente na Europa e nos Estados Unidos da América, implementações de programas de informatização dos atos governamentais que muito se assemelham ao ambicioso projeto brasileiro, trazendo o governo mais próximo ao cidadão e permitindo ao cidadão uma melhor concepção e fiscalização do governo. Mas este assunto generalizado de informatização governamental foge ao escopo deste trabalho que se focará apenas no que diz respeito ao Poder Judiciário, mais precisamente ao Processo Eletrônico e a autoria e autenticidade dos atos nele possíveis de serem praticados virtualmente.

Há agora, algumas questões que intrigam e levantam a desconfiança de todos que em um primeiro momento escutam sobre o uso da Internet como meio da prática processual, pois, sendo a Internet um local público por natureza, totalmente aberta e flexível, como poderemos garantir com total segurança que a comunicação não será violada? Como afirmar com a mais alta aceitação que o interlocutor que está praticando o ato é ele mesmo, e não um impostor? Como garantir que ao se transmitir uma petição do escritório ao Poder Judiciário esta não sofrerá modificações no percurso? São perguntas como essas que as próximas páginas buscarão respostas, seja na tecnologia ou nas limitações impostas pela lei, analisando também os algoritmos de criptografia utilizados e a ICP-Brasil que é o órgão oficial brasileiro de certificação, e os dispositivos de lei já publicados sobre o assunto.

Por meio de uma revisão bibliográfica e jurisprudencial, buscar-se-á enfrentar a questão do processo eletrônico, com objetivo de apontar as diretrizes elencadas na Lei de Informatização do Processo e enfrentar o sistema de chaves-públicas brasileira enquanto método garantidor da autenticidade e integridade documental.

Para tanto, no primeiro capítulo esboçamos um breve histórico da evolução formal do processo, caracterizando o que vem a ser processo eletrônico, que na realidade deveria ser

chamado de procedimento eletrônico, e quais os atos possíveis de serem praticados utilizando-se este novo método.

No capítulo 2 há o enfoque dos principais princípios jurídicos e constitucionais que quando aplicados ao processo judicial eletrônico podem sofrer algum tipo de readequação ou necessidade de nova interpretação. Neste capítulo apenas comparamos a adequação dos princípios entre o processo eletrônico e o processo convencional.

No último capítulo abordamos a opção brasileira por uma autoridade certificadora pública e centralizada, materializada na ICP-Brasil e a Infra-Estrutura de Chaves Públicas e exibindo casos de outras nações que implantam procedimento parecido. Na análise da ICP-Brasil focamos suas regras, organização interna e segurança proporcionada pela utilização da criptografia assimétrica e o certificado digital.

CAPÍTULO 1 – PROCESSO, DO ORAL AO ELETRÔNICO

1.1 O Processo Oral, Imediato

No início todos os processos eram orais e presenciais, exigia-se das partes a presença física incondicional como requisito processual, como condição da ação. Essa característica que remonta a época do império romano, com inicio aproximado em 754 a.C., é o inicio da solução dos conflitos operada pelo Estado, é a hetero tutela tomando o espaço da até então auto-tutela praticada pelas partes.

Nessa época todos os atos, sem exceção, eram compostos de debates orais, ou nas palavras de Clementino (2008, p. 39), “uma pequena peça teatral”. Não havia nenhuma forma de papel escrito ou documento que armazenassem os debates orais realizados ou as sentenças proferidas pelos magistrados ou pelos juízes que nesta época eram cargos distintos como nos alerta Clementino (2008, p. 38).

1.2 O Processo Reduzido a Termo, em Papel

Com o passar do tempo, mais precisamente na era romana identificada como *extraordinaria cognitio* em 294 d.C. até o início da era feudal no século X, foram se adotando formas de se anotar os atos processuais, passando a se utilizar o papel como meio de viabilização processual, onde tudo que era relevante deveria ser escrito, deveria ser *reduzido a termo*, inclusive adotando uma forma de petição inicial escrita.

> Consoante sói acontecer em termos evolutivos no Direito, este procedimento não substitui de plano o anterior, com ele convivendo por décadas, até sua revogação por Diocleciano, em 294 d.C. Nesse procedimento, o próprio Magistrado decidia a causa, sem remetê-la à figura do iudex. Esse procedimento foi largamente utilizado no Direito Justinianeu, em que os estudiosos encontram campo bastante fértil de estudo. Seus institutos em muito se assemelham ao nosso Processo civil, havendo previsão da apresentação do *libellus conventionis*, o qual podemos comparar à petição inicial do Processo moderno, no qual o autor expunha os fatos ao Magistrado, por escrito. (CLEMENTINO, 2008, p. 39, grifo do autor)

Durante a fase feudal da história, entre os séculos X e XII, há uma pausa na evolução jurídica, pois, segundo Clementino (2008, p. 41) “o direito medieval caracterizou-se por ser eminentemente prático e costumeiro, sem prévia teorização. Neste período, vigia uma pulverização da jurisdição, que somente voltou a ter unidade com o advento do absolutismo”.

Com a criação do Estado, em sua moderna concepção, retoma-se a evolução jurídica, que passa por diversas fases, mas seu detalhamento foge ao escopo deste texto, que neste momento se foca apenas na característica e forma de apresentação e evolução processual. Esta característica evoluiu desde a escrita manual na era romana e medieval, passando pela era da máquina de escrever inventada após a revolução industrial e chegando até aos documentos impressos por computadores da era atual.

Calmon (2007, p. 12, grifo do autor) nos mostra que o início da adoção da máquina de escrever também gerou discussões:

> Quando se começou a utilizar a máquina de escrever, muito se questionou sobre a validade jurídica dos documentos elaborados com essa engenhoca, *moderna*, mas ninguém podia duvidar de sua fidelidade, pois o datilógrafo lê cada letra imediatamente ao toque sobre a tecla correspondente. Igualmente, ao procederem à leitura tão logo seja concluído o ditado, os interessados podem apor suas assinaturas, conferindo imediatamente validade ao documento. Por conta dessa facilidade de utilização e de compreensão, venceram-se logo as resistências à validade da sentença datilografada, pois a assinatura do juiz em todas as laudas conferia-lhe a necessária autenticidade e todos podiam compreender a técnica de uma máquina de escrever.

Após a adoção do processo reduzido a termo, em nenhum momento deixou-se de utilizar o papel nas petições e atos processuais, pois só o que está escrito poderá ser anexado aos autos e dele fazer parte. Até testemunhos, de claro caráter oral e em alguns litígios única prova, deve ser reduzido a termo para fazer-se constar dos autos para assim ser considerado e tratado com o devido valor.

Em mais de 2000 anos mudou-se apenas a forma de registro dos atos, antes manuscrito, depois datilografado e agora digitado, mas sem alterar a sua essência, valor e obrigatoriedade. As ações processuais são essencialmente um bloco de papel registrando os pedidos e as defesas, as procurações, documentos, certidões e atos processuais registrados seqüencialmente e cronologicamente.

1.3 O Processo Reduzido a Termo, em Meio Eletrônico

Com a popularização dos computadores e a revolução causada pela massificação do uso da Internet após os anos 90, está em curso uma modificação social de grandes proporções, onde tudo e todos devem se adequar a nova realidade, e delas buscar obter proveitos.

O órgão judiciário não pode ficar de fora desse avanço, deve se alinhar aos anseios da sociedade e deve ir além disso, deve buscar formas de se beneficiar com a evolução e se adequar a nova realidade social, onde o computador e a Internet deixaram de ser um item de

status restrito a apenas classes sociais mais abastadas, para se tornar um item de primeira necessidade e disponível a maioria da população.

> Assim tem sido a sociedade desde o início do século XX. Uma invenção nova é apenas um luxo enquanto é novidade, mas com o passar dos tempos torna-se obrigatória sua utilização. Quem viveria hoje sem o chuveiro, a luz elétrica, o automóvel, o forno de microondas, o telefone, o telefone celular e o computador? Quem ainda entrega sua declaração de renda preenchendo um formulário de papel? (CALMON, 2007, p. 60).

Almeida Filho (2008, p. 23) nos mostra que a adoção de meios eletrônicos pelo ordenamento jurídico pátrio remonta à Lei 8.245/91 conhecida como Lei do Inquilinato, prevendo a prática de ato processual, no caso a citação, com o uso do *fac-símile* ou outro método similar. Contudo, por disposição expressa do texto legal, a citação somente será possível desde que prevista contratualmente.

Nesta esteira, o governo aprovou a Lei 11.419 de 19 de Dezembro de 2006 que introduz o Processo Judicial Eletrônico. Já em seu artigo 1º, esta Lei nos informa que o Processo Eletrônico se restringe a tramitação dos processos, comunicação de atos e transmissão de peças processuais, ficando claro que a mudança se dá apenas na forma e não no processo judicial em si. “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”.

> A nova lei viabiliza a informatização do rito ordinário da imensa maioria das ações, intimações, certificações, etc. Daí a necessidade de discutir qual modelo de *software* adotar. Essa decisão envolve mais do que questões jurídico-processuais. Envolve a segurança dos tribunais, a diminuição dos seus custos e a qualidade dos serviços e atinge os interesses privados do milionário mercado de produção de *softwares* para o Judiciário brasileiro. (FALCÃO, 2007, p. 37, grifo do autor)

Da informatização do judiciário, há muito que se decidir. Uma destas decisões se relaciona a qual software utilizar. O Judiciário faz boa escolha ao utilizar software livre, ao passo que este lhe garante propriedade sobre o software e também possibilidade de auditar as rotinas automatizadas no intuito de auferir a segurança e eficácia das rotinas. Também permite ao Judiciário não depender de apenas um provedor de serviços de software, permitindo buscar no mercado diversos parceiros, ou até, criar sua própria equipe interna.

Falcão (2007, p. 37, grifo do autor) nos mostra que outros órgãos do Governo Federal já aderiram ao software livre, e com isso estão conseguindo economias:

> O Serviço Federal de Processamento de Dados (Serpro), que processa grande parte das informações do Governo Federal, vem utilizando *software* livre, o

> que já promoveu uma redução de custos de cerca de R$ 14,8 milhões, tendo exigido investimentos em serviços e treinamento de apenas R$ 396 mil. E Embrapa, Dataprev, Marinha do Brasil, Instituto Nacional da Tecnologia da Informação e Ministério do Desenvolvimento Agrário estão usando algum tipo de *software* livre há pelo menos dois anos. A direção é esta. E está correta.

Agora, independente do software a ser utilizado, é necessário a discussão sobre os termos e formas da comunicação dos atos processuais.

A expressão '*reduzido a termo*' em meio eletrônico tem seu significado um pouco modificado, pois o processo toma esta característica quando, depois de redigido e verificado, é assinado digitalmente e enviado ao órgão competente por um meio eletrônico, e não mais em meio palpável como papel.

O artigo 1º, § 2º da Lei nº 11.419 de 19 de Dezembro de 2006 define o que vem a ser meio eletrônico em seu inciso I, e em seu inciso II nos informa, em linhas gerais, como será feita a comunicação eletrônica processual:

> § 2o Para o disposto nesta Lei, considera-se:
> I - meio eletrônico qualquer forma de armazenamento ou tráfego de documentos e arquivos digitais;
> II - transmissão eletrônica toda forma de comunicação a distância com a utilização de redes de comunicação, preferencialmente a rede mundial de computadores;
> (BRASIL, 2006)

O termo 'meio eletrônico' deve ser entendido como o meio de comunicação usando-se das técnicas e tecnologias empregadas na informática, ou seja, com o uso de computadores. Este entendimento é derivado do confronto de textos jurídicos brasileiros e estrangeiros como nos mostra Calmon (2007, p.55, grifo do autor)

> Não se pode basear apenas em dicionário uma definição para a expressão "meio eletrônico", dada a enorme abrangência do significado do adjetivo empregado. Valendo-se, porém, da comparação entre alguns textos legais brasileiros e estrangeiros e da doutrina técnica e jurídica, não se encontra dificuldade para compreender que a expressão "meio eletrônico" se refere à telemática, ou seja, à comunicação por intermédio de computadores.

Para se usar o meio eletrônico como meio de comunicação é necessário um método de reconhecimento da autoria do documento, o que é conseguido utilizando-se a assinatura eletrônica.

A assinatura eletrônica é gênero da qual a assinatura digital é espécie. A assinatura eletrônica engloba todo e qualquer meio de identificação do autor de uma mensagem eletrônica adotando-se o princípio da neutralidade tecnológica. Já a assinatura digital se firma

na tecnologia atual com o uso de criptografia assimétrica empregando o par de chaves, pública e privada, para garantir a origem e validade da mensagem eletrônica.

A assinatura digital sozinha garante a integridade do documento em relação à chave pública utilizada, mas nada afirma sobre se a chave pertence ao autor ali apontado. Para se resolver essa deficiência utiliza-se conjuntamente o certificado digital, onde um terceiro idôneo confirme se a chave pública pertence ao remetente da mensagem. Este terceiro no Brasil é a ICP-Brasil.

A assinatura digital, conjuntamente com o certificado digital, é o que garante ao processo eletrônico sua validade, autenticidade e integridade tal qual a rudimentar assinatura e a autenticação que o órgão recebedor o faz na versão em papel, o que explicaremos em detalhes mais adiante, pois não é assim tão simples.

O que se propõe com a adoção dos meios eletrônicos de trâmite processual, não é retirar a principal característica da ação que é a busca da resolução do conflito ou da tutela jurisdicional solicitada, também não será possível zerar o uso de papel, é tão somente tornar algumas partes do processo mais ágeis, descentralizadas geograficamente, e com isso acelerar o trâmite processual, buscando a satisfação do direito pleiteado em menor tempo possível.

> Em se tratando do Princípio da Celeridade, o Processo Eletrônico reduz o tempo de tramitação do Processo, abreviando igualmente a concretização do comando contido na sentença, restituindo partes mais rapidamente à paz social. (CLEMENTINO, 2008, p. 176)

Outra vantagem no uso do processo judicial eletrônico está na diminuição dos volumosos arquivos necessários para se armazenar os feitos após processados e julgados. Esses novos processos serão armazenados em computadores e poderão existir cópias em locais geograficamente distantes, evitando-se assim a perda acidental dos processos por falhas nos equipamentos de informática, ou até em caso de tragédias ocorridas ao local de armazenamento.

Trata-se de uma garantia que assegura o desenvolvimento processual de acordo com regras previamente estabelecidas, como diz Clementino:

> A adoção do Processo Eletrônico apenas confere nova roupagem ao Processo Judicial. O Processo Judicial Eletrônico deverá estar sujeito às mesmas formalidades essenciais que o Processo tradicional, no tocante a ser obedecido o procedimento legalmente previsto para a apuração da verdade, em que seja assegurado o contraditório e a ampla defesa, umbilicalmente ligados ao Princípio do Devido Processo Legal. (CLEMENTINO, 2008, p. 144)

A obediência ao Devido Processo Legal impõe que seja mantida a observância de um conjunto de normas que disciplinem a função jurisdicional do Estado, no que em nada se inova em relação ao tradicional Processo.

Além do Poder Judiciário, a lei de forma indireta também nos indica que as outras esferas de poder também devem seguir esta evolução, é o que nos aponta Marinoni (2007, p. 115-116) no trecho a seguir:

> [...], a lei recomenda o uso do meio eletrônico como forma preferencial para a comunicação de atos processuais entre órgãos do Poder Judiciário (cartas precatórias, rogatórias e de ordem) ou entre este e outros Poderes. Isto implica a determinação indireta de que essas estruturas disponibilizem, com prioridade, instrumentos capazes, em todas as suas esferas, de transmitir e receber essas comunicações. Por conta disso, é imperioso criar política pública de integração dos órgãos públicos, de forma a integrá-los todos à rede mundial de computadores e de os adequar às exigências da lei, para que possam receber e transmitir essas informações por meio eletrônico.

Assim, todos os órgãos públicos deverão buscar formas de se adequar as novas exigências legais. A integração a rede mundial de computadores permitirá um maior controle e transparência a todos os órgãos, e uma maior celeridade e eficiência de todas as esferas de poder: Executivo, Legislativo e Judiciário.

1.4 Direito da Informática ou Direito Eletrônico?

Direito da informática diz respeito apenas e respectivamente ao direito aplicado sobre aquilo que se pratica no uso de computadores, limitando sua aplicação apenas a ciência da informática. Mas atualmente, diversos equipamentos dito eletrônicos, são capazes de se comunicar com redes e também com a Internet, ficando de fora da terminologia “Direito da Informática” e, portanto, fora do raio de ação do referido direito.

É muito mais abrangente e didático adotar-se a terminologia “Direito Eletrônico”, pois esta abrange não apenas as comunicações e atos praticados com o uso de computadores, mas também tudo aquilo que de uma forma ou de outra empregue aparelhos eletrônicos para estas práticas. Assim, partilhamos da definição criada por Almeida Filho (2008, p. 42):

> [...] entendemos por Direito eletrônico o conjunto de normas e conceitos doutrinários, destinados ao estudo e normatização de toda e qualquer relação onde a informática seja o fator primário, gerando direitos e deveres secundários. É, ainda, o estudo abrangente, com o auxílio de todas as normas codificadas de direito, a regular as relações dos mais diversos meios de comunicação, dentre eles os próprios da informática.

Com o emprego desta nova terminologia estende-se a abrangência deste novo ramo do direito, e se aproxima da terminologia empregada pela Lei 11.419 que adota os termos “meio eletrônico”, “transmissão eletrônica” e “processo eletrônico”.

1.5 Processo Judicial Eletrônico

A informatização do Poder Judiciário, em cujo contexto se insere o processo eletrônico, é uma vertente de um programa governamental de descentralização dos atos públicos, denominado e-governo. Os princípios e diretrizes do e-governo estão expressos no trecho abaixo, extraído em seu sítio principal na internet:

> O desenvolvimento de programas de Governo Eletrônico tem como princípio a utilização das modernas tecnologias de informação e comunicação (TICs) para democratizar o acesso à informação, ampliar discussões e dinamizar a prestação de serviços públicos com foco na eficiência e efetividade das funções governamentais.
> No Brasil, a política de Governo Eletrônico segue um conjunto de diretrizes que atuam em três frentes fundamentais: junto ao cidadão; na melhoria da sua própria gestão interna; e na integração com parceiros e fornecedores.
> O que se pretende com o Programa de Governo Eletrônico brasileiro é a transformação das relações do Governo com os cidadãos, empresas e também entre os órgãos do próprio governo de forma a aprimorar a qualidade dos serviços prestados; promover a interação com empresas e indústrias; e fortalecer a participação cidadã por meio do acesso a informação e a uma administração mais eficiente.
> (GOVERNO ELETRÔNICO, 2009)

O e-governo é a iniciativa pública brasileira em utilizar os recursos tecnológicos disponíveis no intuito de dar transparência, eficiência e efetividade à coisa pública. Assim, a informatização do judiciário é o braço evolutivo proporcionado pelo e-governo aplicado ao Poder Judiciário, que se materializa na Lei de Informatização do Processo Judicial.

Com a aprovação da Lei nº 11.419 tem-se início a implementação da Informatização do Processo Judicial. Esta Lei é auto aplicável e determina que o Poder Judiciário implemente as medidas necessárias para que sua finalidade seja alcançada. Já em seu artigo 1º a lei limita sua abrangência:

> 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.
>
> § 1º Aplica-se o disposto nesta Lei, indistintamente, aos processos civil, penal e trabalhista, bem como aos juizados especiais, em qualquer grau de jurisdição.

> § 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)

Esta lei abrange as peças processuais, como as petições, contestações e sentenças, a comunicação dos atos processuais, entre eles as citações, intimações e cartas rogatórias, e também o trâmite processual. Abaixo, Calmon (2007, p. 54, grifo do autor) nos informa que não há ressalvas na abrangência temática desta lei:

> Não há que se ressalvar os processos que versem sobre os considerados direitos indisponíveis, nem tampouco os que tenham a participação da Fazenda Pública, do Ministério Público, de incapaz ou de jurisdicionado sem advogado (nos casos permitidos por lei).

Calmon (2007, p. 54) também nos alerta que "a divisão do processo em diversos ramos é decorrente de tradição e a doutrina internacional divide o processo apenas entre o civil e o penal". No Brasil, a doutrina dividiu o processo em diversos ramos como o administrativo, eleitoral, militar, trabalhista e tributário, mas ainda assim os processos são apenas civil e penal, e aqueles apenas especialidades destes. Nas palavras de Calmon (2007, p. 55), "Não há, pois, exceção, para a aplicação da nova Lei nº 11.419".

> 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.
>
> § 1º O credenciamento no Poder Judiciário será realizado mediante procedimento no qual esteja assegurada a adequada identificação presencial do interessado.
>
> § 2º Ao credenciado será atribuído registro e meio de acesso ao sistema, de modo a preservar o sigilo, a identificação e a autenticidade de suas comunicações.
> (BRASIL, 2006)

Há que se ressaltar que os atos praticados pelas partes só serão admitidos por meio eletrônico se utilizarem assinatura eletrônica, consubstanciada na assinatura digital e certificado digital emitido nos moldes da ICP-Brasil, e prévio cadastramento no Poder Judiciário.

1.5.1 Tramitação de Processos Judiciais

A tramitação de processos judiciais, segundo Calmon (2007, p. 52), nada mais é do que o caminhar do processo, os passos pelo qual o processo deve passar para se garantir seu processamento. Esses passos em nada se alteram, pois as exigências processuais não foram mudadas, apenas se ganha eficiência e agilidade.

> O processo começa com uma petição inicial dirigida ao juiz. Entregue em cartório, a petição é entregue ao juiz pelo escrivão. Depois de despachada, caso seja considerada apta, será ordenada a citação do réu. Daí o processo segue a prática concatenada de atos, que são praticados pelas partes, pelo juiz, pelo escrivão e pelos auxiliares, como perito, avaliador e oficial de justiça. Esse é o tramitar do processo. Com os autos de papel, o movimento físico é facilmente observado. Ora os autos estão conclusos, ora à disposição das partes, ora uma delas os retira do cartório, ora os autos estão com o perito e assim sucessivamente, até que chegue a seu termo, com a entrega do bem da vida àquele a quem o juiz tenha reconhecido ser o seu titular. (CALMON, 2007, p. 52)

Visto que a Tramitação do Processo Judicial nada mais é do que o caminhar do processo dentro de seu desenvolvimento natural, fica claro que o novo procedimento proposto pelo Processo Judicial Eletrônico em nada altera a sua essência processual, muda-se apenas a forma que passa a ser eletrônica, com ganhos em eficiência e agilidade.

A título de exemplificação, Freitas e Brotto (2008) nos exibe o caso de dois sistemas desenvolvidos para o Poder Judiciário, denominados e-proc (Sistema de Processo Eletrônico) e o e-cint (Citação e Intimação por meio eletrônico).

> O “e-cint” é um sistema de citação e intimação eletrônicas, dando ciência às partes e advogados que aderirem a esse canal de comunicação. É sistema interligado ao e-proc, sendo dele uma espécie, utilizada para intimar e citar igualmente as autoridades, advogados, peritos e partes que aderirem ao sistema. (FREITAS e BROTTO, 2008)

Freitas e Brotto (2008) especificam ainda o escopo do sistema e-proc: “O ‘e-proc’ refere-se ao sistema de peticionamento eletrônico, que objetiva o encaminhamento de petições e documentos via Internet, chegando diretamente à Vara endereçada”.

1.5.2 Comunicação de Atos Processuais

Na comunicação dos atos processuais, se incluem os atos praticados pelas partes, pelo juiz e pelo escrivão ou chefe de secretaria. Estes atos podem ser, por exemplo:

Declarações de vontade que produzem, modificam ou extinguem direitos processuais, sentenças, decisões interlocutórias, despachos, etc.

> Os atos processuais podem ser praticados pelas partes, pelo juiz e pelo escrivão ou chefe de secretaria. Os atos das partes consistem em declarações de vontade e produzem a constituição, a modificação ou a extinção de direitos processuais. São praticados oralmente (em audiência) ou mediante petições, arrazoados, papéis ou documentos entregues em cartório.
> Os atos do juiz consistem em sentenças, decisões interlocutórias ou despachos. (CALMON, 2007, p. 52)

Estes atos não sofreram modificações em sua essência e continuam os mesmos, mas a Lei 11.419 fez algumas adaptações no que se refere ao protocolo e aos prazos processuais. O protocolo antes autenticado sobre o documento, agora será eletrônico e deverá ser fornecido com a data e hora do envio do documento eletrônico. Os prazos são os mesmos, mas a norma processual, artigo nº 172, § 3º do Código de Processo Civil, nos informa que o prazo se finda ao término do horário de expediente, mas como a justiça manterá seus serviços informáticos disponíveis 24 horas do dia, a Lei nº 11.419 tornou tempestivos os atos praticados eletronicamente até as 24 horas do último dia do prazo.

> Lei 11.419 Art. 3º Consideram-se realizados os atos processuais por meio eletrônico no dia e hora do seu envio ao sistema do Poder Judiciário, do que deverá ser fornecido protocolo eletrônico.
> Parágrafo único. Quando a petição eletrônica for enviada para atender prazo processual, serão consideradas tempestivas as transmitidas até as 24 (vinte e quatro) horas do seu último dia.
> (BRASIL, 2006)

> Art. 172 CPC. Os atos processuais realizar-se-ão em dias úteis, das 6 (seis) às 20 (vinte) horas.
> § 1º Serão, todavia, concluídos depois das 20 (vinte) horas os atos iniciados antes, quando o adiamento prejudicar a diligência ou causar grave dano.
> § 2º A citação e a penhora poderão, em casos excepcionais, e mediante autorização expressa do juiz, realizar-se em domingos e feriados, ou nos dias úteis, fora do horário estabelecido neste artigo, observado o disposto no art. 5º, inciso Xl, da Constituição Federal.
> § 3º Quando o ato tiver que ser praticado em determinado prazo, por meio de petição, esta deverá ser apresentada no protocolo, dentro do horário de expediente, nos termos da lei de organização judiciária local.
> (BRASIL, 1976)

> Nota-se, então, que a Lei nº 11.419 não está promovendo qualquer alteração de caráter processual, mas sim promovendo significativa alteração do horário de expediente, uniformizando-o quando se tratar de comunicações por meio eletrônico.
> Tudo, então, lógico e coerente, pois permanece a regra do horário de expediente, mas considera-se que o computador tem expediente ininterrupto. (CALMON, 2007, p. 76)

Calmon (2007, p. 76), também afirma ser mais benéfico para as partes esta alteração dos prazos, mas entende ser necessária a implantação de regras da organização judiciária que facilitem o pagamento de custas e o cumprimento de outras formalidades, sob pena de que de nada adiantará o prazo de 24 horas para o envio de petições se as guias de recolhimento de taxas não puderem ser pagas.

CAPÍTULO 2 - PRINCÍPIOS JURÍDICOS E O PROCESSO ELETRÔNICO

Como em qualquer forma de execução de atos jurídicos e processuais, é necessário que se atente aos princípios jurídicos sob pena de nulidade dos atos processuais praticados. É imperioso que se observe os princípios basilares da CF, respeitando o Estado Democrático de Direito, e os princípios garantidores do processo e sua fruição.

Nesta ótica, passamos a analisar os principais princípios constitucionais e jurídicos aplicáveis ao Processo Eletrônico e sua aplicabilidade e observância dentro do procedimento Judicial Eletrônico.

2.1 Igualdade

A igualdade é um princípio constitucional, expresso no artigo 5º caput da carta magna, e como tal deve ser buscado e garantido a todo custo pelos operadores do direito e por todo o ordenamento jurídico, como nos informa e exemplifica Moraes (2006, p. 31):

> A Constituição Federal de 1988 adotou o princípio da igualdade de direitos, prevendo a igualdade de aptidão, uma igualdade de possibilidades virtuais, ou seja, todos os cidadãos têm o direito de tratamento idêntico pela lei, em consonância com os critérios albergados pelo ordenamento jurídico. Desta forma, o que se veda são as diferenciações arbitrárias, as discriminações absurdas, pois, o tratamento desigual dos casos desiguais, na medida em que se desigualam, é exigência tradicional do próprio conceito de Justiça, pois o que realmente protege são certas finalidades, somente se tendo por lesado o princípio constitucional quando o elemento discriminador não se encontra a serviço de uma finalidade acolhida pelo direito, sem que se esqueça, porém, como ressalvado por Fábio Konder Comparato, que as chamadas liberdades materiais têm por objetivo a igualdade de condições sociais, meta a ser alcançada, não só por meio de leis, mas também pela aplicação de políticas ou programas de ação estatal.

A busca pela modernidade e pela tecnologia é um caminho sem volta que nos permite fazer mais em menos tempo, mas também é um fator de segregação social. Vivemos em um país onde a maioria da população não tem computador, e dos que o possuem apenas uma parcela acessa a rede mundial de computadores de forma satisfatória.

> A diversidade de capacidade econômica do público a ser atingido impõe certas dificuldades. Nas relações de direito privado entre pessoas físicas, a utilização de tais recursos limitada pelo fato de a imensa maioria da população brasileira não ter Computador. Além disso, dentro os que o tem, uma grande parte não dispõe de acesso à Internet. (CLEMENTINO, 2008, p. 136)

Esta mesma preocupação quanto ao alcance da inclusão digital é esboçada por Freitas e Brotto (2008):

> [...] De forma que não basta apenas o investimento em tecnologias para um Judiciário mais célere e eficaz, se não há investimento na sociedade com políticas públicas para a informação, informatização, a fim de que a inclusão digital não se resuma em exclusão social.

Mas esta dificuldade social, com seus excluídos digitais, não deve ser vista como um empecilho, pois como a quase totalidade dos atos processuais deve ser praticada por advogado, e nesta condição, nas palavras de Clementino (2008, p. 137):

> [...] acaba por nivelar as partes também quanto ao aspecto de promover a sua inclusão digital, haja vista que o profissional do Direito, via de regra, encontra-se bastante familiarizado com o uso das novéis tecnologias, cujo domínio, aliás, é uma exigência cujo atendimento não pode, hodiernamente, desconsiderar.

Ainda, temos que considerar que não só advogados particulares usarão o Processo Judicial Eletrônico, mas a Fazenda Pública e o Ministério Público também deverão se utilizar dos novos procedimentos. Nesta posição, há que se ressaltar que o Princípio da Igualdade ficará prejudicado, haja vista que à Fazenda Pública e ao Ministério Público os prazos são contados em dobro e em quádruplo como indicado no artigo 188 do Código de Processo Civil, desequilibrando a balança da igualdade. Neste contexto, visto a maior celeridade e facilidade possibilitada pelo Processo Judicial Eletrônico, há a necessidade de que o dispositivo do artigo 188 do Código de Processo Civil seja revisto, e desejável, seja revogado.

> Por disposição legal, os prazos são dilatados e a doutrina vacila entre admitir tratar-se de uma garantia a uma inconstitucionalidade. Entendemos que a norma não mais tem seu objetivo legítimo, porque as vozes em defesa desta distorção tratam a Fazenda como necessitando de mais prazos por conta de uma infinidade de processos em que atua.
> A Fazenda, atualmente, tornou-se uma litigante contumaz. E com os novos meios informáticos colocados à disposição, nem mesmo a deficiência atribuída por muitos pode garantir o dobro, e, até mesmo, o quádruplo de prazo indicado no artigo 188 do CPC.
> A posição em que se encontra a Fazenda e o Ministério Público no sistema processual é uma violação ao princípio da igualdade. (ALMEIDA FILHO, 2008, p. 66)

Com isso, cabe aos legisladores e a todos os poderes buscar formas de garantir a igualdade e equilíbrio entre o Estado nas figuras da Fazenda Pública e do Ministério Público, e o povo. Não se pode existir um órgão público que tem função primeira a de fiscal da lei, e ao mesmo tempo estar acima da Lei.

E cabe ao governo por meio de planos de inclusão social propiciar a integração desse contingente de excluídos à tecnologia digital. Há programas públicos neste sentido, com o intuito de universalizar o uso de computadores e o acesso a Internet. Como exemplo, podemos citar os decretos nº 3.753 e nº 3.754 de 19/02/2001 que definem metas para a universalização de serviços de telecomunicações em escolas públicas de ensino médio e de ensino profissionalizante.

2.2 Devido Processo Legal

Este princípio é uma garantia de que o processo terá seu trâmite de forma pré-definida, regrada. Ele também garante dupla proteção ao indivíduo, atuando tanto no âmbito material de proteção ao direito de liberdade, quanto no âmbito formal, ao assegurar a paridade total de condições com o Estado como vemos no trecho abaixo:

> O devido processo legal configura dupla proteção ao indivíduo, atuando tanto no âmbito material de proteção ao direito de liberdade, quanto no âmbito formal, ao assegurar-lhe paridade total de condições com o Estado-persecutor e plenitude de defesa (direito a defesa técnica, à publicidade do processo, à citação, de produção ampla de provas, de ser processado e julgado pelo juiz competente, aos recursos, à decisão imutável, à revisão criminal). (MORAES, 2006, p. 93, grifo do autor)

O Devido Processo Legal é um princípio aglutinador de todos os princípios processuais explícitos e implícitos na CF, bem como previstos no Código de Processo Penal. Assim, só haverá a concretização do justo processo, se houver a observância do contraditório e ampla defesa, inocência, juiz natural e imparcial, promotor natural, publicidade dos atos processuais, razoabilidade no tempo do julgamento, etc.

Ainda dentro das garantias incluídas neste princípio, há também a razoável duração do processo e celeridade processual, que dentro do contexto processual eletrônico ganha novos contornos e valoração. O processo judicial eletrônico, nas palavras de Clementino (2008, p. 144), tem a ambição de imprimir maior celeridade e segurança aos Atos Processuais.

Mas como nos alerta Clementino (2008, p. 144), o Processo Eletrônico apenas confere nova roupagem ao Processo Judicial, pois este deverá estar sujeito às mesmas formalidades essenciais que o Processo tradicional:

> Destarte, a obediência ao Princípio do Devido Processo Legal impõe que seja mantida a obediência a um conjunto de normas que disciplinem a função jurisdicional do Estado, no que em nada se inova em relação ao tradicional Processo.

Sendo assim, não há danos a este princípio com a adoção do Processo Eletrônico, somente colhem-se frutos devido ao incremento dado a celeridade processual.

2.3 Contraditório e Ampla Defesa

Este princípio encontra-se inserido no rol dos Direitos Fundamentais e está expresso na carta magna de 1988 em seu artigo 5º, inciso LV. Sendo assim, deve o Estado prover todas as necessidades para que este direito seja garantido às partes. Mas como ajustá-lo a nova necessidade das assinaturas digitais, onde as partes devem possuir a assinatura digital para estar em juízo?

Ao que nos parece, alinhado as palavras de Almeida Filho (2008, p. 72), "entendemos que o processo eletrônico insere novo pressuposto processual, que é, exatamente, a necessidade da certificação digital para poder atuar no feito".

Sendo assim, é necessário que todos os advogados obtenham a assinatura digital para com isso poder praticar atos eletronicamente. Neste sentido, a OAB criou sua AC imediatamente subseqüente a AC CERTISIGN que por sua vez é certificada pela AC Raiz da ICP-Brasil.

A iniciativa da OAB consiste em substituir as carteiras profissionais comuns por uma baseada em SmartCard contendo a assinatura digital no formato A3 que exige a presença do interessado em adquirir a certificação. Este SmartCard se parece com um cartão de crédito bancário, mas com a presença de um chip eletrônico embutido. Neste chip encontra-se a chave privada do advogado e sua certificação digital, onde em conjunto, permitem assinar digitalmente qualquer documento ou mensagem eletrônica.

Desta forma, fica clara a posição de Almeida Filho (2008, p. 72) da qual aderimos:

> Entendemos que a conjugação do artigo 5º, II, da Constituição deva ser prestigiado, mas não podemos, por outro lado, impedir ao autor que se valha do seu direito de ação. É por esta razão que entendemos que novos pressupostos processuais são inseridos, diante do processo eletrônico.

Com essa nova exigência, cabe a todos os profissionais do direito se adequarem a nova necessidade, onde a OAB já está preparada para fornecer as assinaturas digitais conjuntamente com a carteira profissional do advogado.

2.4 Oralidade

O CPC em seu artigo 169 determina que em se tratando de processo eletrônico os atos praticados na presença do juiz devem ser armazenados em mídia digital em arquivo eletrônico inviolável. Essa premissa autoriza o uso de qualquer mídia digital, seja ela um documento, um arquivo de áudio ou um arquivo de vídeo, abrindo um leque de possibilidades antes inimaginável. Qualquer mídia digital que se use pode ser assinada digitalmente, garantindo assim seu conteúdo, autoria e validade jurídica nos moldes da ICP-Brasil.

> A substituição da forma oral pela forma escrita deu-se em razão de diversos fatores, mas principalmente por motivo da necessidade de registro das soluções dadas às demandas, para obstar-se a sua repetição sobre o mesmo objeto litigioso. O aumento expressivo da população somente ampliou essa necessidade, haja vista que hodiernamente a quantidade de feitos julgados supera a capacidade de memória de qualquer ser humano, diante do grande aumento populacional e do elevado grau de especialização das funções judicantes que se alcançou com o tempo (CLEMENTINO, 2008, p. 159)

Não só a transcrição do ato praticado oralmente deve ser considerado, mas também sua gravação, seja ela somente em áudio ou em áudio+vídeo.

Clementino (2008, p. 161) informa que o princípio da oralidade no Processo Judicial Eletrônico resta atendido quando:

> a) Reduz o número de Documentos escritos que instruem o Processo;
> b) Simplifica o ritmo processual;
> c) Garante a perenidade da prova oral na sua integralidade, por intermédio de gravação em arquivo eletrônico de fácil armazenamento.

Resta então dizer que este princípio não se encontra prejudicado no processo eletrônico, e sim, maximizado pelas novas possibilidades abertas pela utilização dos recursos informáticos e a possibilidade de armazenamento dos feitos em mídia digital.

2.5 Publicidade

Este princípio é de grande importância processual, pois decorre dele a garantia e a fiscalização do judiciário no tocante a vedação de julgamento por tribunais de exceção e até de abusos praticados pelas autoridades judiciárias.

Nas palavras de Moraes (2006, p. 299):

> A publicidade se faz pela inserção do ato no Diário Oficial ou por edital afixado no lugar próprio para divulgação de atos públicos, para conhecimento do público em geral e, conseqüentemente, início da produção de seus efeitos, pois somente a publicidade evita os dissabores existentes em

> processos arbitrariamente sigilosos, permitindo-se os competentes recursos administrativos e as ações judiciais próprias.
> A regra, pois, é que a publicidade somente poderá ser excepcionada quando o interesse público assim determinar, prevalecendo esse em detrimento do princípio da publicidade.

Mas a publicidade dos atos processuais sejam eles atos isolados ou todo o feito, no meio eletrônico assume novos contornos. A depender da forma de publicidade a ser permitida ou autorizada dos processos, será possível a sítios específicos como o Google[1], Yahoo[2], Bing[3] e outros desta categoria, catalogar estes processos, tornando o acesso simplificado a qualquer um que se achar interessado.

> Nesse passo, o presente estudo discute uma das imperfeitas facetas do diploma [Lei 11.419/2006], relativa à desmesurada publicidade dos atos processuais praticados nesse substrato, cujos efeitos repercutem diretamente em garantias constitucionais consagradas no Estado Democrático de Direito, quais sejam, a intimidade e privacidade do cidadão litigante em processo judicial. Por outro lado, paradoxalmente, a utilização da tecnologia no processo judicial é capaz de enaltecer a garantia da publicidade processual, baluarte essencial da democracia, possibilitando sua expressão otimizada. (PAULA, 2009, p. 18, grifo nosso)

> A publicidade excessiva, como vem ocorrendo hodiernamente e se ampliará com a inserção do Processo Eletrônico em nosso sistema processual, viola princípios constitucionais de relevante importância, como a da intimidade e o da própria personalidade. (ALMEIDA FILHO, 2008, p. 82)

Desta forma, há na aplicação deste princípio no Processo Judicial Eletrônico uma grande discussão ainda fervilhando, colocando em posição de conflito princípios e garantias constitucionais, que de um lado visam à proteção da intimidade e privacidade, e de outro, os pilares da democracia.

2.6 Instrumentalidade e da Economia Processual

O Princípio da Instrumentalidade diz respeito à forma de execução dos atos processuais, e no processo judicial eletrônico continua a ser respeitado, pois no processo judicial eletrônico apenas a forma dos atos processuais foi alterada, não a sua essência. Portanto, este princípio encontra-se aplicado aos atos eletrônicos tal qual o é no procedimento anterior, apenas sua forma foi modificada. Este princípio está implícito no Código de

[1] Sítio da Internet com característica de catalogar conteúdo em páginas que são rastreadas automaticamente por programas por ele desenvolvidos. É capaz de catalogar documentos pelo seu conteúdo.
[2] Idem.
[3] Idem.

Processo Civil ao menos nos dois artigos abaixo e deve ser respeitado independente da tecnologia empregada:

> Art. 154 CPC. Os atos e termos processuais não dependem de forma determinada senão quando a lei expressamente a exigir, reputando-se válidos os que, realizados de outro modo, lhe preencham a finalidade essencial.
> Parágrafo único. Os tribunais, no âmbito da respectiva jurisdição, poderão disciplinar a prática e a comunicação oficial dos atos processuais por meios eletrônicos, atendidos os requisitos de autenticidade, integridade, validade jurídica e interoperabilidade da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil. (BRASIL, 1973)

> Art. 244 CPC. Quando a lei prescrever determinada forma, sem cominação de nulidade, o juiz considerará válido o ato se, realizado de outro modo, lhe alcançar a finalidade. (BRASIL, 1973)

Em ambos os artigos fica latente que a forma não é importante, desde que o fim seja alcançado. No artigo 154, parágrafo único, há inclusive a previsão legal para que os tribunais utilizem o meio eletrônico para a prática e a comunicação oficial de atos processuais. Neste mesmo artigo encontramos a obrigatoriedade quando se utiliza dos meios eletrônicos de se atender aos requisitos da ICP-Brasil, ou seja, proceder à assinatura digital dos documentos.

> Desta forma, a atenção ao Princípio da Instrumentalidade resta atendida na utilização do Processo Eletrônico quando são dispensadas formalidades arcaicas e obsoletas em prestígio da efetividade do Processo. Não se pode olvidar que o Processo é simples meio e não um fim em si mesmo. (CLEMENTINO, 2008, p. 168)

Aliado ao Princípio da Instrumentalidade encontra-se intimamente ligado o Princípio da Economia Processual, que nas palavras de Clementino (2008, p. 168): “O Princípio da Economicidade está ligado à idéia de que o Processo Judicial deve ser barato, sem deixar de lado a exigência da celeridade e, principalmente, o ideal da Justiça”. Este ideário está expresso na CF em seu artigo 5º, inciso LXXVIII onde “a todos, no âmbito judicial e administrativo, são assegurados a razoável duração do processo e os meios que garantam a celeridade de sua tramitação”.

O princípio da Economicidade Processual não diz respeito apenas aos custos da ação em si, Portanova (2003, p. 25) apud Clementino (2008, p. 168) “expõe quatro diferentes facetas desse Princípio: a) economia de custos; b) economia de tempo; c) economia de atos e d) eficiência na administração da Justiça”.

> Desde os primórdios do Processo, no Direito Romano, já existiam os ancestrais das chamadas “custos do Processo”. À época exigia-se a prestação de caução, que era perdida pela parte vencida. Contudo mesmo eles dispensavam tal exigência daqueles que fossem comprovadamente pobres. Mas as custas do Processo não envolvem apenas o adiantamento de custos,

> mas também o custeio dos gastos com passagens para que o causídico possa, eventualmente, deslocar-se a variáveis distâncias, na busca dos interesses do seu cliente, além do pagamento de honorários periciais etc. (CLEMENTINO, 2008, p. 169, grifo do autor)

Analisando apenas o trecho exposto por Clementino, é possível observar pontos onde o Processo Eletrônico possibilita vantagens tanto em custos como em celeridade processual, pois, permite ao advogado executar os atos processuais sem a necessidade de se locomover ao fórum ou tribunal. E, uma vez praticado o ato, este instantaneamente estará a disposição do órgão jurisdicional sem a necessidade de qualquer ação por parte dos serventuários da justiça. Só este ponto já é de grande valia, pois além de reduzir o excesso de trabalho dos serventuários, reduz os custos do advogado e, portanto, do cliente.

> Desta forma, a atenção ao Princípio da Economicidade resta atendida na utilização do Processo Eletrônico quando:
> a) A sua adoção implica redução de custos em relação ao modelo anterior;
> b) Sua implementação resulta em maior celeridade na obtenção da prestação jurisdicional, o que, por via de conseqüência, diminui sensivelmente o custo da prestação jurisdicional;
> c) Pelo fato de tornar mais barato o acesso à Justiça, contribui para ensejar aos hipossuficientes a plena realização de seus direitos.
> (CLEMENTINO, 2008, p. 171)

Um ganho indireto desta economicidade está na valorização da visão externa do órgão jurisdicional, hoje tão malogrado, encontrando-se depreciado pela grande demora na entrega da tutela jurisdicional.

CAPÍTULO 3 – SEGURANÇA NOS ATOS PRATICADOS ELETRONICAMENTE

3.1 Internet

A Internet é uma grande rede de computadores que surgiu de um projeto menor chamado ARPANET – Advanced Research Projects Agency Net na UCLA - University of California, Los Angeles. Essa rede anterior era usada para interligar os laboratórios de pesquisa pertencentes ao Departamento de Defesa dos EUA.

Surgiu de uma necessidade militar, no auge da guerra fria, de se manter as comunicações mesmo que algumas conexões fossem perdidas como resultado de um bombardeio, por exemplo. Tornando a comunicação mais eficiente e descentralizada, armazenando a informação em diversos computadores espalhados pelo mundo.

Essa preocupação com a permanência da comunicação é a que permeou o projeto do embrião da rede, norteando o desenvolvimento de forma a se garantir que a comunicação só seria interrompida se todos os computadores, ou nós, da rede fossem destruídos.

Uma característica marcante do projeto da ARPANET é que os pacotes de dados enviados de um computador a outro não teriam rota fixa, ou seja, o computador de origem apenas cria o pacote e o envia ao nó mais próximo indicando o destino, este nó decide qual será o próximo nó e o encaminha, e assim sucessivamente até chegar ao destino indicado no pacote. Esta característica aliada a informações descentralizadas, em um ambiente de guerra, possibilitaria a manutenção de um sistema de informações e tecnologias militares essenciais.

Os nós principais da rede são chamados backbone[4], que são computadores de grande porte, mas cada computador conectado a rede passa a ser um nó dela da mesma forma.

Nas palavras de Clementino (2008, p. 69), é nítida a intenção de se garantir a comunicação sob qualquer circunstância: “A idéia que inspirava a rede é de que cada uma de suas partes pudesse funcionar como cérebro, sem que se estivesse vinculado a um único centro de armazenamento e processamento de dados”.

A rede é baseada em um protocolo de comunicação chamado TCP/IP – *Transfer Control Protocol/Internet Protocol*, que desmonta os dados a serem transmitidos em pequenos pacotes que são enviados ao destino usando-se a rede. O computador de destino, ao receber estes pacotes, reordena-os e remonta a informação originalmente enviada.

[4] Espinha Dorsal [tradução livre]

O protocolo TCP/IP é o responsável por controlar cada computador através de um número IP definido e não repetido na rede. Este número IP em sua versão padrão chamada IPv4 contém 4 partes de 8 bits compondo 32 bits totais, representados graficamente separados por pontos, como exemplo: 172.18.25.1, já a versão IPv6 é composta de 8 partes de 16 bits compondo 128 bits totais, representados graficamente separados por dois pontos ‘:’, como exemplo: 3ffe:6a88:85a3:08d3:1319:8a2e:0370:7344.

Mas estes endereços são complicados e difíceis de se memorizar, por isso a rede possui um método de conversão destes números para algo mais inteligível, que são os endereços de domínio no formato, por exemplo: www.fundanet.br, assim, quando um computador querer acessar um endereço de domínio, um serviço na rede do tipo DNS presente nos nós, faz a tradução do nome do domínio para o IP correspondente, e assim encontra o computador de destino.

O nome INTERNET só surgiu quando diversas universidades e laboratórios dos EUA adotaram a nova forma de comunicação. Estes novos participantes deram um novo sentido à rede, tornando-a um novo modo de difundir o conhecimento científico.

Em 1990 a rede separa-se em dois blocos, a MILNET, rede das organizações militares norte americanas, e a NSFNET, rede para os pesquisadores. Assim a ARPANET foi encerrada oficialmente, passando a se chamar INTERNET. Neste mesmo ano inicia-se a abertura comercial da Internet nos EUA e o Brasil se conecta a ela. A abertura comercial da Internet em solo pátrio só ocorre em 1995, ficando neste período inicial restrito as universidades.

No ano de 1992, Tim Berners-Lee cria a WWW – *World Wide Web* (Teia de Alcance Mundial), um sistema de hipertexto que permite a interligação de diversos documentos espalhados pela Internet. Deste conceito criado por Tim Berners-Lee nasce o navegador, hoje ferramenta indispensável ao uso da Internet. Em pouco tempo a Internet se confundiria com a Web, e também integrando outros serviços como o navegador e o e-mail.

Nas palavras de Santos (2006, p. 52), “Em sua fase embrionária, o acesso à internet era restrito a poucos. Hoje, a rede mundial de computadores se transformou no principal meio de comunicação, capaz de promover o alargamento da cidadania e a inclusão social”.

Mas a Internet não se resume apenas ao HTTP – Hyper Text Transfer Protocol, que dá suporte ao WWW e o protocolo POP e SMTP do e-mail, este são apenas duas das utilidades possíveis da rede. Existem outros, apenas a título de exemplificação, como o FTP – File Transfer Protocol usado para transferências de arquivos, o SSH - Security Shell usado

para se controlar máquinas remotamente e o HTTPS que é uma variante do HTTP, mas com segurança baseada em certificado digital.

3.2 Origem da Criptografia

Calmon (2007, p. 14, grifo do autor) nos informa com clareza a origem do termo e a utilidade da criptografia:

> Criptografia vem do grego *kryptos*, que significa esconder, ocultar, seguido de *graphein*, escrever. Criptografia, então, quer dizer *escrita oculta*, que resulta da adição de um código a uma linguagem conhecida. Esse código é normalmente denominado *chave* e somente as pessoas que o conhecem é que logram êxito em decifrar qualquer mensagem com ele utilizada. Em palavras mais simples, criptografia é uma *mensagem secreta*.

Seu uso remonta a antiguidade onde já se denota o temor em se manter o sigilo de uma informação ou de que uma mensagem pudesse ser interceptada, como nos mostra Calmon (2007, p. 15, grifo do autor):

> Os primeiros registros da criptografia remontam ao século XX antes de Cristo. Egito e Índia são exemplos de utilização dessas técnicas nos tempos antigos. Até mesmo o famoso *Kama-sutra*, de VATSYAYANA, relaciona comunicações secretas com uma das 64 artes que as mulheres deveriam conhecer e praticar. Encontram-se registros de que na civilização mesopotâmica utilizava-se a criptografia; como exemplo uma fórmula para fabricar esmaltes para louças de barro, datada de 1.500 a.C.

A estenografia é uma forma de ocultação de mensagens, mas se baseia na troca de letras ou palavras por símbolos. Essa associação entre as letras ou palavras e os símbolos, se restritas apenas aos interlocutores, consiste numa forma básica de ocultação da mensagem. Houaiss (2004) define estenografia como a "técnica de escrita que utiliza caracteres abreviados especiais, permitindo que se anote as palavras com a mesma rapidez com que são pronunciadas; taquigrafia, logografia, pasistenografia".

A criptografia e a estenografia são uma criação antiga da humanidade, já usada há muitos séculos no intuito de ocultar mensagens, como nos mostra Clementino (2008, p. 99):

> A Criptografia nasceu há muitos séculos, tendo-se desenvolvido amplamente desde seus primórdios: a Estenografia. Esta é registrada na maioria dos dicionários como sinônimo de Criptografia. Contudo, utilizar-se-á aqui o conceito utilizado por Singh, para quem esta difere da Criptografia por valer-se da ocultação da própria mensagem.

A criptografia é baseada na substituição ou transposição. A substituição consiste na troca de uma letra por outra de forma a embaralhar seu conteúdo, enquanto na transposição as letras são rearranjadas, gerando um anagrama.

3.3 Criptografia Simétrica

A mais comum das criptografias, baseada em uma mesma chave com capacidade para cifrar e para decifrar a mensagem.

A mesma fórmula utilizada para cifrar a mensagem era suficiente para decifrá-la. Por isso, na criptografia simétrica se utiliza apenas uma chave, e esta, deve ser de conhecimento de ambas as partes, remetente e destinatário.

Por se tratar de chave única, há um grande risco de que caia em mão erradas.

Com a evolução das técnicas matemáticas passou-se a se utilizar cálculos matemáticos para embaralhar a mensagem tornando mais difícil a sua interceptação e decodificação, mas ainda assim, utilizando apenas uma chave.

Durante o século XX se dá a grande evolução da criptografia, como nos mostra Clementino (2008, p. 99): “A Criptografia desenvolveu-se a passos largos durante e após a Segunda Grande Guerra, em razão das necessidades estratégicas”.

Evolução essa proporcionada pelo uso de máquinas, como a Enigma do alemão Arthur Scherbius, a Type X britânica e a Sigaba americana. Com o advento dos computadores, há um salto na utilização das técnicas criptográficas, tornado a vida dos criptoanalistas e dos criptógrafos mais agitada.

> O trabalho dos criptógrafos e criptoanalistas era incessante. Além das cifras Enigma os aliados tiveram que descobrir as chaves de Lorenz, máquina que era usada para codificar a comunicação entre Hitler e seus generais, muito mais complexa que a Enigma. Desse trabalho hercúleo surgiu o precursor do Computador moderno: o Colossus, composto por 1.500 válvulas eletrônicas, bastante mais rápidas do que os relés eletromecânicos que eram utilizados até então. ... Se, de um lado as máquinas eram usadas para se desvendarem as cifras, por outro, passou-se a empregá-las para criá-las, o que levou à exponenciação dos recursos de ambos: criptoanalistas e criptógrafos. (CLEMENTINO, 2008, p. 102 e 103)

Com essa evolução permitida pelos computadores e o barateamento da tecnologia, Clementino nos informa que com isso passou-se a utilizar chaves cada vez maiores na tentativa de se proteger a comunicação e permitiu o acesso de milhões de pessoas em todo o mundo a essa forma de tecnologia.

> O Governo americano, por intermédio da *National Security Agency* – NSA passou então a preocupar-se com a utilização de Criptografia pelos entes privados, entendendo por bem limitar o número de chaves a aproximadamente 100.000.000.000.000.000[5] (tecnicamente se fala em 56 bits, porque este número consiste em 56 dígitos quando escrito em linguagem binária). (CLEMENTINO, 2008, p.103, grifo do autor)

Mas, ao mesmo tempo que evoluem os computadores, mais fácil se torna a descoberta das chaves, pois computadores podem checar milhões de chaves em curto espaço de tempo, e a cada dia novos e mais potentes computadores são criados.

Ainda assim, o uso de chaves simples implica que o remetente e o destinatário as conheça, para assim desvendar a mensagem. Com isso temos um ponto fraco nesta prática que consiste no pré compartilhamento da chave. Nas palavras de Clementino (2008, p. 104): "A necessidade de compartilhamento dessa chave era o ponto fraco da Criptografia, pelo risco que esta caísse em mão erradas".

Surgia assim uma necessidade em se obter uma forma mais efetiva de se proteger a comunicação, ainda mais com o advento da Internet, que segundo Clementino (2008, p. 104), o grande fluxo de dados das mais diversas naturezas trafegando em grande velocidade pela rede, as energias empregadas para conseguir-se a superação do problema relativo às chaves cresceram muito.

3.4 Hash

Os algoritmos de Hash são usados para se conseguir uma assinatura do arquivo, uma forma de se efetuar cálculos sobre os dados de um arquivo ou mensagem e obter uma seqüência única de bits, normalmente inferiores a 512 bits, e comumente chamados de "check-sum".

É possível assinar documentos utilizando-se Hash associado a chaves assimétricas no intuito de se garantir a integridade de documentos. Desta forma, a inclusão ou retirada de apenas 1 bit do arquivo ou do "check-sum" é capaz de identificar que o documento foi alterado.

Esta forma de verificação não garante a confidencialidade do documento, mas é capaz de confirmar se o conteúdo foi adulterado ou não.

[5] O número de chaves possíveis em 56 bits é equivalente a 2^{56} = 72.057.594.037.927.936 combinações possíveis.

Figura 1 – Esboço da função HASH com aplicação de chave privada.

Como exposto na figura acima, a criptografia se aplica apenas ao resultado da função Hash, não criptografando o conteúdo do arquivo. O processo inverso é impossível tanto no caso da criptografia assimétrica empregada, quando na função Hash utilizada.

Seus formatos mais conhecidos são: MD4, MD5, SHA-1 e WHIRLPOOL. Nos formatos MD4, MD5 e SHA-1 já foram reportados métodos de ataque, o que significa que há falhas em sua segurança.

3.5 Criptografia Assimétrica

Na década de 1970, 3 pesquisadores norte americanos criaram o modelo Assimétrico de Codificação/Decodificação, utilizando um par de chaves, uma pública e outra privada. Mas, mesmo sendo os inventores da técnica, eles (Whitfield Diffie, Martin Hellman e Ralph Merkle) não conseguiram colocá-la em prática. Eles previram que para seu modelo funcionar era necessário a descoberta e utilização de “funções de mão única”, onde uma vez efetuado o cálculo de criptografia, o processo inverso não seria capaz de restaurar a mensagem.

Entendendo estas dificuldades, o trio: Ronald Rivest, Adi Shamir e Leonard Adleman, criaram o sistema RSA de criptografia, e nas palavras de Clementino, tornando-se a cifra mais influente da Criptografia moderna.

Como nos mostra Clementino (2008, p. 1005), uma das características do modelo assimétrico é que a chave utilizada para cifrar a mensagem, não é capaz de decifrá-la. É esta a principal característica que diferencia a criptografia assimétrica da criptografia simétrica.

> A criptografia assimétrica ou de chave pública, por seu turno, foi desenvolvida recentemente, a partir de estudos feitos nos anos 70 pelos pesquisadores norte-americanos Whitfield Diffie, Martin Hellman e Ralph Merkle, considerados os inventores dos conceitos de criptografia de chave pública. (MENKE, 2003).

O RSA baseia-se em um par de chaves onde uma delas é de uso privado e jamais deve ser divulgado. A outra de uso público podendo até constar de catálogo público como nos mostra Clementino (2008, p. 105):

> O sistema funcionava então da seguinte forma: o interessado em comunicar-se dispõe de duas chaves. Uma, é de apenas seu conhecimento, jamais necessitando revelá-la para quem quer que seja. Uma outra, de conteúdo disponível, podendo até constar de uma espécie de catálogo público. Quem quiser mandar uma mensagem sigilosa para alguém, bastaria buscar a Chave Pública dessa pessoa em um catálogo público. Dessa forma encriptaria a mensagem que somente poderia ser lida pelo destinatário, único a conhecer a Chave Privada apta a desencriptar a mensagem sigilosa.

Esse par de chaves é conseguido a partir de funções matemáticas modulares de mão única envolvendo a multiplicação de números primos. Quanto maior os números primos utilizados, maior a segurança.

> As "funções de mão única", baseadas em funções modulares idealizadas pelo referido trio[6] envolviam multiplicação de números primos grandes o suficiente para tornar praticamente impossível a operação inversa para descobri-los. O nível de segurança aumenta à medida que os números primos utilizados são maiores. (CLEMENTINO, 2008, p. 105, grifo do autor)

Com o uso dos computadores, a obtenção de números primos relativamente grandes se tornou uma tarefa fácil, e o cálculo criptográfico necessário a encriptação da mensagem pode ser feito em poucos instantes.

Mas como alerta Clementino (2008, p. 105), deverão ser utilizados números primos cada vez maiores para que assim se garanta a segurança desejada.

3.6 Criptografia Quântica

A Criptografia Quântica ainda é um sonho, pois os computadores quânticos necessários para se efetuar este tipo de criptografia ainda são apenas projetos. Clementino (2008, p. 106, grifo nosso) nos dá uma idéia do que será possível esperar da criptografia quântica:

> Acredita-se, todavia, que o destino de mais essa forma de Encriptação (Assimétrica) esteja fadada a ser decifrada quando se materializar o sonho ainda distante dos físicos e matemáticos quanto à construção do Computador Quântico que representaria um passo gigantesco no avanço tecnológico. Compara-se a distância tecnológica entre Computador quântico e os supercomputadores convencionais com distância que separa este de um ábaco quebrado. Dessa forma, nenhuma Cifra criada em um Computador

[6] Ronald Rivest, Adi Shamir e Leonard Adleman. Inventores do sistema RSA de criptografia.

> convencional resistiria à velocidade de processamento de um Computador quântico.

Ainda, Clementino (2008, p. 107) nos mostra que esta forma de criptografia quântica é o sonho dos Criptógrafos, e que um sistema de cifração assim restabeleceria a privacidade em seu grau máximo, e ainda, não seria apenas um sistema perfeito, mas absolutamente inquebrável por toda a eternidade.

3.7 Chaves Públicas e Chaves Privadas

Enquanto a criptografia quântica não se torna realidade, cabe usar o sistema mais confiável atualmente, o baseado no sistema RSA de criptografia, com seu par de chaves: A chave pública e a chave privada.

A chave privada do individuo deve ser mantida em absoluto sigilo, e de preferência, em um cartão protegido por senha ou equipamento que o leia e criptografe as mensagens sem interferência ou necessidade de se carregar a chave para a memória do computador.

A chave pública, como o nome já informa é pública, e pode inclusive acompanhar a mensagem cifrada. Neste caso, a mensagem poderá ser lida por qualquer pessoa, mas jamais poderá ser alterada.

A possibilidade de se divulgar a chave pública permite que se monte um banco de dados destas chaves. Desta possibilidade nasceu o projeto, em vários países, das autoridades certificadoras raiz.

No Brasil, por ordem e disposição legal da Medida Provisória nº 2.200-2, quem disponibiliza, armazena e verifica essas chaves públicas é a ICP-Brasil. Ela é capaz de gerar novo par de chaves ao indivíduo e será obrigada a armazenar em banco de dados público as chaves públicas de todos os nela registrados.

Com a chave pública armazenada na ICP-Brasil, qualquer um que queira verificar a autenticidade de um documento poderá requisitar a ICP-Brasil que confirme se a chave pública pertence ao remetente da mensagem.

Também é possível neste modelo, mandar mensagem cifrada a qualquer pessoa utilizando-se de sua chave pública. Desta forma, somente o detentor da chave privada, par daquela pública, será capaz de visualizar o conteúdo da mensagem. Nem mesmo o autor da mensagem será capaz de decifrar a mensagem que acaba de cifrar com a chave pública do destinatário.

3.8 Assinatura Eletrônica e Assinatura Digital

Não há na legislação brasileira uma definição pacífica do que seja Assinatura Eletrônica, mas há algum consenso de que assinatura eletrônica é gênero da qual a assinatura digital é espécie.

Nas palavras de Calmon (2007, p. 21, grifo do autor), "Assinatura (ou firma) é a identificação da pessoa mediante a aposição de seu nome ou sinal, é a escrita do nome de forma personalizada, buscando-se atingir dois objetivos: o reconhecimento do autor da assinatura e ser essa provida de estilo pessoal a ponto de dificultar a falsificação".

Assim, Assinatura Eletrônica é a aposição sobre um documento eletrônico de identificação pessoal inequívoca, privilegiando a neutralidade tecnológica, e nas palavras de Calmon (2007, p. 21), sem "fazer referência a uma tecnologia específica, sob pena de se tornar rapidamente uma definição ultrapassada".

Neste sentido, Calmon (2007, p. 21 e 22) nos informa que a UNCITRAL - Comissão das Nações Unidas Para Leis de Comércio Internacional estabelece na Lei Modelo Sobre Comércio Eletrônico:

> Que se considera assinado eletronicamente um documento quando for utilizado algum método para identificar a pessoa e indicar sua aprovação para a informação contida na mensagem eletrônica e tal método seja tão confiável quanto seja apropriado para os propósitos para os quais a mensagem foi gerada ou comunicada, levando-se em consideração todas as circunstâncias do caso, incluindo qualquer acordo das partes a respeito.

Quanto a Assinatura Digital, esta é derivada diretamente da Assinatura Eletrônica e deve respeitar os princípios nela descritos. A Assinatura Digital é dependente da tecnologia atual e dela faz uso, baseando-se na tecnologia de chaves assimétricas.

Para se assinar digitalmente um documento é necessário a utilização por parte do remetente, de sua chave privada e da chave pública do destinatário. Enquanto que o destinatário necessita de sua chave privada e da chave pública do remetente.

Consideremos que 'A' tem seu par de chaves E_A e D_A. Onde E_A é sua chave pública e D_A chave privada. 'B' também tem seu par de chaves E_B e D_B.

Para 'A' enviar um documento assinado a 'B', ele deve pegar sua mensagem 'M' e aplicar sobre ela sua chave privada D_A obtendo a mensagem cifrada C. Deve ainda aplicar sobre C a chave pública de 'B' denominada E_B. Resumindo, a mensagem assinada digitalmente ficará da seguinte forma: $C = D_A(M) \rightarrow M_{\text{Assinada}} = E_B(C)$.

‘B’ ao receber a mensagem, deverá fazer o processo inverso para poder obter a mensagem original e atestar a origem, ou seja: Aplica sobre a mensagem assinada sua chave privada obtendo desta forma a mensagem C, e sobre esta deve aplicar a chave pública de ‘A’ para obter a mensagem M original. Resumindo: $C = D_B (M_{Assinada}) \rightarrow M = E_A(C)$.

‘B’, armazenando o par M e C, a mensagem original e a mensagem cifrada por ‘A’, garante a integridade e identidade do remetente. É impossível a ‘B’ alterar a mensagem C, pois só conseguirá C se tiver a chave privada de A, D_A. O par M e C é único, e a autoria não poderá ser negada por ‘A’.

Esta criação garante a autenticidade e autoria na entrega de documentos, o que facilita o andamento dos processos eletrônicos, mas ainda há espaço para possíveis fraudes, como alerta Calmon (2007, p. 27):

> A utilização da técnica da criptografia assimétrica para a elaboração da assinatura digital, caracterizada por uma chave privada e uma chave pública, ambas do remetente da mensagem, deixa espaço para uma sutil indagação: como o destinatário da mensagem pode ter certeza de que as chaves pública e privada utilizadas pertencem realmente ao remetente?

Desta forma, para que se evite fraudes, entra em cena o Certificado Digital expedido por um terceiro confiável pelas partes que associará o Certificado Digital ao autor da mensagem eletrônica assinada digitalmente.

3.9 Certificado Digital

O Certificado Digital é um arquivo de computador, como vemos na definição encontrada na enciclopédia Wikipédia, que normalmente acompanha intrinsecamente a mensagem ou documento certificado. Uma vez certificado uma mensagem ou documento, o Certificado Digital do remetente sempre se encontrará em anexo.

> O certificado digital é um documento eletrônico assinado digitalmente por uma terceira parte confiável que associa o nome e atributos de uma pessoa a uma chave pública. O fornecimento de um certificado digital é um serviço semelhante ao de identificação para a expedição de carteiras de identidade. O interessado é identificado mediante a sua presença física pelo terceiro de confiança – com a apresentação dos documentos necessários - e este lhe emite o certificado digital. (MENKE, 2003)

Abaixo temos o que a Lei nº 11.419 de 19/12/2006 que dispõe sobre a Informatização do Processo Judicial espera para que se garanta a identificação inequívoca do signatário dos atos praticados em meio eletrônico:

> 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)

Deste artigo extraímos que não somente a Assinatura Digital é esperada, mas também que esta esteja associada a um Certificado Digital expedido por Autoridade Certificadora credenciada.

O procedimento da assinatura eletrônica descrito no tópico anterior, aplicado ao documento, ainda precisa de um terceiro aceito pelas partes que se comunicam para confirmar a autoria e autenticidade do documento, atestando a origem e dando credibilidade ao documento eletrônico. Para que este terceiro atue, é necessário que o documento contenha um Certificado Digital de propriedade do remetente, expedido pelo terceiro, onde se encontre seus dados de identificação e sua chave pública.

> O certificado digital é um documento eletrônico assinado digitalmente por uma terceira parte confiável que associa o nome e atributos de uma pessoa a uma chave pública. O fornecimento de um certificado digital é um serviço semelhante ao de identificação para a expedição de carteiras de identidade. O interessado é identificado mediante a sua presença física pelo terceiro de confiança – com a apresentação dos documentos necessários - e este lhe emite o certificado digital. (MENKE, 2003).

Assim, quando o remetente deseje mandar um documento ou mensagem assinada, este agrega ao documento ou mensagem seu Certificado Digital e o encripta usando o método descrito acima. O destinatário ao receber o documento ou mensagem, solicita ao terceiro que verifique a autenticidade e validade do documento ou mensagem. O terceiro, checará o Certificado Digital juntamente com a chave pública do remetente confirmando se o par pertence realmente ao remetente, e após, atesta a veracidade do documento ou mensagem.

> 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 na 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. (MENKE, 2003, grifo do autor).

Este terceiro certificador no Brasil é um órgão público criado especificamente para este fim, instituído pela Medida Provisória nº 2.200-2 de 24 de agosto de 2001 (DOU 27.08.2001), denominado Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil em seu 1º artigo.

3.10 Infra-Estrutura de Chaves Públicas em outros países

Há no mundo, principalmente na Europa (primeiramente na Alemanha e depois na UE) e nos Estados Unidos da América, implementações de sistemas de infra-estrutura de chaves públicas que em muito se assemelham ao modelo brasileiro. O modelo alemão é muito parecido com o modelo brasileiro, colocando um órgão público como Autoridade Certificadora Raiz do sistema de chaves públicas.

> Na Europa, a Alemanha foi o primeiro país a editar uma lei específica sobre o tema. A *Signaturgesetz*, de 1º de agosto de 1997 introduziu as condições estruturais para a adoção das assinaturas eletrônicas (*Rahmenbedingungen für elektronische Signaturen*) naquele país. Já sob a égide desta lei, no seu parágrafo quarto, alínea 1, o legislador alemão previa a obrigatoriedade de os prestadores de serviços de certificação digital obterem uma licença perante o órgão público competente para que pudessem iniciar as suas atividades. (MENKE, 2003).

Nos Estados Unidos da América, pela sua característica federalista e o alto grau de independência dos estados federados, não ficou definido um órgão público como AC-Raiz, existindo diversas implementações dentro daquele país, inclusive com mais de uma AC por estado da federação. Esta opção adotada gera uma multiplicidade de ACs sem a necessidade de se garantir a interoperabilidade e permitindo até a adoção de tecnologias totalmente incompatíveis, dificultando assim a tentativa do governo central norte americano de integrar as ACs existentes.

> Curiosamente, há que se ressaltar que nos Estados Unidos da América o desenvolvimento e a expansão das infra-estruturas de chaves públicas se deu de forma bastante desorganizada de sorte que hoje em dia são diversas as ICPs em funcionamento naquele país, com base tanto em iniciativas governamentais quanto em iniciativas privadas.
> As razões desse fenômeno são diversas, sendo que um dos motivos principais é o fato de que a autonomia dos estados federados fez com que cada unidade da federação editasse a sua própria lei sobre assinaturas digitais

> e matérias afins, sem que houvesse uma harmonia principiológica permeando esses diplomas.
> Todavia, cientes de que "PKI is no good if you are only talking to yourself", os norte-americanos há alguns anos promoveram a iniciativa do projeto *Federal Bridge Certification Authority*, que tem por escopo fundamental viabilizar a intercomunicação entre os titulares de certificados digitais que adquiriram as suas chaves de Autoridades Certificadoras diversas. Em que pese os esforços, os próprios envolvidos no projeto têm reconhecido que a iniciativa se transformou numa "empreitada que tem sido marcada pelo lento progresso". (MENKE, 2003, grifo do autor).

É clara a vantagem de se ter uma certificadora raiz regulamentada pelo Estado, pois nas palavras de Menke (2003), imprime maior confiança e credibilidade ao sistema, pois se tem uma garantia maior quanto aos procedimentos técnico-administrativos que serão empregados na atividade.

Outra vantagem da padronização e centralização da ICP em um órgão estatal está na possibilidade de se firmar acordos internacionais que possibilitem o reconhecimento recíproco de certificados digitais.

> Daí a razão de ser mais racional e de resultados certamente melhores a implementação, desde o princípio, de uma ICP nacional. Outro aspecto é que, havendo uma ICP mais abrangente, como são a brasileira e a alemã, torna-se bem mais viável e atraente a celebração de acordos internacionais de reconhecimento recíproco de certificados digitais, o que possibilitará transações eletrônicas internacionais mais seguras, entre empresas, e entre consumidores e empresas. (MENKE, 2003).

É clara a vantagem em se padronizar e centralizar os métodos de certificação digital, e colocando esta atividade a cargo de uma entidade certificadora estatal confere maior credibilidade e transparência ao modelo adotado. Desta forma possibilita-se interoperabilidade entre as ACs nacionais que estão vinculadas a AC-Raiz a cargo da ICP-Brasil e também permite com maior facilidade a interoperabilidade da AC-Raiz e outras ACs internacionais, como o caso Alemão que tanto se assemelha ao adotado pelo Brasil.

3.11 ICP-Brasil e a Infra-Estrutura de Chaves Públicas

Começamos analisando a Medida Provisória nº 2.200-2 de 24 de agosto de 2001, este é o marco inicial dado pelo governo no sentido de criar uma infra-estrutura segura de chaves públicas garantidora da identidade inequívoca dos interlocutores em uma comunicação ocorrida em meio eletrônico.

Por força da emenda constitucional nº 32 de 11 de setembro de 2001, artigo 2º, todas "as medidas provisórias editadas em data anterior à da publicação desta emenda continuam

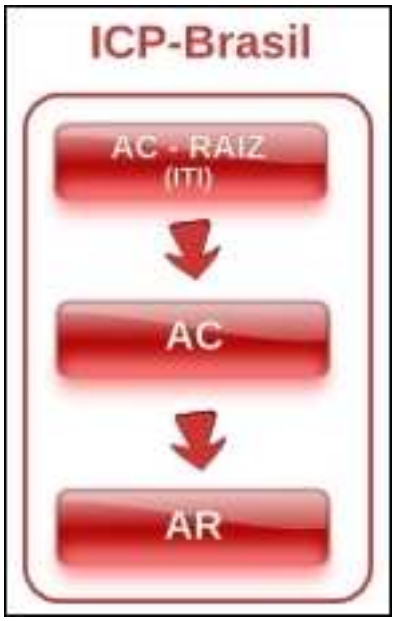
em vigor até que Medida Provisória ulterior as revogue explicitamente ou até deliberação definitiva do Congresso Nacional". Do entendimento desta emenda constitucional, a Medida Provisória nº 2.200-2 passa a ser então uma "Medida Permanente", não necessitando ser reavaliada pelo Congresso Nacional.

Esta "Medida Permanente" nº 2.200-2 cria a Infra-Estrutura de Chaves Públicas Brasileira a ICP-Brasil, entidade governamental responsável pela autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica. Sua criação foi indispensável para o início da informatização do judiciário, criando as regras pelas quais se garantirá a segurança da comunicação, valendo-se para tanto, de chaves criptográficas que serão utilizadas na validação via assinatura eletrônica do documento ora enviado.

> MP 2.200-2 Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR. (BRASIL, 2001)

A ICP-Brasil é organizada conforme o previsto no artigo 2º da referida Medida Provisória, composta de uma entidade certificadora raiz – AC Raiz, de entidades certificadoras – AC e de autoridades de registro ARs. Graficamente representada pela figura abaixo:

Figura 2 – Organograma da ICP-Brasil



Fonte: Sítio do Instituto Nacional de Tecnologia da Informação

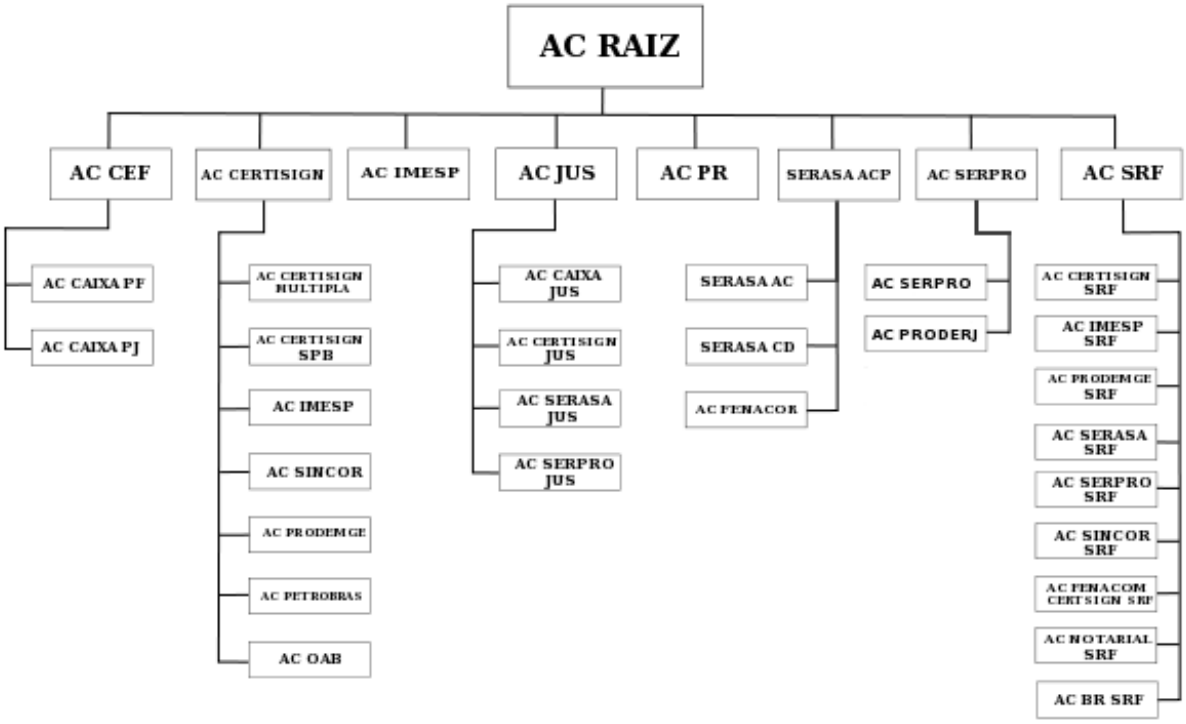
Respeitando o organograma definido na Medida Provisória nº 2.200-2, a ICP-Brasil se organizou, se estruturou e criou diversas ACs, cada uma com abrangência fixa e

determinada, cada uma com seu universo de usuários. A mesma MP também delimitou as funções de cada ente do organograma acima, determinando que a AC Raiz não possa emitir certificados ao usuário final e cabe a ela executar a fiscalização e auditoria das ACs e ARs.

> MP 2.200-2 Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.
> Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final. (BRASIL, 2001)

A MP, em seu artigo 8º: “Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicas e as pessoas jurídicas de direito privado.”, permitiu que pessoas jurídicas de direito privado pudessem se credenciar como ACs e ARs.

Figura 3 – Cadeia Hierárquica da ICP-Brasil



Fonte: Sítio do Instituto Nacional de Tecnologia da Informação

Acima está graficamente exposta a cadeia hierárquica atual, com base na AC Raiz que compõe a ICP-Brasil.

Toda esta estrutura foi montada no intuito de se dividir as ACs por área de atuação. Criando ACs para a CEF (AC CEF) que é uma estatal, a CERTISIGN[7] (AC SERTISIGN) que é uma empresa privada, para a IMESP (AC IMESP), para o Poder Judiciário (AC JUS), para a Presidência da República (AC PR), para a SERASA EXPERIAN[8] (AC SERASA) que foi a primeira empresa privada a ser homologada pela ICP-Brasil, o SERPRO (AC SERPRO) e a SRF (AC SRF). Mas o que vem a ser uma ICP? Menke (2003, grifo do autor) conceitua a infra-estrutura de chaves públicas como:

> [...] um sistema que tem por finalidade precípua, mas não exclusiva, atribuir certificados digitais (e conseqüentemente assinaturas digitais) a um universo de usuários. Em realidade, além de fornecerem estes documentos eletrônicos às pessoas naturais, aos órgãos e às entidades públicas e privadas, os entes que compõem uma ICP - os terceiros de confiança – desempenham a tarefa de gerenciar o ciclo de vida dos certificados, uma vez que a qualquer momento pode haver necessidade de revogar e emitir novos certificados, como no caso de comprometimento da chave privada de determinado titular de um certificado digital.

Com o advento da Lei nº 11.419 de 19 de dezembro de 2006 o governo dá um novo e significativo passo na adoção dos meios eletrônicos para tramitação de processos judiciais, comunicação e tramitação de peças processuais. É esta lei que regulamenta a nova forma de tramitação dos autos processuais e altera dispositivos do código de processo civil para contemplar as inovações. Esta lei afirma que todos os atos praticados eletronicamente deverão ser assinados digitalmente utilizando-se de uma entidade certificadora, a ICP - Brasil, que confirmará a identidade dos interlocutores para assim garantir a autenticidade, a integridade e a validade jurídica dos documentos e atos praticados por meio eletrônico.

> A expedição de certificados de autenticação é uma atividade que nasceu despretensiosamente, pois não se imaginava desde o início que iria torna-se um novo modo de agir da sociedade; mas hoje ela é uma prática disseminada nas relações pessoais, econômicas, privadas e públicas; e em pouquíssimo tempo se tornaria tão essencial à vida humana quanto já tem sido a Internet. (CALMON, 2007, p. 30).

Esses documentos assinados digitalmente ainda dependem de uma entidade que os valide e ateste a identidade dos interlocutores, conferindo ao documento eletrônico a real validade. Menke (2003) conceitua o certificado digital da seguinte forma:

---

[7] Empresa privada de certificação digital
[8] Idem

> O certificado digital é um documento eletrônico assinado digitalmente por uma terceira parte confiável que associa o nome e atributos de uma pessoa a uma chave pública. O fornecimento de um certificado digital é um serviço semelhante ao de identificação para a expedição de carteiras de identidade. O interessado é identificado mediante a sua presença física pelo terceiro de confiança – com a apresentação dos documentos necessários - e este lhe emite o certificado digital.

Não interessa saber se um Documento Eletrônico teve origem em um determinado computador, porque ainda nesse caso poder-se-iam levantar questionamentos a respeito da autenticidade. Deve-se garantir a autoria inequívoca do documento, ou seja, qual o signatário deste, não importando em qual computador ou localidade está.

> A certeza da Autenticidade deve ser uma característica que diga respeito à pessoa do signatário do Documento e não de um equipamento que este utilize. É necessário que, no Processo Judicial Eletrônico, tenha-se absoluta certeza de que o remetente indicado seja efetivamente o signatário daquele Documento eletronicamente produzido e transmitido. Essa garantia relativa à autoria do Documento leva ao Princípio do não-repúdio, que significa que o autor do Documento não poderá negar a sua autoria. (CLEMENTINO, 2008, p. 95 e 96)

A comparação no Meio Eletrônico se dá entre *Bits* e não entre imagens ou padrões. Desta afirmação chega-se a conclusão de que não há espaço no Meio Eletrônico para suposição da autoria, há a confirmação ou negação da autoria, mas não uma possibilidade desta.

Analisando a iniciativa do TRF 4ª Região acerca dos sistemas e-proc e e-cint suscitados por Freitas e Brotto (2008), encontra-se a adoção e permissão de uso destes sistemas na Resolução nº 13 de 11 de março de 2004 do TRF 4ª Região.

Tal resolução é de cunho administrativo e versa sobre regras de operacionalização do trâmite processual, trânsito de petições e atos processuais.

> Resolução nº 13 TRF 4ª Região. Art. 4º. Os autos serão integralmente digitais, sendo responsabilidade de cada usuário a inserção de documentos nos processos, cuja autenticidade e origem será garantida através de sistema de segurança com geração de chaves eletrônicas para os documentos.
> Parágrafo único: O juiz da causa poderá determinar a exclusão de peças indevidamente juntadas aos autos. (BRASIL, 2004)

De acordo com a Resolução nº 13 os documentos eletrônicos deverão ser assinados utilizando um sistema de segurança com geração de chaves eletrônicas. Essa assinatura deverá ser nos moldes da ICP-Brasil, utilizando um certificado digital expedido por uma das ACs.

Quanto à necessidade de cadastramento no tribunal exigida pela Lei nº 11.419, os dois sistemas acima mencionados o exigem para acesso e estão regulamentados pelo Provimento nº 01 de Maio de 2004, do TRF 4ª Região.

Desta forma, ambos os sistemas se enquadram na necessidade legal quanto à exigência de cadastramento prévio no Poder Judiciário e da assinatura eletrônica. Mas, o sistema permite o envio de peças e a prática de atos processuais sem o uso da assinatura eletrônica, exigindo apenas que a parte guarde o original até o trânsito em julgado da ação. Neste caso, abre-se uma brecha de segurança que não é bem vinda, pois será possível argüição de nulidades e questionamento da autenticidade documental. Para se atenuar esta possibilidade, o parágrafo único do artigo 4º da Resolução nº 13 permite ao juiz excluir peças que foram indevidamente juntadas.

Mesmo no caso de documentos digitalizados onde o original é em papel, entendemos ser necessária a assinatura eletrônica como forma de se atestar a origem e validade do documento, porque, esse documento digitalizado, assinado eletronicamente pela parte, terá a presunção de que é verdadeiro e não poderá ser alterado durante o trâmite processual.

CONSIDERAÇÕES FINAIS

A disposição do governo brasileiro em criar a base necessária para a informatização de todos os órgãos da administração direta e indireta é uma grande evolução rumo a transparência, efetividade e celeridade pública.

O Brasil não é o único país a procurar a modernização, há movimentos neste sentido em várias nações, como exemplo a Alemanha e os Estados Unidos da América, reconhecidamente países ricos e sérios, mostrando que o caminho escolhido pelo Brasil não é uma aventura, e sim a escolha certa para os novos tempos.

Em especial, a informatização do judiciário surge no momento em que os processos se acumulam nas justiças de primeiro grau, nos tribunais e até no Supremo Tribunal Federal. O processo judicial eletrônico, se bem implantado e difundido como está sendo, contribuirá para uma maior efetividade da justiça, uma maior capacidade técnica e operacional, permitindo reduzir os gargalos existentes e conseqüentemente entregar aos jurisdicionados a tutela de seus direitos tão almejados em tempo adequado.

Cabe aos legisladores buscar o tratamento adequado e a correção das ambigüidades ainda existente na legislação aplicada à informatização do judiciário, para assim garantir que a sua aplicabilidade não sofrerá restrições, ou seja, motivo de questionamentos intermináveis nos tribunais superiores.

Deve-se também ser estendida a informatização a todas as áreas e poderes do governo (Executivo, Judiciário e Legislativo), em todas as esferas de poder (Federal, Estadual e Municipal) e a todos os órgãos ao governo coligados, para assim, estar todo o governo em sincronia e com capacidade de gerir a coisa pública da melhor forma possível. Há projetos em andamento neste sentido, portanto, incumbe ao governo maiores impulsos, para assim acelerar o processo de informatização e a adoção das novas práticas que proporcionarão transparência a administração, efetividade na gestão pública e economia aos cofres públicos.

Como visto no decorrer deste trabalho, a escolha brasileira por uma entidade pública na posição de certificadora raiz, a ICP-Brasil, é acertada, pois permite com alto grau de segurança, garantir autenticidade, integridade e validade jurídica aos documentos.

Sendo todas as mensagens e documentos assinados digitalmente e certificados, e trafegando pela Internet por sistemas criptografados e igualmente certificados, é possível garantir a comunicação sem possibilidade de interceptação ou adulteração indevida, garantindo também a identidade do remetente e do destinatário sem qualquer dúvida.

REFERÊNCIAS

ABRÃO, Carlos Henrique. **Processo Eletrônico**. São Paulo: Juarez de Oliveira, 2009. 143 p.

ALMEIDA FILHO, José Carlos de Araújo. **Processo Eletrônico e Teoria Geral do Processo Eletrônico**. Rio de Janeiro: Forense, 2008. 466 p.

BRASIL. Lei nº 5.869, de 11 de janeiro de 1973. **Institui o Código de Processo Civil brasileiro**. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L5869.htm>. Acesso em: 07 set 2009.

_____. Medida Provisória nº 2.200-2 de 24 de janeiro de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. **Diário Oficial Eletrônico da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 27 de ago 2001, p. 65. Disponível em <http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm>. Acesso em: 07 set 2009.

_____. Resolução nº 13 de 11 de março de 2004. Implanta e estabelece normas para o funcionamento do Processo Eletrônico nos Juizados Especiais Federais no âmbito da Justiça Federal da 4ª Região. BIE - Boletim Informativo Especial Corregedoria-Geral da Justiça, Porto Alegre, RS, 20 abr. 2004, p. 174-06.

_____. Lei nº 11.419 de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial; altera a Lei n. 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Poder Legislativo, Brasília, DF, 20 dez. 2006, p. 2. Disponível em <http://www.planalto.gov.br/ccivil_03/ _Ato2004-2006/2006/Lei/_quadro2006.htm>. Acesso em: 07 set 2009.

CALMON, Petrônio. **Comentários à Lei de Informatização do Processo Judicial**. Rio de Janeiro: Forense, 2007. 160 p.

CLEMENTINO, Edilberto Barbosa. **Processo Judicial Eletrônico**. Curitiba: Juruá Editora, 2008. 210 p.

FALCÃO, Joaquim. O Judiciário e o Software Livre. **Revista Jurídica Consulex**. Brasília, ano 11, nº 240, p. 36-37, 15 jan 2007.

FREITAS, Cinthia Obladen de Almendra; BROTTO, Alexia A. Rodrigues. SISTEMAS COMPUTACIONAIS PARA O PODER JUDICIÁRIO: FERRAMENTAS, ACESSO E INCLUSÃO SOCIAL. **Anais do XVII Congresso Nacional do CONPEDI**. Brasília, 2008.

GOVERNO ELETRÔNICO. **Ministério do Planejamento, Orçamento e Gestão**. Disponível em: < http://www.governoeletronico.gov.br/o-gov.br>. Acesso em: 30 set. 2009.

HOUAISS, Antônio; VILLAR, Mauro de Salles. **Dicionário Houaiss da Língua Portuguesa**. Rio de Janeiro: Objetiva, 2004. 2925 p.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. **Curso de Processo Civil: Processo de Conhecimento**. São Paulo: Revista dos Tribunais, 2007. v. 2. 815 p.

MENKE, Fabiano. Assinaturas Digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a ICP alemã. **Revista de Direito do Consumidor**, São Paulo, v. 48, 2003.

MORAES, Alexandre de. **Direito Constitucional**. 19ª ed. São Paulo: Atlas, 2006. 948p.

PAULA, Wesley Roberto de. **Publicidade no Processo Judicial Eletrônico:** Busca da Indispensável Relativização. São Paulo: LTr, 2009. 174 p.

R.L. Rivest, A. Shamir, and L. Adleman. **A Method for Obtaining Digital Signatures and Public-Key Cryptosystems**. MIT - Massachusetts Institute of Technology, Cambridge, Massachusetts, USA, 1977.

SANTOS, Ana Cristina Batista Santos. Informatização Judicial: Realidade Urgente. **Revista Jurídica Consulex**, ano 10, nº 236, p. 52-54, 15 nov 2006.

ANEXOS

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
2. A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems.

A message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret prime numbers p and q. Decryption is similar; only a different, secret, power d is used, where $e \cdot d \equiv 1 \pmod{(p-1)\cdot(q-1)}$. The security of the system rests in part on the difficulty of factoring the published divisor, n.

Key Words and Phrases: digital signatures, public-key cryptosystems, privacy, authentication, security, factorization, prime number, electronic mail, message-passing, electronic funds transfer, cryptography.

CR Categories: 2.12, 3.15, 3.50, 3.81, 5.25

*General permission to make fair use in teaching or research of all or part of this material is granted to individual readers and to nonprofit libraries acting for them provided that ACM's copyright notice is given and that reference is made to the publication, to its date of issue, and to the fact that reprinting privileges were granted by permission of the Association for Computing Machinery. To otherwise reprint a figure, table, other substantial excerpt, or the entire work requires specific permission as does republication, or systematic or multiple reproduction.

This research was supported by National Science Foundation grant MCS76-14294, and the Office of Naval Research grant number N00014-67-A-0204-0063.

Author's Address: Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139 E-mail addresses: rivest@theory.lcs.mit.edu

I Introduction

The era of "electronic mail" [10] may soon be upon us; we must ensure that two important properties of the current "paper mail" system are preserved: (a) messages are *private*, and (b) messages can be *signed*. We demonstrate in this paper how to build these capabilities into an electronic mail system.

At the heart of our proposal is a new encryption method. This method provides an implementation of a "public-key cryptosystem," an elegant concept invented by Diffie and Hellman [1]. Their article motivated our research, since they presented the concept but not any practical implementation of such a system. Readers familiar with [1] may wish to skip directly to Section V for a description of our method.

II Public-Key Cryptosystems

In a "public key cryptosystem" each user places in a public file an encryption procedure E. That is, the public file is a directory giving the encryption procedure of each user. The user keeps secret the details of his corresponding decryption procedure D. These procedures have the following four properties:

(a) Deciphering the enciphered form of a message M yields M. Formally,

$$D(E(M) = M. \tag{1}$$

(b) Both E and D are easy to compute.

(c) By publicly revealing E the user does not reveal an easy way to compute D. This means that in practice only he can decrypt messages encrypted with E, or compute D efficiently.

(d) If a message M is first deciphered and then enciphered, M is the result. Formally,

$$E(D(M) = M. \tag{2}$$

An encryption (or decryption) procedure typically consists of a *general method* and an *encryption key*. The general method, under control of the key, enciphers a message M to obtain the enciphered form of the message, called the *ciphertext* C. Everyone can use the same general method; the security of a given procedure will rest on the security of the key. Revealing an encryption algorithm then means revealing the key.

When the user reveals E he reveals a very *inefficient* method of computing $D(C)$: testing all possible messages M until one such that $E(M) = C$ is found. If property (c) is satisfied the number of such messages to test will be so large that this approach is impractical.

A function E satisfying (a)-(c) is a "trap-door one-way function;" if it also satisfies (d) it is a "trap-door one-way permutation." Diffie and Hellman [1] introduced the

concept of trap-door one-way functions but did not present any examples. These functions are called "one-way" because they are easy to compute in one direction but (apparently) very difficult to compute in the other direction. They are called "trap-door" functions since the inverse functions are in fact easy to compute once certain private "trap-door" information is known. A trap-door one-way function which also satisfies (d) must be a permutation: every message is the cipertext for some other message and every ciphertext is itself a permissible message. (The mapping is "one-to-one" and "onto"). Property (d) is needed only to implement "signatures."

The reader is encouraged to read Diffie and Hellman's excellent article [1] for further background, for elaboration of the concept of a public-key cryptosystem, and for a discussion of other problems in the area of cryptography. The ways in which a public-key cryptosystem can ensure privacy and enable "signatures" (described in Sections III and IV below) are also due to Diffie and Hellman.

For our scenarios we suppose that A and B (also known as Alice and Bob) are two users of a public-key cryptosystem. We will distinguish their encryption and decryption procedures with subscripts: E_A, D_A, E_B, D_B.

III Privacy

Encryption is the standard means of rendering a communication private. The sender enciphers each message before transmitting it to the receiver. The receiver (but no unauthorized person) knows the appropriate deciphering function to apply to the received message to obtain the original message. An eavesdropper who hears the transmitted message hears only "garbage" (the ciphertext) which makes no sense to him since he does not know how to decrypt it.

The large volume of personal and sensitive information currently held in computerized data banks and transmitted over telephone lines makes encryption increasingly important. In recognition of the fact that efficient, high-quality encryption techniques are very much needed but are in short supply, the National Bureau of Standards has recently adopted a "Data Encryption Standard" [13, 14], developed at IBM. The new standard does not have property (c), needed to implement a public-key cryptosystem.

All classical encryption methods (including the NBS standard) suffer from the "key distribution problem." The problem is that before a private communication can begin, *another* private transaction is necessary to distribute corresponding encryption and decryption keys to the sender and receiver, respectively. Typically a private courier is used to carry a key from the sender to the receiver. Such a practice is not feasible if an electronic mail system is to be rapid and inexpensive. A public-key cryptosystem needs no private couriers; the keys can be distributed over the insecure communications channel.

How can Bob send a private message M to Alice in a public-key cryptosystem? First, he retrieves E_A from the public file. Then he sends her the enciphered message $E_A(M)$. Alice deciphers the message by computing $D_A(E_A(M)) = M$. By property (c) of the public-key cryptosystem only she can decipher $E_A(M)$. She can encipher a

private response with E_B, also available in the public file.

Observe that no private transactions between Alice and Bob are needed to establish private communication. The only "setup" required is that each user who wishes to receive private communications must place his enciphering algorithm in the public file.

Two users can also establish private communication over an insecure communications channel without consulting a public file. Each user sends his encryption key to the other. Afterwards all messages are enciphered with the encryption key of the recipient, as in the public-key system. An intruder listening in on the channel cannot decipher any messages, since it is not possible to derive the decryption keys from the encryption keys. (We assume that the intruder cannot modify or insert messages into the channel.) Ralph Merkle has developed another solution [5] to this problem.

A public-key cryptosystem can be used to "bootstrap" into a standard encryption scheme such as the NBS method. Once secure communications have been established, the first message transmitted can be a key to use in the NBS scheme to encode all following messages. This may be desirable if encryption with our method is slower than with the standard scheme. (The NBS scheme is probably somewhat faster if special-purpose hardware encryption devices are used; our scheme may be faster on a general-purpose computer since multiprecision arithmetic operations are simpler to implement than complicated bit manipulations.)

IV Signatures

If electronic mail systems are to replace the existing paper mail system for business transactions, "signing" an electronic message must be possible. The recipient of a signed message has proof that the message originated from the sender. This quality is stronger than mere authentication (where the recipient can verify that the message came from the sender); the recipient can convince a "judge" that the signer sent the message. To do so, he must convince the judge that he did not forge the signed message himself! In an authentication problem the recipient does not worry about this possibility, since he only wants to satisfy *himself* that the message came from the sender.

An electronic signature must be *message*-dependent, as well as *signer*-dependent. Otherwise the recipient could modify the message before showing the message-signature pair to a judge. Or he could attach the signature to any message whatsoever, since it is impossible to detect electronic "cutting and pasting."

To implement signatures the public-key cryptosystem must be implemented with trap-door one-way permutations (i.e. have property (d)), since the decryption algorithm will be applied to unenciphered messages.

How can user Bob send Alice a "signed" message M in a public-key cryptosystem? He first computes his "signature" S for the message M using D_B:

$$S = D_B(M) \ .$$

(Deciphering an unenciphered message "makes sense" by property (d) of a public-key cryptosystem: each message is the ciphertext for some other message.) He then encrypts S using E_A (for privacy), and sends the result $E_A(S)$ to Alice. He need not send M as well; it can be computed from S.

Alice first decrypts the ciphertext with D_A to obtain S. She knows who is the presumed sender of the signature (in this case, Bob); this can be given if necessary in plain text attached to S. She then extracts the message with the encryption procedure of the sender, in this case E_B (available on the public file):

$$M = E_B(S) \ .$$

She now possesses a message-signature pair (M, S) with properties similar to those of a signed paper document.

Bob cannot later deny having sent Alice this message, since no one else could have created $S = D_B(M)$. Alice can convince a "judge" that $E_B(S) = M$, so she has proof that Bob signed the document.

Clearly Alice cannot modify M to a different version M', since then she would have to create the corresponding signature $S' = D_B(M')$ as well.

Therefore Alice has received a message "signed" by Bob, which she can "prove" that he sent, but which she cannot modify. (Nor can she forge his signature for any other message.)

An electronic checking system could be based on a signature system such as the above. It is easy to imagine an encryption device in your home terminal allowing you to sign checks that get sent by electronic mail to the payee. It would only be necessary to include a unique check number in each check so that even if the payee copies the check the bank will only honor the first version it sees.

Another possibility arises if encryption devices can be made fast enough: it will be possible to have a telephone conversation in which every word spoken is signed by the encryption device before transmission.

When encryption is used for signatures as above, it is important that the encryption device not be "wired in" between the terminal (or computer) and the communications channel, since a message may have to be successively enciphered with several keys. It is perhaps more natural to view the encryption device as a "hardware subroutine" that can be executed as needed.

We have assumed above that each user can always access the public file reliably. In a "computer network" this might be difficult; an "intruder" might forge messages purporting to be from the public file. The user would like to be sure that he actually obtains the encryption procedure of his desired correspondent and not, say, the encryption procedure of the intruder. This danger disappears if the public file "signs" each message it sends to a user. The user can check the signature with the public file's encryption algorithm E_{PF}. The problem of "looking up" E_{PF} itself in the public file is avoided by giving each user a description of E_{PF} when he first shows up (in person) to join the public-key cryptosystem and to deposit his public encryption procedure. He then stores this description rather than ever looking it up again. The need for a

courier between every pair of users has thus been replaced by the requirement for a single secure meeting between each user and the public file manager when the user joins the system. Another solution is to give each user, when he signs up, a book (like a telephone directory) containing all the encryption keys of users in the system.

V Our Encryption and Decryption Methods

To encrypt a message M with our method, using a public encryption key (e, n), proceed as follows. (Here e and n are a pair of positive integers.)

First, represent the message as an integer between 0 and $n-1$. (Break a long message into a series of blocks, and represent each block as such an integer.) Use any standard representation. The purpose here is not to encrypt the message but only to get it into the numeric form necessary for encryption.

Then, encrypt the message by raising it to the eth power modulo n. That is, the result (the ciphertext C) is the remainder when M^e is divided by n.

To decrypt the ciphertext, raise it to another power d, again modulo n. The encryption and decryption algorithms E and D are thus:

$$\begin{aligned} C \quad \equiv \quad & E(M) \equiv M^e \pmod{n}, \text{ for a message } M \ . \\ & D(C) \equiv C^d \pmod{n}, \text{ for a ciphertext } C \ . \end{aligned}$$

Note that encryption does not increase the size of a message; both the message and the ciphertext are integers in the range 0 to $n-1$.

The *encryption key* is thus the pair of positive integers (e, n). Similarly, the *decryption* key is the pair of positive integers (d, n). Each user makes his encryption key public, and keeps the corresponding decryption key private. (These integers should properly be subscripted as in n_A, e_A, and d_A, since each user has his own set. However, we will only consider a typical set, and will omit the subscripts.)

How should you choose your encryption and decryption keys, if you want to use our method?

You first compute n as the product of two primes p and q:

$$n = p \cdot q \ .$$

These primes are very large, "random" primes. Although you will make n public, the factors p and q will be effectively hidden from everyone else due to the enormous difficulty of factoring n. This also hides the way d can be derived from e.

You then pick the integer d to be a large, random integer which is relatively prime to $(p-1) \cdot (q-1)$. That is, check that d satisfies:

$$\gcd(d, (p-1) \cdot (q-1)) = 1$$

("gcd" means "greatest common divisor").

The integer e is finally computed from p, q, and d to be the "multiplicative inverse" of d, modulo $(p-1)\cdot(q-1)$. Thus we have

$$e \cdot d \equiv 1 \pmod{(p-1)\cdot(q-1)}.$$

We prove in the next section that this guarantees that (1) and (2) hold, i.e. that E and D are inverse permutations. Section VII shows how each of the above operations can be done efficiently.

The aforementioned method should not be confused with the "exponentiation" technique presented by Diffie and Hellman [1] to solve the key distribution problem. Their technique permits two users to determine a key in common to be used in a normal cryptographic system. It is not based on a trap-door one-way permutation. Pohlig and Hellman [8] study a scheme related to ours, where exponentiation is done modulo a prime number.

VI The Underlying Mathematics

We demonstrate the correctness of the deciphering algorithm using an identity due to Euler and Fermat [7]: for any integer (message) M which is relatively prime to n,

$$M^{\phi(n)} \equiv 1 \pmod{n}\ . \tag{3}$$

Here $\phi(n)$ is the Euler totient function giving number of positive integers less than n which are relatively prime to n. For prime numbers p,

$$\phi(p) = p - 1\ .$$

In our case, we have by elementary properties of the totient function [7]:

$$\begin{aligned} \phi(n) &= \phi(p)\cdot\phi(q) \\ &= (p-1)\cdot(q-1) \\ &= n - (p+q) + 1\ . \end{aligned} \tag{4}$$

Since d is relatively prime to $\phi(n)$, it has a multiplicative inverse e in the ring of integers modulo $\phi(n)$:

$$e \cdot d \equiv 1 \pmod{\phi(n)}. \tag{5}$$

We now prove that equations (1) and (2) hold (that is, that deciphering works correctly if e and d are chosen as above). Now

$$\begin{aligned} D(E(M)) &\equiv (E(M))^d \equiv (M^e)^d \pmod{n} = M^{e\cdot d} \pmod{n} \\ E(D(M)) &\equiv (D(M))^e \equiv (M^d)^e \pmod{n} = M^{e\cdot d} \pmod{n} \end{aligned}$$

and

$$M^{e\cdot d} \equiv M^{k\cdot\phi(n)+1} \pmod{n} \text{ (for some integer } k).$$

From (3) we see that for all M such that p does not divide M

$$M^{p-1} \equiv 1 \pmod{p}$$

and since $(p-1)$ divides $\phi(n)$

$$M^{k\cdot\phi(n)+1} \equiv M \pmod{p}.$$

This is trivially true when $M \equiv 0 \pmod{p}$, so that this equality actually holds for *all* M. Arguing similarly for q yields

$$M^{k\cdot\phi(n)+1} \equiv M \pmod{q}\ .$$

Together these last two equations imply that for all M,

$$M^{e\cdot d} \equiv M^{k\cdot\phi(n)+1} \equiv M \pmod{n}.$$

This implies (1) and (2) for all $M, 0 \leq M < n$. Therefore E and D are inverse permutations. (We thank Rich Schroeppel for suggesting the above improved version of the authors' previous proof.)

VII Algorithms

To show that our method is practical, we describe an efficient algorithm for each required operation.

A How to Encrypt and Decrypt Efficiently

Computing $M^e \pmod{n}$ requires at most $2 \cdot \log_2(e)$ multiplications and $2 \cdot \log_2(e)$ divisions using the following procedure (decryption can be performed similarly using d instead of e):

Step 1. Let $e_k e_{k-1} \ldots e_1 e_0$ be the binary representation of e.
Step 2. Set the variable C to 1.
Step 3. Repeat steps 3a and 3b for $i = k, k-1, \ldots, 0$:
  Step 3a. Set C to the remainder of C^2 when divided by n.
  Step 3b. If $e_i = 1$, then set C to the remainder of $C \cdot M$ when divided by n.
Step 4. Halt. Now C is the encrypted form of M.

This procedure is called "exponentiation by repeated squaring and multiplication." This procedure is half as good as the best; more efficient procedures are known. Knuth [3] studies this problem in detail.

The fact that the enciphering and deciphering are identical leads to a simple implementation. (The whole operation can be implemented on a few special-purpose integrated circuit chips.)

A high-speed computer can encrypt a 200-digit message M in a few seconds; special-purpose hardware would be much faster. The encryption time per block increases no faster than the cube of the number of digits in n.

B How to Find Large Prime Numbers

Each user must (privately) choose two large random numbers p and q to create his own encryption and decryption keys. These numbers must be large so that it is not computationally feasible for anyone to factor $n = p \cdot q$. (Remember that n, but not p or q, will be in the public file.) We recommend using 100-digit (decimal) prime numbers p and q, so that n has 200 digits.

To find a 100-digit "random" prime number, generate (odd) 100-digit random numbers until a prime number is found. By the prime number theorem [7], about $(\ln 10^{100})/2 = 115$ numbers will be tested before a prime is found.

To test a large number b for primality we recommend the elegant "probabilistic" algorithm due to Solovay and Strassen [12]. It picks a random number a from a uniform distribution on $\{1, \ldots, b-1\}$, and tests whether

$$\gcd(a, b) = 1 \text{ and } J(a, b) = a^{(b-1)/2} \pmod{b}, \tag{6}$$

where $J(a, b)$ is the Jacobi symbol [7]. If b is prime (6) is always true. If b is composite (6) will be false with probability at least $1/2$. If (6) holds for 100 randomly chosen values of a then b is almost certainly prime; there is a (negligible) chance of one in 2^{100} that b is composite. Even if a composite were accidentally used in our system, the receiver would probably detect this by noticing that decryption didn't work correctly. When b is odd, $a \leq b$, and $\gcd(a, b) = 1$, the Jacobi symbol $J(a, b)$ has a value in $\{-1, 1\}$ and can be efficiently computed by the program:

$$\begin{aligned} J(a,b) = &\textbf{if } a = 1 \textbf{ then } 1 \textbf{ else} \\ &\textbf{if } a \text{ is even } \textbf{then } J(a/2, b) \cdot (-1)^{(b^2-1)/8} \\ &\textbf{else } J(b \pmod{a}, a) \cdot (-1)^{(a-1)\cdot(b-1)/4} \end{aligned}$$

(The computations of $J(a, b)$ and $\gcd(a, b)$ can be nicely combined, too.) Note that this algorithm does *not* test a number for primality by trying to factor it. Other efficient procedures for testing a large number for primality are given in [6,9,11].

To gain additional protection against sophisticated factoring algorithms, p and q should differ in length by a few digits, both $(p-1)$ and $(q-1)$ should contain large prime factors, and $\gcd(p-1, q-1)$ should be small. The latter condition is easily checked.

To find a prime number p such that $(p-1)$ has a large prime factor, generate a large random prime number u, then let p be the first prime in the sequence $i \cdot u + 1$, for $i = 2, 4, 6, \ldots$. (This shouldn't take too long.) Additional security is provided by ensuring that $(u-1)$ also has a large prime factor.

A high-speed computer can determine in several seconds whether a 100-digit number is prime, and can find the first prime after a given point in a minute or two.

Another approach to finding large prime numbers is to take a number of known factorization, add one to it, and test the result for primality. If a prime p is found

it is possible to *prove* that it really is prime by using the factorization of $p-1$. We omit a discussion of this since the probabilistic method is adequate.

C How to Choose d

It is very easy to choose a number d which is relatively prime to $\phi(n)$. For example, any prime number greater than $\max(p,q)$ will do. It is important that d should be chosen from a large enough set so that a cryptanalyst cannot find it by direct search.

D How to Compute e from d and $\phi(n)$

To compute e, use the following variation of Euclid's algorithm for computing the greatest common divisor of $\phi(n)$ and d. (See exercise 4.5.2.15 in [3].) Calculate $\gcd(\phi(n), d)$ by computing a series $x_0, x_1, x_2, \ldots$, where $x_0 \equiv \phi(n), x_1 = d$, and $x_{i+1} \equiv x_{i-1} \pmod{x_i}$, until an x_k equal to 0 is found. Then $\gcd(x_0, x_1) = x_{k-1}$. Compute for each x_i numbers a_i and b_i such that $x_i = a_i \cdot x_0 + b_i \cdot x_1$. If $x_{k-1} = 1$ then b_{k-1} is the multiplicative inverse of $x_1 \pmod{x_0}$. Since k will be less than $2\log_2(n)$, this computation is very rapid.

If e turns out to be less than $\log_2(n)$, start over by choosing another value of d. This guarantees that every encrypted message (except $M = 0$ or $M = 1$) undergoes some "wrap-around" (reduction modulo n) .

VIII A Small Example

Consider the case $p = 47, q = 59, n = p \cdot q = 47 \cdot 59 = 2773$, and $d = 157$. Then $\phi(2773) = 46 \cdot 58 = 2668$, and e can be computed as follows:

$x_0 = 2668, \quad a_0 = 1, \quad b_0 = 0,$
$x_1 = 157, \quad a_1 = 0, \quad b_1 = 1,$
$x_2 = 156, \quad a_2 = 1, \quad b_2 = -16$ (since $2668 = 157 \cdot 16 + 156$) ,
$x_3 = 1, \quad a_3 = -1, \quad b_3 = 17$ (since $157 = 1 \cdot 156 + 1$) .

Therefore $e = 17$, the multiplicative inverse $\pmod{2668}$ of $d = 157$.

With $n = 2773$ we can encode two letters per block, substituting a two-digit number for each letter: blank = 00, A = 01, B = 02, ..., Z = 26. Thus the message

```
ITS ALL GREEK TO ME
```

(Julius Caesar, I, ii, 288, paraphrased) is encoded:

```
0920 1900 0112 1200 0718 0505 1100 2015 0013 0500
```

Since $e = 10001$ in binary, the first block ($M = 920$) is enciphered:

$$M^{17} = (((((1)^2 \cdot M)^2)^2)^2)^2 \cdot M = 948 \pmod{2773} .$$

The whole message is enciphered as:

0948 2342 1084 1444 2663 2390 0778 0774 0219 1655 .

The reader can check that deciphering works: $948^{157} \equiv 920 \pmod{2773}$, etc.

IX Security of the Method: Cryptanalytic Approaches

Since no techniques exist to *prove* that an encryption scheme is secure, the only test available is to see whether anyone can think of a way to break it. The NBS standard was "certified" this way; seventeen man-years at IBM were spent fruitlessly trying to break that scheme. Once a method has successfully resisted such a concerted attack it may for practical purposes be considered secure. (Actually there is some controversy concerning the security of the NBS method [2].)

We show in the next sections that all the obvious approaches for breaking our system are at least as difficult as factoring n. While factoring large numbers is not provably difficult, it is a well-known problem that has been worked on for the last three hundred years by many famous mathematicians. Fermat (1601?-1665) and Legendre (1752-1833) developed factoring algorithms; some of today's more efficient algorithms are based on the work of Legendre. As we shall see in the next section, however, no one has yet found an algorithm which can factor a 200-digit number in a reasonable amount of time. We conclude that our system has already been partially "certified" by these previous efforts to find efficient factoring algorithms.

In the following sections we consider ways a cryptanalyst might try to determine the secret decryption key from the publicly revealed encryption key. We do not consider ways of protecting the decryption key from theft; the usual physical security methods should suffice. (For example, the encryption device could be a separate device which could also be used to generate the encryption and decryption keys, such that the decryption key is never printed out (even for its owner) but only used to decrypt messages. The device could erase the decryption key if it was tampered with.)

A Factoring n

Factoring n would enable an enemy cryptanalyst to "break" our method. The factors of n enable him to compute $\phi(n)$ and thus d. Fortunately, factoring a number seems to be much more difficult than determining whether it is prime or composite.

A large number of factoring algorithms exist. Knuth [3, Section 4.5.4] gives an excellent presentation of many of them. Pollard [9] presents an algorithm which factors a number n in time $O(n^{1/4})$.

The fastest factoring algorithm known to the authors is due to Richard Schroeppel (unpublished); it can factor n in approximately

$$\exp\sqrt{ln(n) \cdot ln(ln(n))} \quad = \quad n^{\sqrt{\ln\ln(n)/\ln(n)}}$$

$$= (\ln(n))^{\sqrt{\ln(n)/\ln(\ln(n))}}$$

steps (here ln denotes the natural logarithm function). Table 1 gives the number of operations needed to factor n with Schroeppel's method, and the time required if each operation uses one microsecond, for various lengths of the number n (in decimal digits).

Table 1

Digits	*Number of operations*	*Time*
50	1.4×10^{10}	3.9 hours
75	9.0×10^{12}	104 days
100	2.3×10^{15}	74 years
200	1.2×10^{23}	3.8×10^{9} years
300	1.5×10^{29}	4.9×10^{15} years
500	1.3×10^{39}	4.2×10^{25} years

We recommend that n be about 200 digits long. Longer or shorter lengths can be used depending on the relative importance of encryption speed and security in the application at hand. An 80-digit n provides moderate security against an attack using current technology; using 200 digits provides a margin of safety against future developments. This flexibility to choose a key-length (and thus a level of security) to suit a particular application is a feature not found in many of the previous encryption schemes (such as the NBS scheme).

B Computing $\phi(n)$ Without Factoring n

If a cryptanalyst could compute $\phi(n)$ then he could break the system by computing d as the multiplicative inverse of e modulo $\phi(n)$ (using the procedure of Section VII D).

We argue that this approach is no easier than factoring n since it enables the cryptanalyst to easily factor n using $\phi(n)$. This approach to factoring n has not turned out to be practical.

How can n be factored using $\phi(n)$? First, $(p+q)$ is obtained from n and $\phi(n) = n-(p+q)+1$. Then $(p-q)$ is the square root of $(p+q)^2-4n$. Finally, q is half the difference of $(p+q)$ and $(p-q)$.

Therefore breaking our system by computing $\phi(n)$ is no easier than breaking our system by factoring n. (This is why n must be composite; $\phi(n)$ is trivial to compute if n is prime.)

C Determining d Without Factoring n or Computing $\phi(n)$.

Of course, d should be chosen from a large enough set so that a direct search for it is unfeasible.

We argue that computing d is no easier for a cryptanalyst than factoring n, since once d is known n could be factored easily. This approach to factoring has also not turned out to be fruitful.

A knowledge of d enables n to be factored as follows. Once a cryptanalyst knows d he can calculate $e \cdot d - 1$, which is a multiple of $\phi(n)$. Miller [6] has shown that n can be factored using any multiple of $\phi(n)$. Therefore if n is large a cryptanalyst should not be able to determine d any easier than he can factor n.

A cryptanalyst may hope to find a d' which is equivalent to the d secretly held by a user of the public-key cryptosystem. If such values d' were common then a brute-force search could break the system. However, all such d' differ by the least common multiple of $(p-1)$ and $(q-1)$, and finding one enables n to be factored. (In (3) and (5), $\phi(n)$ can be replaced by $\text{lcm}(p-1, q-1)$.) Finding any such d' is therefore as difficult as factoring n.

D Computing D in Some Other Way

Although this problem of "computing e-th roots modulo n without factoring n" is not a well-known difficult problem like factoring, we feel reasonably confident that it is computationally intractable. It may be possible to prove that any general method of breaking our scheme yields an efficient factoring algorithm. This would establish that any way of breaking our scheme must be as difficult as factoring. We have not been able to prove this conjecture, however.

Our method should be certified by having the above conjecture of intractability withstand a concerted attempt to disprove it. The reader is challenged to find a way to "break" our method.

X Avoiding "Reblocking" When Encrypting A Signed Message

A signed message may have to be "reblocked" for encryption since the signature n may be larger than the encryption n (every user has his own n). This can be avoided as follows. A threshold value h is chosen (say $h = 10^{199}$) for the public-key cryptosystem. Every user maintains two public (e, n) pairs, one for enciphering and one for signature-verification, where every signature n is less than h, and every enciphering n is greater than h. Reblocking to encipher a signed message is then unnecessary; the message is blocked according to the transmitter's signature n.

Another solution uses a technique given in [4]. Each user has a single (e, n) pair where n is between h and $2h$, where h is a threshold as above. A message is encoded as a number less than h and enciphered as before, except that if the ciphertext is greater than h, it is repeatedly re-enciphered until it is less than h. Similarly for decryption the ciphertext is repeatedly deciphered to obtain a value less than h. If n is near h re-enciphering will be infrequent. (Infinite looping is not possible, since at worst a message is enciphered as itself.)

XI Conclusions

We have proposed a method for implementing a public-key cryptosystem whose security rests in part on the difficulty of factoring large numbers. If the security of our method proves to be adequate, it permits secure communications to be established without the use of couriers to carry keys, and it also permits one to "sign" digitized documents.

The security of this system needs to be examined in more detail. In particular, the difficulty of factoring large numbers should be examined very closely. The reader is urged to find a way to "break" the system. Once the method has withstood all attacks for a sufficient length of time it may be used with a reasonable amount of confidence.

Our encryption function is the only candidate for a "trap-door one-way permutation" known to the authors. It might be desirable to find other examples, to provide alternative implementations should the security of our system turn out someday to be inadequate. There are surely also many new applications to be discovered for these functions.

Acknowledgments. We thank Martin Hellman, Richard Schroeppel, Abraham Lempel, and Roger Needham for helpful discussions, and Wendy Glasser for her assistance in preparing the initial manuscript. Xerox PARC provided support and some marvelous text-editing facilities for preparing the final manuscript.

Received April 4, 1977; revised September 1, 1977.

References

1. Diffie, W., and Hellman, M. New directions in cryptography. *IEEE Trans. Inform. Theory IT-22*, (Nov. 1976), 644-654.

2. Diffie, W., and Hellman, M. Exhaustive cryptanalysis of the NBS data encryption standard. *Computer* 10 (June 1977), 74-84.

3. Knuth, D. E. *The Art of Computer Programming, Vol 2: Seminumerical Algorithms.* Addison-Wesley, Reading, Mass., 1969.

4. Levine, J., and Brawley, J.V. Some cryptographic applications of permutation polynomials. *Cryptologia* 1 (Jan. 1977), 76-92.

5. Merkle, R. Secure communications over an insecure channel. Submitted to *Comm. ACM.*

6. Miller, G.L. Riemann's hypothesis and tests for primality. Proc. Seventh Annual ACM Symp. on the Theory of Comptng. Albuquerque, New Mex., May 1975, pp. 234-239; extended vers. available as Res. Rep. CS-75-27, Dept. of Comptr. Sci., U. of Waterloo, Waterloo, Ont., Canada, Oct. 1975.

7. Niven, I., and Zuckerman, H.S. *An Introduction to the Theory of Numbers.* Wiley, New York, 1972.

8. Pohlig, S.C., and Hellman, M.E. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. To appear in IEEE Trans. Inform. Theory, 1978.

9. Pollard, J.M. Theorems on factorization and primality testing. *Proc. Camb. Phil. Soc. 76* (1974), 521-528.

10. Potter, R.J., Electronic mail. *Science 195*, 4283 (March 1977), 1160-1164.

11. Rabin, M.O., Probabilistic algorithms. In *Algorithms and Complexity*, J. F. Traub, Ed., Academic Press, New York, 1976, pp. 21-40.

12. Solovay, R., and Strassen, V. A Fast Monte-Carlo test for primality. *SIAM J. Comptng.* (March 1977), 84-85.

13. *Federal Register, Vol. 40*, No. 52, March 17, 1975.

14. *Federal Register, Vol. 40*, No. 149, August 1, 1975.