UNIVERSIDADE FEDERAL DA BAHIA
INSTITUTO DE CIÊNCIA DA INFORMAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

MAURO LEONARDO DE BRITO ALBUQUERQUE CUNHA

FORMAS E NORMAS DE [JUS]VALIDAÇÃO DA INFORMAÇÃO:
das marcas pessoais à criptografia, ao logical e à assinatura digital

Salvador
2006

MAURO LEONARDO DE BRITO ALBUQUERQUE CUNHA

FORMAS E NORMAS DE [JUS]VALIDAÇÃO DA INFORMAÇÃO:
das marcas pessoais à criptografia, ao logical e à assinatura digital

Dissertação apresentada ao programa de Pós-graduação em Ciência da Informação, Instituto de Ciência da Informação, Universidade Federal da Bahia, como requisito parcial para a obtenção do grau de Mestre em Ciência da Informação.

Orientadora: Profa. Teresinha Fróes Burnham, PhD
Co-orientador: Prof. Dr. Hernane B. de B. Pereira

Salvador
2006

Dados Internacionais de Catalogação na Publicação (CIP).

Cunha, Mauro Leonardo de Brito Albuquerque.

C972 Formas e normas de [jus]validação da informação: das marcas pessoais ao logical e à assinatura digital / Mauro Leonardo de Brito Albuquerque Cunha. – Salvador, 2006.

147 f. ; 29 cm.

Dissertação (Mestrado em Ciência da Informação) – Programa de Pós-Graduação em Ciência da Informação, Instituto de Ciência da Informação, Universidade Federal da Bahia.

"Orientação: Profª. Drª Teresinha Fróes Burnham. Programa de Pós-Graduação em Ciência da Informação. Co-orientação: Prof. Hernane Borges Barros Pereira"

1. Ciência da Informação. 2. Computação. 3. Criptografia Assimétrica. 4. Forma. 5. Norma. Universidade Federal da Bahia, Programa de Pós-Graduação em Ciência da Informação. II. Burnham, Teresinha Fróes. III. Título.

CDD 005.8

Ficha Catalográfica elaborada por Gislene Soares Guerra CRB-5/ 1382

MAURO LEONARDO DE BRITO ALBUQUERQUE CUNHA

FORMAS E NORMAS DE [JUS]VALIDAÇÃO DA INFORMAÇÃO: das marcas pessoais à criptografia, ao logical e à assinatura digital

Dissertação aprovada com distinção como requisito parcial para a obtenção do grau de Mestre em Ciência da Informação, pela seguinte banca examinadora.

.....
Profa. Dra. Teresinha Fróes Burnham, PhD.

.....
Prof. Dr. Hernane Borges de Barros Pereira

.....
Prof. Dr. Jacques Maurice Gauthier

Salvador, 21 de Fevereiro de 2006

Este trabalho é dedicado àqueles a quem, pela via da exclusão tecnológica, nega-se o acesso à informação [jurídica] essencial para sua emancipação, a todos quantos duvidem das urnas eletrônicas e sintam que há algo de podre na gestão das informações da previdência social. Se a criptografia é excludente, o conhecimento de criptologia é emancipatório.

AGRADECIMENTOS

Pelo apoio, pela doação do tempo que deveria ter sido a eles dedicado:

A D'us, porquanto o afastamento científico não é só do objeto da pesquisa, mas do mundo, da natureza, dos seres amados.

A Flávia, que antes de caminhar pela ciência, é mulher, e que antes de mulher, é ser humano, por ter aberto mão da minha devida companhia, do meu abraço, das minhas palavras ternas; e por ter suportado meus humores, minhas ausências, minhas irritabilidades e ansiedades do quotidiano.

A meus pais, Mauro e Maria, pelo apoio a cada passo de meu ainda inacabado processo de educação. Tendes sido por horas pontos de referência, e por outras, bússulas, que permitem que eu me oriente, chegando quase sempre a um destino melhor do que eu pudesse esperar.

A Gustavo, meu irmão, pelas longas conversas sobre assuntos ainda mais longos, e por nunca teres me deixado esquecer a importância política da atividade científica para a emancipação dos povos.

A Lúcia, por ter me cedido um computador comportado, quando todos os demais se haviam rebelado ... e por tantos outras pequenas ajudas quotidianas que fazem uma grande diferença.

Ao povo de Pernambuco, pátria, imortal: pela dúvida e, sobretudo, pela fé [na dúvida, inclusive].

Ao povo baiano, pelo mistério e pelo senso justo de revolta contra a ‘elite’ baiana e brasileira.

Pela {[des]/[re]}orientação, [re]leituras, colaboração, [re]visão a Teresinha Fróes, e também, a Hernane Pereira.

Pela leitura, pelos conselhos e pelas notas:

Aos membros da pré-banca: Jacques Gauthier, Augusto Galeão, Marcelo Moret.

A Flávia, minha esposa, a Mauro, meu pai, com destaque na revisão minuciosa das demonstrações matemáticas, e ao Prof. Dr. Rubens Silva, por mostrar que no semi-árido da ciência brotam também esperanças de vida e luta.

Pelas leituras e comentários:

A Geraldo, Flávia, Geórgia, Patruska e Ms. Ainsworth, que são, para minha honra e meu deleite, colegas de caminhada, na condição de monitores do curso de bacharelado em direito do Centro Universitário da Bahia (FIB).

Pelos livros e textos a Teresinha Fróes Burnham, a Paul Burnham, ao Prof. Dr. Benjamin de Almeida, amigo estimado, companheiro de investigações e companheiro de Centro Universitário, ao Prof. Dr. Rubens Silva.

Pela cumplicidade em vários momentos e de várias maneiras aos colegas da REDPECT, Rede Cooperativa de Pesquisa e Intervenção em (In)formação, Currículo e Trabalho. Vocês são o ALTERego do eu sem self fazendo ciência.

“Uma ordem havia surgido da Decadência e da Des*ordem*.”

São João da Cruz

“Sei não, só sei que foi assim”.
Xicó, personagem de Ariano Suassuna n'O Auto da Compadecida.

RESUMO

Esta dissertação buscou explorar a validação jurídica dos processos de informação jurídica ou juridicisada pelo referido processo. São dois, portanto, os objetivos: conceituar os processos de informação jurídica e conceituar os processos de sua validação jurídica. Buscou-se, pois, recompor ponto a ponto o itinerário do surgimento à validação jurídica das tecnologias de validação da informação desde as marcas pessoais pré-históricas até a tecnologia criptográfica assimétrica que proporcionou o advento da assinatura digital. Os conceitos de forma, de norma e de padrão são analisados com o fulcro na problematização do tema da validação nos processos humanos de comunicação da informação.

Palavras-chave: 1. Forma. 2. Norma. 3. Padrão. 4. Informação Jurídica – validação. 5. Sistemas Criptográficos Assimétricos. 6. Assinatura Digital. 7. Infra Estruturas de Chaves Públicas. 8. Problema de Merkle.

ABSTRACT

This paper means to explore legal validation of information processes, wether the information is legal or legalized by its validation process. It had, thus, two main objectives, i.e.: to conceptualize legal information processes and to conceptualize legal validation processes pursuant to the latter. A step-by-step trace of the path from the advent to the legal validation of information processes – since the beginning of it as pre-historical personal marks, up to the latest asymmetric cryptographic technologies that allow the upcoming of digital signatures. The concepts of norm, form, pattern and standard are thus analyzed, meaning to further comprehend the ever-evolving quest for validation in human information communication processes.

Keywords: 1. Form. 2. Norm. 3. Standard. 4. Legal information – validation. 5. Assymetric Cryptographic Systems. 6. Digital Signature. 7. Public Key Infrastructures. 8. Merkle problem.

LISTA DE ILUSTRAÇÕES

Figura 1	Máquina Enigma	104
Figura 2	Máquina Bombe	104
Figura 3	Máquina Colossus	104
Figura 4	Máquina Colossus	104
Figura 5	Máquina Colossus	104
Quadro 1	Exemplo da Cifra de Cæsar	97

LISTA DE ABREVIATURAS E SIGLAS

DH	Sistema criptográfico assimétrico Diffie-Hellman
EE.UU	Estados Unidos [da América]
GNU	GNU is Not Unix
GPL	General Public License
GCHQ	General Code Head Quarters
ICI	Instituto de Ciência da Informação da Universidade Federal da Bahia
ICP	Infra-estrutura de chaves públicas
ICP-Brasil	Infra-estrutura de cahves públicas brasileira, sistema normativo instituído pela Medida Provisória 2.200-2
IP	*Internet Protocol*, Protocolo do Entre-redes, Protocolo de Internet.
00.NN.GG.	Organizações Não-Governamentais.
REDPECT	Rede Cooperativa de Pesquisa e Intervenção em (In)formação, Currículo e Trabalho.
RSA	Sistema criptográfico assimétrico RSA, criado por Rivest, Shamir e Adleman.
TCP	*Transmission Control Protocol*, Protocolo de Controle de Transmissão.
TGS	Teoria Geral dos Sistemas.

SUMÁRIO

1	**INTRODUÇÃO: um [re]começo da [in]formação do [re]conhecimento jurídico**	16
1.1	CIÊNCIA NORMAL E CIÊNCIA DA NORMA: RESISTÊNCIAS AO ESTUDO CIENTÍFICO DOS PROCESSOS JUS-INFORMACIONAIS	19
1.2	FUNDAMENTAL[?]MENTE DIFERENTE	20
1.3	PENSANDO CIÊNCIA SINCERAMENTE: considerações metodológicas	22
1.4	DAS PEDRAS NO CAMINHO À BASE PARA CAMINHAR COM COERÊNCIA[?]	23
1.5	A VERDADE COMO PERGUNTA? CAMINHO PARA A SINCERIDADE METODOLÓGICA?	24
1.6	AS PARTES DA DISSERTAÇÃO E SUA FUNÇÃO	29
2	**OBJETO E OBJETIVOS**	32
2.1	LIMITES E EXTENSÃO DO TRABALHO	33
2.2	PERCEPÇÃO E ABORDAGEM DO OBJETO: entre luz e trevas – só na penumbra é concebível a visão	34
2.3	CONSTRUÇÃO DO OBJETIVO	36
2.4	O OBJETO DA PESQUISA E A SUA CIRCUNSTÂNCIA PLURAL E MULTI-REFERENCIAL	37
2.5	ESTABELECIMENTO DE OBJETIVOS ESPECÍFICOS	37
3	**[IN]FORMAÇÃO DOS SISTEMAS JURÍDICOS**	41
3.1	VISÃO DO DIREITO COMO SISTEMA DE INFORMAÇÕES	41
3.2	VISÃO WIENERIANA: fluxos retro-alimentados de informação jurídica	42
3.3	AS TEORIAS DA AUTOPOIESE COMO TEORIAS DOS SISTEMAS	45
3.4	O CONCEITO AMPLO DE INFORMAÇÃO ADOTADO NA PESQUISA E A TEORIA DA AUTOPOIESE	46
3.5	A TEORIA DA AUTOPOIESE JURÍDICA E OS FLUXOS DA	48

	INFORMAÇÃO JURÍDICA	
3.6	DO INFORMACIONAL E DO JURÍDICO AO JUS-INFORMACIONAL: dos pactos instituidores da linguagem à juridicidade na sociedade da informação	48
3.7	INFORMAÇÃO JURÍDICA E DECISÃO JURÍDICA NAS SOCIEDADES DA INFORMAÇÃO	50
3.8	A MENSAGEM JURÍDICA: a norma jurídica como informação [jurídica] e o enunciado jurídico como dado [jurídico]	51
3.9	O SILÊNCIO QUE NÃO CALA: o paradoxo de a validade da decisão não [poder] ser conseqüência da validade da informação	52
3.10	O FLUXO DE INFORMAÇÃO JURÍDICA COMO REGULAÇÃO SOCIAL: a informação é base para a conduta	54
3.11	DA HOMEOSTASE À LINGUAGEM: a fala, a escrita, a imprensa e a internet	56
4	**ASPECTOS {JUS[IN]}FORMAIS DAS INFORMAÇÕES JURÍDICAS NA ORALIDADE E NA ESCRITA**	58
4.1	PACTOS: natureza [jus]-informacional	58
4.2	PREENCHIMENTO DO VAZIO INFORMACIONAL DOS PACTOS PELO EVENTO SANEADOR DA DECISÃO	60
4.3	INFORMAÇÃO JURÍDICA EM SOCIEDADES SEM ESCRITA	62
5	**FORMA COMO NORMA E NORMA COMO FORMA: informação jurígena e jurídica como normatividade**	64
5.1	TERMINOLOGIA	64
5.2	FORMA-NORMA: da pré-história ao direito do espaço cibernético	66
5.3	CONTRIBUTOS DA CIÊNCIA DA INFORMAÇÃO PARA A CIÊNCIA JURÍDICA	71
5.4	NORMA COMO MENSAGEM PRESCRITIVA DE CONDUTA, E/OU COMO INFORMAÇÃO	71
5.5	SISTEMAS JUSNORMATIVOS COMO SISTEMAS DE INFORMAÇÃO	73
5.6	O TERMO INFORMAÇÃO NA LINGUAGEM JUSCIENTÍFICA	73
5.7	POLÍTICA DE DIREITOS HUMANOS COMO POLÍTICA DE SUSTENTAÇÃO DO ESTADO DE DIREITO	74

5.8	EFEITOS INFORMACIONAIS DA POLÍTICA PARAFISCAL GERANDO RESTRIÇÕES À PRIVACIDADE E À LIBERDADE INFORMACIONAL DO AUTOR DE LOGICAIS	75
5.9	SÓCIOS NA INFORMAÇÃO, O MODELO GNU/GPL	76
5.10	ESCAPE DOS PRODUTORES DE LOGICAIS GNU DA FORÇA [TRIBUTÁRIA] DO ESTADO PELO ABANDONO DO USO DA MOEDA	78
5.11	CONCLUSÕES PARCIAIS	79
6	**BASES CONCEITUAIS: assinatura e da criptografia**	81
6.1	REQUISITOS [JURÍDICOS] PARA A ADOÇÃO DO USO DA CRIPTOGRAFIA NA VALIDAÇÃO DE FLUXOS DE INFORMAÇÃO JURÍDICA NÃO-MILITAR	81
6.2	DEMONSTRAÇÃO DOS REQUISITOS [JURÍDICOS] PARA A ADOÇÃO DO USO DA CRIPTOGRAFIA NA VALIDAÇÃO DE FLUXOS DE INFORMAÇÃO JURÍDICA NÃO-MILITAR	81
6.3	INTRODUÇÃO À CRIPTOGRAFIA	84
6.4	NOÇÕES GERAIS	86
6.5	ESTEGANOGRAFIA	86
6.6	CRIPTOGRAFIA X ESTEGANOGRAFIA	87
7	**ASSINATURAS: validação da informação jurídica**	89
7.1	DAS MARCAS PESSOAIS PRIMITIVAS À ASSINATURA CURSIVA	89
7.2	A IMPRENSA CHINESA SOMA-SE AO ALFABETO OCIDENTAL: os tipos móveis de Gutemberg	90
7.3	A IMPRENSA NO BRASIL: exclusividade de acesso às prensas como fundamento da garantia de origem dos documentos	91
7.4	COPYRIGHT E DIREITO AUTORAL: situações excepcionais	92
7.5	A IMPORTÂNCIA DAS ASSINATURAS PARA A JUSVALIAÇÃO DAS INFORMAÇÕES JURÍDICAS MEDIANTE ESCRITOS COMUNICANTES DE DECLARAÇÕES PESSOAIS DE VONTADE	93
8	**CRIPTOGRAFIA CONVENCIONAL OU SIMÉTRICA**	96
8.1	E O PODER USA CRIPTOGRAFIA: Cæsar, a Cifra e o Direito	97

	Romano	
8.2	TRANSIÇÃO: precursores da criptografia assimétrica na criptografia convencional	99
8.3	EFEITOS JUS-[IN]FORMACIONAIS DO USO DA CRIPTOGRAFIA CONVENCIONAL	106
8.4	INTERCÂMBIO PÚBLICO DE CHAVES SECRETAS: UM PROGRESSO NA APLICAÇÃO PRÁTICA DA CRIPTOGRAFIA CONVENCIONAL	107
8.5	CRIPTOGRA FIA ASSIMÉTRICA	110
8.5.1	**Privacidade: direito, sigilo e criptografia assimétrica**	110
8.5.2	**Validade e validação jurídicas das informações, mediante aplicação da criptografia assimétrica**	110
8.6	SURGE UM NOVO PARADIGMA EM CRIPTOLOGIA [ENTRE OS MILITARES DA GRÃ-BRETANHA E OS CIVIS ESTADUNIDENSES]	111
9	**ASSINATURA DIGITAL: validação da informação jurídica**	113
9.1	CONCEITO DE ASSINATURA DIGITAL	113
9.1.1	**Assinatura eletrônica não é o mesmo que assinatura digital**	113
9.2	O QUE É UMA ASSINATURA DIGITAL	114
9.3	ENTRE DIREITO E MATEMÁTICA: A QUEM PERTENCE ESTA CHAVE? AUTORIDADES CERTIFICADORAS E INFRA-ESTRUTURAS DE CHAVES PÚBLICAS	115
9.4	O SISTEMA PÚBLICO BRASILEIRO DE VALIDAÇÃO DAS ASSINATURAS DIGITAIS: A ICP-Brasil	117
10	**CONSIDERAÇÕES CONCLUSIVAS: o fecho é uma abertura radical**	118
	REFERÊNCIAS	120
	APÊNDICE	130
	ANEXO	143

1 **INTRODUÇÃO: um [re]começo da [in]formação do [re]conhecimento jurídico**

O caráter público juridicamente requerido das informações seria inútil sem validação destas informações.

Sistemas que permitam um fluxo mais transparente de *in***forma**ções a que o acesso deve ser, por imperativo jurídico, garantido ao povo, dependem da assinatura digital como elemento de validação jurídica, nos termos da Medida Provisória 2.200-2, para servirem como documento juridicamente aceitável.

Não basta, pois, aos cidadãos, às empresas e às OO.NN.GG. ter acesso à *in***forma**ção: muitas vezes é fundamental ter acesso a *in***forma**ções juridicamente validadas, sobretudo diante do Judiciário e da Administração Pública brasileiros, costumeiramente **forma**listas, oficialistas e burocráticos, num sentido pervertido e não-weberiano da palavra.

Há que se conferir, por outro lado, transparência ao sigilo. Explica-se: na democracia, o sigilo das *in***forma**ções públicas é excepcional, devendo somente acontecer diante da previsão jurídica expressa, obedecendo esta última a limites estabelecidos pelo processo constitucional (LUHMANN, 1985a, p. 27-34). O Estado não deve, sob pena de desestruturar o próprio processo constitucional que justifica (KELSEN, 1998, p. 215-249) a sua existência, manter em sigilo *in***forma**ções cujo acesso pelo público é previsto pelo direito objetivo[1].

Há várias características próprias do modo de escrever utilizado para compor a dissertação. Nesta seção se mostra como e porque vários dos artifícios estilísticos foram usados e, mais importante, explica-se o que significa o seu emprego.

Partes das orações são frequentemente grafadas entre colchetes. Um exemplo deste procedimento está contido no seguinte trecho:

O itinerário que se traça para que, de um conceito, outros se possam derivar, é, por conseguinte, sempre sinuoso e recursivo; mas os conceitos se distinguem, ainda que não seja tão claro [nem tão facilmente determinável] onde o campo de validade de aplicação de cada conceito comece ou acabe.

As partes entre colchetes deverão ser desprezadas numa leitura sintética, ao passo que deverão ser levadas em alta conta numa leitura analítica. Vez que a

[1] Por direito objetivo entende-se o conjunto das normas de um sistema jurídico interpretado genericamente, i.e., sem referência a qualquer relação jurídica. Vide KELSEN (1998).

intenção é que o leitor possa comutar livremente sua leitura entre análise e síntese, pode ser útil comparar as leituras sintética e analítica, para que se compreenda, entre análise e síntese, o indizível.

As palavras são comumente tratadas com menção à sua etimologia e, por conseguinte, com menção às [significações das] partes que as compõem

Um exemplo disto é como se grafa a palavra *in***forma**ção – os radicais in e forma estão destacados, para lembrar em que sentido se fala de informação, i.e, no sentido em que, pelos processos informacionais, o amorfo é submetido a uma forma, causando sua conformação à mesma, ainda que à custa de sua deformação, i.e., do distanciamento de seu aspecto anterior, seja amorfo, seja de subsunção a uma forma precedente.

Durante a dissertação este artifício é muitas vezes usado para [conferir a ou] exacerbar o caráter polissêmico [de] uma palavra.

A numeração dos capítulos, das páginas e das seções se inicia sempre por zero.

Contar a partir do zero é uma arbitrariedade tanto quanto o é contar a partir do um ou do menos dois. Ocorre que a contagem a partir do um tem como fundamento o corpo, mais *especifica***mente** as mãos e os dedos de quem conta, ao passo que a contagem a partir do zero tem como fundamento uma operação de uma parte interessantíssima do corpo humano, o cérebro [, que é partícipe da formação da mente, que, de seu turno, coopera para a criação da linguagem, que torna possível o surgimento da consciência].

A contagem a partir do um tem por fundamento a pseudo-exterioridade característica do poder olhar seu próprio dedo como um objeto exterior e discreto. Tornar discreto um objeto passa por separá-lo daquilo de que ele não se pode separar: o dedo sem a mão não é mais um dedo, a árvore arrancada da terra não é propriamente mais uma árvore. A repartição e a classificação são os comportamentos que tornam possível imputar a um objeto suas fronteiras, seus limites. Isto é profundamente tratado por Castoriadis (2000).

A contagem a partir do zero tem por fundamento radical a impossibilidade de fundamentar o nada. O nada fundamentado na ausência do tudo não é um nada pleno. O nada pleno é aquele que necessariamente precede, e que, portanto, dá origem ao tudo e, por conseguinte, ao todo. O vazio da mente é tratado com detalhes por Varela; Thompson; Rosch (2003).

A alternância mais ou menos discreta entre presença e ausência, ou entre zero e um surge com o intervalo silêncio/fala, que é longamente tratado por Burke; Ornstein (1998). Assim como, na experiência do falante, o silêncio não se concebe jamais completo, nem a fala se concebe jamais plena, na contagem, nem zero, nem um são números exatos. Mas, assim como na fala, pode-se distinguir [com uma clareza incerta, mas que em geral é bastante,] os eventos de fala dos eventos de silêncio, na experiência da contagem pode-se, em geral, separar-se o zero do um. Interessantemente a justaposição à direita de um zero a um um, torna este um muito mais valioso. O zero é, por fim, ao menos do ponto de vista da grafia hindu-arábica, o maior multiplicador. À esquerda o zero vale nada, mas à direita... ele faz tudo valer muito mais. Por outro lado, elevar qualquer número a zero o reduz ao um, que é um número que já fazia parte da experiência do *homo habilis* (BOURKE; ORNSTEIN,1998).

Ao começar a contagem pelo zero, convida-se o leitor a principiar a leitura a partir de suas incertezas, e não de suas certezas. Como poderia ser possível analisar as convenções humanas com algum afastamento senão pelo recurso ao refúgio ou ao retiro no território da incerteza?

Do ponto de vista da ética que orientou o proceder da démarche, teve-se sempre em alta conta que a incerteza é a grande companheira da humildade e da capacidade renovada de chocar-se, de abismar-se, do ser humano [e, por conseguinte, das ciências humanas, aí compreendida a ciência da informação], que são elementos constitutivos e instituidores do compromisso metodológico com a sinceridade, mais que com a convenção científica chamada de verdade. Do ponto de vista da eticidade que informou este trabalho a única certeza radical – e arbitrária – foi e é a negação da certeza absoluta. A incerteza que se apresenta como não-fundamento básico da abordagem complexa adotada não é a incerteza que exclui a certeza, mas aquela que inclui a certeza como um estado [e como um estágio] da própria incerteza. A certeza admissível é, portanto, aquela que corresponde à contração da incerteza, mas que, para além disto, é parte essencial da continuada renovação da própria incerteza. Mais do que certezas ou incertezas é importante o ciclo dúvidas-certezas-dúvidas.

Da parcialidade da validade de um texto em ciência da informação que verse sobre a validade {e sobre a [jus]validação} das informações em redes telemáticas abertas a partir da consciência da adoção de uma postura ética ao pesquisar

Diferentemente do que ocorre com os textos científicos em geral, não se buscou linearidade na confecção da presente dissertação – nem de raciocínio, nem de linguagem pela qual ele se expressa. Não se prima também por dominar o leitor.

Buscou-se colaborar com o processo de emancipação da personalidade do leitor pela via do contactar o conhecimento científico, para nele, e com ele, desenvolverem-se leitor e autor. Assim, busca-se desenvolver, nas relações interativas das culturas humanas, o próprio raciocínio científico.

Preza-se aqui pela emancipação racional, emotiva e metodológica, tanto do autor quanto do leitor. O leitor deve se sentir, pois, livre para ler este documento na ordem que prefira, e não "seguindo necessariamente a ordem do texto", i.e., a seqüência linear de leitura, que comumente é imposta pelo autor ao leitor.

1.1 CIÊNCIA NORMAL E CIÊNCIA DA NORMA: RESISTÊNCIAS AO ESTUDO CIENTÍFICO DOS PROCESSOS JUS-INFORMACIONAIS

A normatização da ciência, por mais que sofra resistência dos pensadores de vanguarda, contribui para uma padronização, no sentido de imposição de padrões, das ciências normais, vez que as estruturas sociais que permitem e controlam o funcionamento da atividade científica são cada vez mais similarizadas, padronizadas, normatizadas, e financiadas de acordo com as ditas normas da burocráticas [de controle] da ciência. (KUHN, [1997-?]).

Talvez, por isso tenha havido tanta resistência entre os cientistas à emergência de uma ciência jurídica que fosse uma ciência da norma jurídica: não interessaria aos normadores[2] da ciência que a generalidade dos cientistas passasse a estudar as normas [jurídicas] de uma maneira científica.

Seria desinteressante do ponto de vista do controle da atividade científica pelo capital que a generalidade dos cientistas se emancipasse hermeneuticamente ante as normas jurídicas. A ciência da informação e a ciência jurídica encontrariam aí um campo de atuação interdisciplinar claramente definido e de suma importância para o entendimento crítico da importância da atividade dos cientistas na sociedade. Este novo campo se situaria na mesma região de estudo de objeto da informática jurídica, mas com uma perspectiva diferenciada.

---

[2] Aqueles que produzem normas no intento de prescrever a conduta [dos cientistas].

É por este motivo que é tão importante o contributo de Kelsen (1998) não só para a ciência jurídica, mas, como se percebe, para a ciência como um todo. Kelsen fez emergir uma metodologia rigorosa de estudo lógico-**forma**l da norma jurídica, e é a norma jurídica que *con***forma** o funcionamento das atividades científicas nas economias ocidentais.

1.2 FUNDAMENTAL[?]MENTE DIFERENTE

Para ser considerado consistente [e, portanto, válido], um texto científico teria que atender a duas condições filosóficas de base: a primeira é a questão do fundamento (KELSEN, 1998; DOMINGUES, 1991, p. 44-46), e a segunda é a questão da suficiência. Por vezes, o texto da presente dissertação pode parecer não fundamentado. Ele carece mesmo de um fundamento (VARELA; THOMPSON; ROSCH, 2003, p. [223]-239) inicial único. Mas isto não corresponde a dizer que ele não se erija com o apoio de uma rede de múltiplos fundamentos que se co-instituem mutuamente. (CASTORIADIS, 2000).

O procedimento do abandono de fundamento único não é sem precedentes na atividade científica: Einstein (1961, p. 97-100; 105-107; 108; 110), por exemplo, já usava as coordenadas gaussianas para não necessitar de um único centro para a localização x=0; y=0; z=0. Sete pontos jogados a esmo no espaço substituíam o ponto zero. Não somente os textos científicos, mas também a concepção de mundo deixava de ter um único entro x=0; y=0; z=0. Há certamente outros inúmeros exemplos do mesmo tipo de procedimento.

Pode-se mesmo afirmar que está já a morrer aos poucos o emprego de pontos fundamentais pétreos, que emprestariam sua solidez ao discurso científico (PRIGOGINE, 1996, passim) (MORIN, 1999, p. 20-24), e que têm origem num normativismo[3] científico metodológico que já se tornou, de há muito, insustentável (KUHN, 1997; FEYERABEND, 1989).

[3] As idéias de **norma** e de **forma** serão recorrentes no presente trabalho, e têm um capítulo dedicado ao seu estudo. O que vale agora ressaltar é que da experiência da pesquisa ficou claro que o termo **norma** significa padrão para os bibliotecários, ao passo que para os juristas **norma** significa atrator (VARELA; THOMPSON; ROSCH, 2003, p. 104; RUELLE, 1993, p. 79-89; LORENZ, 1996, p. 150-179) para o controle de condutas, de forma que certos padrões de comportamento (WIENER, 1984, p. 48) desviantes do [padrão] estabelecido – ou imaginariamente instituído (CASTORIADIS, 2000) – como aceitável sejam controláveis (ASHBY, 1970, p. 251). Por norma os bibliotecários significam padrão ao qual se pode ou não aderir. Por norma os juristas significam padrão que, inadimplido, i.e., recusado por um sujeito, gera a possibilidade de aplicação de sanção. A sanção (KELSEN,

Edgar Morin assim (1999, p. 32) destaca o que já ocorre na epistemologia, que, com Rescher, deixa de depender de enunciados de base:

> Se a epistemologia complexa tomasse forma, constituiria não uma revolução copernicana, mas uma revolução hubbleana. Hubble mostrou que o universo não tem centro. A epistemologia complexa não tem fundamento. A noção de epistemologia sem fundamento já foi sugerida por Rescher. Em vez de partir dos 'enunciados de base' ou 'protocolares' que, na visão do positivismo lógico, forneciam ao conhecimento um fundamento indubitável, Rescher imagina um sistema em rede cuja estrutura não é hierárquica, sem que nenhum nível seja mais fundamental que os outros [...]" (MORIN, 1999, p. 32).

O caminho (VARELA; THOMPSON; ROSCH, 2003, [223]-239) de explicação científica que ora se inicia é caracterizado pela fundamentação sem fundamento em enunciados de base. A fundamentação que se pretende emprestar ao texto é, como foi a cada passo da pesquisa, gerada por meio de referências que se organizam numa rede de conceitos e de convicções metodológicas convergentes (VARELA; THOMPSON, ROSCH 2003, p. 101). Não se trata de um círculo fechado de coerência, mas de uma ciclicidade aberta (LUHMANN, 1983; 1985a) (TEUBNER, 1996).

Nos limites da abordagem que se fez durante a pesquisa, tanto é praticamente inviável, quanto metodologicamente indesejável, que se promova o afastamento entre sujeito e objeto do conhecimento. "Neste sentido, o operador do conhecimento deve-se tornar, imediatamente, objeto do conhecimento" (MORIN, 1999, p. 36).

É precisamente esta ciclicidade que inspirou o modo de pesquisar, tanto quanto agora inspira o modo de relatar a pesquisa. O itinerário que se traça para que, de um conceito, outros se possam derivar, é sempre sinuoso e recursivo; mas os conceitos se distinguem, ainda que não seja tão claro [nem tão facilmente determinável] onde o campo de validade de aplicação de cada conceito comece ou acabe.

O processo de co-instituição (CASTORIADIS, 2000) dos conceitos não surge – nem poderia surgir – no mundo dos conceitos – como se houvesse um mundo conceitual apartado dos sujeitos; ele ocorre no mundo dos conceitos, que é

1998, p. 121-140) funciona, pois, como um atrator estranho (LORENZ, 1996, p. 168-179) ao padrão de comportamento comunicativo do sujeito.

[re?]criado e reconhecido (CHERRY, 1974, p. 389-457) continuadamente pela sociedade humana, i.e, pelos sujeitos do discurso, inclusive do discurso científico.

E, se é o gregarismo humano que funda a instituição dos conceitos, é o emprego dos conceitos que aprofunda o gregarismo humano. No Capítulo 3, trata-se dos conceitos de **norma** e de **forma**. Eles tanto se entremesclam quanto se distinguem: não há **forma** sem **norma**, nem **norma** sem **forma**; por fim, eles se validam e fundamentam reciprocamente.

1.3 PENSANDO CIÊNCIA SINCERAMENTE: considerações metodológicas

Uma dificuldade ética com a qual se defronta quem pratica a arte de cientista é que seria temerário deixar aberto aos intencionalmente insinceros o campo da ciência. Popper (2000?) fala em falseabilidade, mas nem por isso deve-se buscar a falsidade. A falseabilidade[4] popperiana é, justamente, um esforço de pugnar pela sinceridade. O denunciar a ciência normal – e desmascará-la em sua normalidade [e normatividade!], como faz Kuhn (1997) – é também caminhar no sentido da construção de um compromisso metodológico com a sinceridade.

Vale a pena fugir do conceito de sinceridade, somente porque ele aproxima a ciência da religião? Quando a comunidade científica cria o conceito de ateísmo metodológico, ela não se aproxima demasiado da religião, mesmo que com o intuito de dela apartar-se? Afinal de contas, não é necessário provar a inexistência de deuses ou de um deus para se fazer um discurso vinculado ao ateísmo metodológico?

Não é comum que se justifique a vinculação dos discursos científicos ao ateísmo metodológico, até porque o ateísmo metodológico é aceito pelos grupos prevalentes e hegemônicos que dominam o financiamento das atividades ditas científicas. A ciência não deve, antes de mais nada, deificar-se, nem deificar seus postulados. A verdade é o Deus da ciência? A verdade é na ciência o Deus? Cabe, pois, ao cientista colocar-se como produtor do conhecimento verdadeiro? Ou seria melhor que o cientista se colocasse como um produtor sincero do conhecimento científico?

---

[4] A sinceridade que aqui se propõe corresponde aproximadamente à verdade mitigada pela falseabilidade popperiana. Trata-se não só de honestidade intelectual (AUTOR), mas da tentativa de – a partir da honestidade intelectual – criar bases para uma relação fiduciária com o leitor.

Esta inquietação esteve presente durante todo o trabalho de pesquisa. O relato de seus resultados não se faria sem a prévia nota de que nenhum de seus resultados é 'verdade'. O que se busca é que eles sejam verdadeiros, por verossimilhança. Esta verossimilhança há de ser conquistada e é, por isso que se busca o método.

1.4 DAS PEDRAS NO CAMINHO À BASE PARA CAMINHAR COM COERÊNCIA[?]

Vale uma reflexão sobre o que seja coerência: se a maneira tradicional de escrever no ocidente é linear (BURKE; ORNSTEIN, 1998), paralelamente, a expectativa[5] de coerência dos leitores ocidentais é, por aderência, uma expectativa de linearidade. A coerência é, por conseguinte, sinônimo de ausência de inovação, não devendo, pois, ser cultivada pelos cientistas.

O leitor ocidental reconhece como coerentes os textos que seguem esquemas de redação lineares e tradicionais. A expectativa é, pois, condicionante da atividade de leitura. Assim, onde se lê *A*+*B*=... espera-se com ansiedade[6] a letra *C*, logo após o sinal de igualdade. Este imediatismo ansioso compõe o quadro de irritabilidade característica das sociedades ocidentais.

O teste de coerência[7] que se deve aplicar a um texto complexo e complexificante, como o presente documento, há que ser de outra natureza: sugere-se ao leitor que dê saltos entre as páginas. Teste-se a similitude do padrão[8]

---

[5] A expectativa que durante a pesquisa se construiu sobre a expectativa dos sujeitos cognoscentes ocidentais é uma expectativa de expectativas no sentido luhmanniano (LUHMANN, 1983, p. 45-53) e tem âncora no cognitivismo presente na própria teoria da autopoiese jurídica luhmanniana (Idem, p. 53-66). No cognitivismo luhmanniano as expectativas normativas são uma espécie de expectativa cognitiva.

[6] O termo ansiedade tem aqui o sentido preciso apresentado em Varela; Thompson; Rosch (2003, p. 143-154).

[7] Feyerabend (1989, p. 45) afirma que a "condição de coerência, por força da qual se exige que as hipóteses novas se ajustem a teorias aceitas é [...] desarrazoada, pois preserva a teoria mais antiga e não a melhor. Hipóteses que contradizem teorias bem assentadas proporcionam-nos evidência impossível de obter de outra forma. A proliferação de teorias é benéfica para a ciência, ao passo que a uniformidade lhe debita o poder crítico".

[8] Em língua portuguesa a palavra 'padrão' corresponde a dois termos diferentes nas teorias em inglês: 1. 'pattern' padrão natural, físisco, químico e biológico, ou padronagem de figuras, geralmente em tecidos e papéis; 2. 'standard' padrão [jus]normativo usado para garantir qualidade e especificação. Na presente passagem quer-se trabalhar com a noção de padrão como padrão natural. Uma melhor noção do que se quer aqui dizer por padrão se encontra em Varela Varela; Thompson; Rosch, p. 104), i.e., na noção de padrões cooperativos emergentes, que graficamente se representam por figuras geométricas fractais, cuja estrutura depende da concepção de atratores de Henri de Poincaré (VARELA; THOMPSON; ROSCH, 2003, p. 104; RUELLE, 1993, p. 79-89; LORENZ, 1996, p. 150-179).

argumentativo (PERELMAN; OLBRECHTS-TYTECA, 2002, p. 15-17; 61-70; ALEXY, 2001, p. 129-141) que as compõe.

A coerência do discurso que aqui se constrói não deve ser a de uma única linha de raciocínio baseada em uma fundação[9], mas a de uma pluralidade (FEYERABEND, 1989, p. 45) de teorias.

1.5 A VERDADE COMO PERGUNTA? CAMINHO PARA A SINCERIDADE METODOLÓGICA?

Na presente dissertação não se busca elencar verdades científicas afirmativas. A verdade que se busca neste discurso em particular é a [aproximação da] verdade como modo de caminhar, e não como destino da viagem. A aproximação da verdade [que aqui se busca traçar] passa pelo ganho heurístico (EINSTEIN, 1961, p. 47-48) na formulação de questionamentos (MORIN, 1999, p. 16) e não na produção de respostas inflexíveis, i.e.:

> A busca da verdade está doravante ligada à investigação sobre a possibilidade da verdade. Carrega, portanto, a necessidade de interrogar a natureza do conhecimento para interrogar a sua validade. Não sabemos se teremos de abandonar a idéia de verdade. Não procuraremos salvar a verdade a qualquer preço, isto é, ao preço da verdade. Tentaremos situar o combate pela verdade no nó estratégico do conhecimento do conhecimento. (MORIN, 1999, p. 16)[10].

As respostas fornecidas pelo texto serão, por conseguinte, sempre transitórias.

Sua importância é sempre menor, e é somente mensurável a partir da análise dos ganhos heurísticos[11] que permitam ao investigador fazer novas perguntas, i.e.: a função das respostas é permitir novos questionamentos.

Composto um novo questionamento, a resposta já terá cumprido sua função metodológica e poderá, portanto ser descartada. No presente discurso, vêem-se as

---

[9] O termo 'fundação' é usado no sentido de Varela; Thompson; Rosch (2003, p. 53-55; [223]-239) e quer dizer aquilo que permite o fundamento, que, de seu turno, permite a fundamentação.

[10] Por "conhecimento do conhecimento" Morin (1999, p.16) quer dizer aquilo que se conhece sobre como o ser humano conhece tudo aquilo que se possa conhecer.

[11] A capacidade heurística é, *grosso modo*, a capacidade de explicar. Quanto mais potencial de explicação houver em uma palavra ou expressão, maior será o seu valor heurístico. Vide Einstein (1961, p. 47-48).

verdades como sucessões transitórias na construção do conhecimento. Todas as certezas são individuais. Todo indivíduo morre. [Salvo a noção de Deus, mas isto está para além do ateísmo metodológico, bem como para além do objeto da pesquisa]. Todas as certezas têm fim, pois só se constituem para finalidades dos indivíduos. Só o sujeito epistemológico tem certezas. Na linguagem intersubjetiva, os significados são mais fluidos (SAUSSURE, 1971), pois que são orientados a finalidades comunicacionais. Toda vez que um indivíduo cogita a incerteza, a certeza morre.

Não obstante, toda vez que uma certeza seja instituída (CASTORIADIS, 2000), será gerado um potencial de ganho heurístico. A verdade plena é indizível, ao passo que parcelas mitigadas da verdade são mais facilmente recortadas do amorfo da verdade toda e completa em prol de uma forma de compreensão ou de entendimento parcial, mas humanamente cogitável. A subsunção da verdade ao recorte, nos termos das possibilidades previamente instituídas de objetivação do conhecimento pelas linguagens humanas, é inevitável sempre que se queira falar da verdade em termos de linguagem. As parcelas – todas popperianamente falseadas – da verdade são nada mais nada menos que o triunfo da linguagem sobre a verdade que permite ao ser humano prever e predizer, i.e., ver antes, antever, ver o futuro na condição de futuro como se passado fosse.

Para intuir e, por conseguinte, para inteligir, o cérebro humano constitui, mediante as estruturas da linguagem (CHOMSKY, 1971; PIAGET, 1998; LANGACKER, 1980) uma mentira sobre o passado que é [ao menos em parte] uma aproximação útil da verdade futura.

Por mais inconcebível e inacreditável que este procedimento imaginativo pareça ser é ele a base do pensamento *pre***ditivo** que, de seu turno, está na base da ciência ocidental. A tal ponto que a ciência ocidental tenha a verdade como um valor ferramental e a predição como um valor teleológico. Não é de se estranhar, pois, a submissão da verdade à predição. Tal submissão está evidente no fato de a ciência, e especificamente a física quântica, ter aberto mão da verdade, em benefício da probabilística, pois a segunda possibilita melhor *pre***ver** o futuro.

A relação verdade/falsidade que orienta a concepção metodológica de sinceridade que aqui se prega está baseada, pois, na relação passado/futuro instituída na e pela linguagem humana, fundada nas bases das separações concretas de partes inseparáveis do contínuo do real, o que permite ao ser humano

dar nome ao inominável, criando, pois, objetos discretos, onde antes só havia o tudo amorfo.

O falso do agora pode, mediante a predição, servir como substituto para a verdade ainda não constituída, mas já esperada para o futuro. Neste sentido, nem toda falsidade é uma mentira. A falsidade está muitas vezes contida na criação do novo. Para projetar o novo é preciso saber fingir tê-lo já criado para, só então, poder comunicar aos demais o que se pretende que o novo seja. Neste sentido, o novo já é um falso novo. O concreto passa a ser uma imitação do imaginário, e o real passa a ser uma imitação do concreto.

Se o leitor acredita que a verdade é baseada na realidade, resta perguntar-lhe: e se o real não for mais que a imitação do concreto, que de sua vez é a imitação do imaginário. A mentira do outro passou a ser verdade para o 'si'. Esta é a maior alienação concebível. Este vínculo de alienação só se pode quebrar com mais imaginação. Quando se comunicar para o outro algo que já se tenha criado, mas que ainda não exista. É para isto que, via de regra serve a *in***forma**ção, em particular a jurídica, para dizer o futuro, antes que o futuro tenha acontecido.

A sinceridade, em contraste, exprime uma idéia ligada à de permanência: de negação da existência de passado e de futuro, de celebração pactuada de um presente contínuo e compartilhado. A sinceridade faz parte do pacto metodológico baseado na humildade, cultuada como opção metodológica cuja manutenção é *conditio sine qua non* ao desenvolvimento da pesquisa e ao oferecimento de seus resultados e conclusões, de seus sucessos e de seus insucessos, à comunidade científica.

A verdade baseada em um único ponto de vista é, pois, potencialmente falsa perante todos os demais pontos de vista que se escolham. Kuhn (1997-?) desmascara criticamente a ausência de justificativa para a escolha dos pontos de vista iniciais das análises científicas.

Para além da crítica kuhniana, vale ressaltar que é física (HAWKING, 1990), lógica (CASTORIADIS, 2000), e fisiologicamente (MATURANA, 2001; 2001a) impossível replicar à exatidão qualquer ponto de vista: para cada alteração de ponto de vista há uma mudança de verdade correspondente.

Muito útil para o presente trabalho é a construção do conceito moriniano de metaponto de vista (MORIN, 1999). O metaponto de vista permite uma definição rigorosa de sinceridade: aquilo que se possa metodologicamente chamar de

verdadeira a partir de um metaponto de vista será logicamente meta-verdadeiro, ou, se calhar, metodologicamente sincero.

O presente trabalho busca estudar a emergência da criptografia assimétrica e da assinatura digital como novas **formas** de **forma**lizar os fluxos de *in***forma**ção jurídica por um metaponto de vista. Tal metaponto de vista se constitui pelo entrecruzamento das perspectivas do estudo da *in***forma**ção jurídica pela visada da ciência da *in***forma**ção e pela visada da ciência jurídica, interpretada como ciência das decisões de interpretação da norma jurídica que, de seu turno é já um esquema de interpretação (KELSEN, 1998) dos enunciados jurídicos.

Para que fique claro, em vocabulário de ciência da *in***forma**ção: a norma jurídica é tida como *in***forma**ção, ao passo que o enunciado jurídico é tido como dado.

A adoção de um metaponto de vista possibilita vislumbrar vários ângulos de uma mesma observação. As verdades deixam de ser absolutas, e passam a ser relativas, no sentido de que passam a ser frutos de uma relação entre sujeito-observador e objeto-observado. Veja-se, no exemplo abaixo sobre qual é a imagem que '*real***mente**' aparece na tela de um aparelho de televisão, como as verdades mudam conforme se alterem os pontos de vista:

a) Se o leitor observar demasiado perto uma tela de TV, tudo o que verá são pequenos pontos luminosos, ou seja: verá os *pixels*, mas não verá 'a imagem';
b) A quantidade apropriada de metros que cada telespectador deve guardar da tela observada não é uma grandeza que se possa atribuir nem tão somente à qualidade e tamanho da tela, nem tão somente à acuidade visual do tele-espectador: a distância depende do objetivo;
c) Um proprietário de um televisor, para remover-lhe da tela alguma sujidade, talvez queira olhar mais de perto a tela do aparelho muito mais de perto que quando assiste habitualmente a programação;
d) Não existe portanto 'a distância correta', mas tão somente há distâncias adequadas às diversas necessidades e finalidades pretendidas.

Maturana (2001a) trata da questão da realidade como constructo lingüístico, mental e, em última instância, neurofisiológico do ser humano.

Daí, a presente dissertação ser, não o que o autor deseja que ele seja, não o que está [realmente?] escrito, não o que é entendido pelo leitor. A dissertação é o

acoplamento entre todas estas estruturas. É, pois, inviável definir o presente documento como conduto da verdade.

É natural que a essência mesma desta dissertação seja multifacetada e multi-referencial. Tudo o que se disser sobre a essência do documento será falseado no sentido popperiano. Não há verdade absoluta. Tudo, pois, é [ao menos parcialmente] falso [– e isto inclui tudo o que o leitor pensa que foi dito pelo autor neste documento, bem como tudo o que está escrito, bem como tudo o que o autor pensa ter expressado].

Ao ler com muito detalhe cada frase do presente caminho explicativo, talvez o leitor tenha a impressão de não entender o que lê, assim como quem olha a tela de um televisor de um ponto exageradamente próximo. Um pouco de distanciamento da tela do televisor pode, então, parecer-lhe adequado. 'A imagem' que motiva as transmissões de radioteledifusão só será reconhecível no conjunto de *pixels* se este for observado a uma certa distância[12] pelo telespectador. Distância demais, ou de manos, implica na impossibilidade de se olhar para o televisor na condição de telespectador. O texto foi escrito para possibilitar saltos de leitura e leituras parciais. Não para iludir o leitor numa seqüencialidade redacional normativa e hipnótica, mas vazia de vivências pessoais.

Há que se esclarecer também que aqui não se nega a utilidade da clareza: claro e escuro são elementos igualmente necessários para compor a penumbra que torna possível ao ser humano enxergar. A não-linearidade é em grande parte composta por múltiplas linearidades fracionárias. O não-linear em sentido amplo não exclui a linearidade, por mais que a expressão dê essa impressão. O não-linear, em seu sentido mais amplo, compreende aquilo que, em senso restrito, costuma-se chamar de linear e tanto quanto aquilo que, em sentido restrito, costuma-se chamar de não-linear.

O que se escreve daqui por diante foi construído para ser lido com atenção à evolução do movimento do texto todo, diante das múltiplas leituras que dele se possa fazer. Pode-se optar, pois, por guardar alguma distância dos detalhes em cada parágrafo.

---

[12] Na ciência normal o afastamento é patrocínio exclusivo do autor. Aqui se pretende que o afastamento seja, na medida do possível, fruto de um consensuamento com o leitor. O texto parte da premissa de que o leitor é sujeito. O texto é, pois, construído em uma intersubjetividade, ainda que esta subjectividade seja artificial, i.e., fruto de um esforço redacional.

1.6 AS PARTES DA DISSERTAÇÃO E SUA FUNÇÃO

O objeto do trabalho é a [jus]validação [dos fluxos telemáticos] de *in***forma**ção.

Precisar a significação de alguns termos foi um primeiro passo tomado na dissertação. Com isto, buscou-se conferir maior potencial de compreensão ao trabalho. Os termos cuja significação se precisou foram os seguintes:

a) Primeiramente: *validar, validade* e *validação*;
b) Em segundo lugar, *fundamentar*, *fundamento* e *fundamental* [já que a fundamentação é de ordinário empregada para **jus**tificar a validação];
c) Em terceiro lugar: *norma*, *normal* [já que as normas são de ordinário empregadas como fundamento de validade] *norma jurídica* e *normatividade jurídica* e, paralelamente;
d) Forma, formal, formalidade, formalização e, por fim, informação e informação jurídica.

Durante este processo, detectou-se que o que os cientistas da informação compreendem por validade da informação é diverso daquilo que os cientistas do direito compreendem por validade da informação. Buscou-se, pois, aclarar o qual seria o significado preciso do termo *validade da informação* no corpo da presente dissertação.

Como na dissertação se considerou a informação como sendo um processo cujos resultados são, de um lado, a forma e, de outro, a formalização, decidiu-se que a indagação sobre a validade da informação como se ela fosse um produto seria inadequada. Passou-se então a se indagar sobre a validade dos fluxos de informação, e a não mais considerar que uma informação possa ser válida *per se*. A validade não é, pois, um atributo ou qualidade da informação, mas uma relação que se constrói entre processos informacionais.

Daí por diante, analisaram-se as várias conexões entre validade jurídica e informação. A informação jurídica não foi visada como sendo um recorte classificado da informação. O que se analisou foi um par de constatações: 1) a juridicidade de todo e qualquer fluxo de informações, i.e., o fato de que qualquer fluxo de informações pode ser classificado como lícito ou ilícito e; 2) o aspecto informacional de todo o processo de formação da juridicidade.

Sendo assim, ver-se-á que uma cooperação estreita entre cientistas do direito e da informação terá o potencial de construir uma melhor compreensão da validação dos fluxos de informação por meio das redes telemáticas abertas, em particular, por meio da Internet.

Buscou-se estudar a validação dos fluxos de informação a partir de uma perspectiva que fosse a um só tempo infojurídica[13] e jus-informacional[14] uma tal validação o emprego de um arcabouço híbrido de validação que repousa, de um lado sobre a matemática, de outro sobre o direito começa a despontar como uma solução jurídica e economicamente viável e praticamente implementável, a saber: as infra-estruturas de chaves públicas.

Para compreender como as informações se puderam tornar representações consideradas válidas de uma realidade supostamente exterior ao observador que constituiriam as bases para as argumentações jurídicas, traçou-se um percurso reflexivo sobre as origens da escrita e dos enunciados jurídicos escritos. Analisa-se paralelamente a relação 'enunciado jurídico' – 'norma jurídica' como sendo uma relação 'dado [jurídico]' – 'informação [jurídica]'.

Refletiu-se, logo a seguir, sobre o fato de que o ser humano teria começado a escrever para contar e, logo depois, para prescrever a conduta alheia. Reflete-se sobre a evolução da escrita, inclusive sobre como evoluiu a natureza críptica do escrever.

Os caminhos << ***não [poder] ver*** ► **ver** >> e << ***não [poder] ler*** ► ***[poder] ler*** >> passam a ser percorridos por um caminhar reflexivo. Toda escrita é visada como sendo mais ou menos desafiadora para o seu potencial leitor. A criptografia surge como um dificultador intencional à leitura.

Sendo assim, a criptografia, em primeiro lugar, e a escrita digital, em segundo, são consideradas partes da evolução do [pr]escrever. Somente em terceiro lugar surge a consideração da escrita criptográfica digital como uma evolução da escrita digital. Os adventos da criptografia assimétrica e, depois, das infra-estruturas de chaves públicas são considerados os mais recentes avanços no sentido de se compor uma escrita digital capaz de compor enunciados jurídicos [jus]válidos e, por

[13] Por perspectiva infojurídica se quer expressar 'perspectiva de análise dos fluxos de informação para fins jurídicos'

[14] Por perspectiva jus-informacional se quer expressar 'perspectiva de análise da formação tanto de direitos quanto do próprio sistema jurídico' a partir dos fluxos de informação jusnormativa.

conseguinte, [jus-]confiáveis. Somente depois destas reflexões se passou a expor em linhas gerais do funcionamento da ICP-Brasil.

Ao trilhar este percurso se espera deixar um caminho-espaço aberto para as interlocuções entre cientistas do direito, da informação e da computação, no que se relaciona com a compreensão da validade jurídica das informações digitalmente assinadas e/ou assimetricamente encriptadas.

2 **OBJETO E OBJETIVOS**

O objeto do trabalho é a [jus]validação [dos fluxos telemáticos] de *in***forma**ção. São, pois, termos de suma importância para a compreensão do trabalho os seguintes:

a) Primeiramente: *validar, validade e validação*;

b) Em segundo lugar, *fundamento, fundamentar e fundamental* [já que a fundamentação é de ordinário empregada para **jus**tificar a validação] e, por fim,

c) Norma, normal [já que as normas são de ordinário empregadas como fundamento de validade]

Ocorre que a visada da ciência da informação sobre validade da informação é diversa da visada da ciência jurídica. Na ciência jurídica a visada é sempre em termos de licitude, i.e., em termos de lícito/ilícito (KELSEN, 1998). Já em ciência da informação, a validade da informação tem mais a ver com sua integridade, autenticidade e preservação (UNDERWOOD, 2002). Assim, não obstante uma informação ser considerada válida do ponto de vista da ciência da informação, pode ser – a um só tempo – considerada inválida para fins jurídicos.

A visada da ciência jurídica é mais restrita que a visada mais geral da ciência da informação. E, para os fins desta pesquisa é a mais adequada. A informação ilícita não pode ser considerada válida, ainda que íntegra e autêntica. É o caso da prova obtida por meios ilícitos, ou da informação correta, mas inapropriada, sobre acontecimentos vexatórios na vida de uma criança, que não devem chegar a público. O fluxo incontido da informação seria, nesses casos, ilícito e, portanto, inválido.

Uma particularidade da visada desta pesquisa é que a informação não é considerada válida *per se*. Só o fluxo da informação pode ser considerado válido/inválido ou lícito/ilícito. Outra particularidade é que nenhum fluxo informacional pode ser considerado válido ou inválido *per se*. Há um claro elemento teleológico na análise da validade/invalidade ou licitude/ilicitude do fluxo informacional. Um fluxo que deveria ser evitado pode ser reativado para que se possa cumprir uma investigação, ou uma perícia.

A validade do fluxo de informações pode ser limitada até mesmo por contrato ou legislação. Um determinado certificado digital pode ser aceito como

validador para transações de até R$ *n,00*. Para qualquer quantia superior a *n* reais, o certificado restaria inválido por força contratual, ou de lei.

Assim, se de um lado a ciência jurídica pode se beneficiar dos frutos da ciência da informação para melhor tratar os fluxos [juridicamente validáveis] de informação jurídica, por outro, a ciência da informação pode se beneficiar dos frutos da ciência jurídica nos estudos de validade/invalidade de um documento para uma finalidade determinável qualquer.

Esta cooperação entre cientistas do direito e da informação possibilitará uma melhor compreensão da validação dos fluxos de informação por meio das redes telemáticas abertas, em particular, por meio da Internet. Para uma tal validação o emprego de um arcabouço híbrido de validação que repousa, de um lado sobre a matemática, de outro sobre o direito começa a despontar como uma solução jurídica e economicamente viável e praticamente implementável, a saber: as infra-estruturas de chaves públicas. Mas, para compreender o funcionamento de uma infra-estrutura de chaves públicas será primeiro necessário compreender a criptografia e a assinatura digital. É este, em síntese, tanto o objeto quanto o percurso [de objetificação do objeto] desta dissertação

2.1 LIMITES E EXTENSÃO DO TRABALHO

O trabalho de pesquisa se debruçou justamente sobre as estruturas do universo da *in***forma**ção jurídica, mas nem todas as estruturas deste universo são objeto da *démarche*.

A visada da *démarche* científica ora relatada exclui os estudos sobre o fluxo de documentos da área jurídica não afetos à questão da possibilidade de aplicação em larga escala da assinatura digital e da criptografia assimétrica. Estes podem ser melhor desenvolvidos em sede apropriada, em uma pesquisa que suceda e dê continuidade ao esforço que ora se encerra.

Definiram-se, então, estes limites: apenas interessam à análise que se levou a cabo aqueles aspectos dos fluxos de *in***forma**ção jurídica que, regra geral, são excluídos das análises que costumeiramente se fazem no campo da ciência da *in***forma**ção, i.e., interessaram somente à pesquisa aqueles aspectos dos fluxos de *in***forma**ção jurídica que são ora demasiado grandes (o sistema jurídico), ora demasiado pequenos (a norma jurídica e seus elementos), para serem submetidos à

observação direta ou literária pelo profissional da *in***forma**ção. Busca-se estudar o lado dos fluxos de *in***forma**ção jurídica que só pode ser vislumbrado por meio de uma leitura jus-hermenêutica que se contente somente e tão somente com a classificação válido/inválido nos termos de lícito/ilícito.

Na interpretação jurídica do dia-a-dia, busca-se fundamentar (KELSEN, 1998; 2000c) a tomada de decisão (FERRAZ JUNIOR, 2003, p. 310-316; PIMENTEL, 2000) em relação a uma dada situação submetida à análise de um julgador. E isto se faz por intermédio – e na circunstância – de uma cultura de interpretação (MAXIMILIANO, 1984) da *in***forma**ção jurídica que é, a um só tempo[15] (OST, 199[9]?), normativa (KELSEN, 1998) e sistêmica (CANARIS, 1996).

Diante da concepção de *in***forma**ção jurídica como *in***forma**ção normativa e sistêmica, é necessário criar um discurso – e aqui se pugna ao menos pela criação de suas bases – que permita compreender as ligações hermenêuticas plurais (BOUCAULT; RODRIGUEZ, 2002) entre processos hermenêuticos (SCHLEIERMACHER, 2001; MAXIMILIANO, 1984; STRECK, 2003) jus-*in***forma**cionais – que se desenvolvem no universo da norma jurídica (KELSEN, 1986; KELSEN e KLUG, 1984) – com aqueles processos hermenêuticos jus-*in***forma**cionais – que se desenvolvem no universo do sistema jurídico (CANARIS, 1996) auto-referente (LAVIÉ, 1986) – ou, melhor dizendo, do sistema jurídico autopoiético (LUHMANN, 1983; 1985a; TEUBNER, 1996).

2.2 PERCEPÇÃO E ABORDAGEM DO OBJETO: ENTRE LUZ E TREVAS – SÓ NA PENUMBRA É CONCEBÍVEL A VISÃO

Luz diretamente direcionada aos olhos de um observador pode até resultar em cegueira permanente; já sua ausência impedirá que o observador veja qualquer coisa que seja. A quantidade apropriada de luz necessária para que se possa ver difere de um observador para outro, mas todo e qualquer observador depende do contraste: a visão só se constitui, pois, na penumbra (MATURANA, 2001, p. 77-105).

A aparência oblíqua da linguagem usada no texto é mais fruto da defasagem lingüística do mundo científico do que duma intenção estilística do autor, que teria preferido traçar linhas menos confusas, embora igualmente entremescladas. Cada

[15] OST (199[9]?) trabalha com a noção de tempo no direito. Para uma noção mais ampla da evolução do conceito de tempo vide HAWKING (1990).

campo da ciência sofre uma decalagem lingüística em relação aos demais. Ocorre que o entremesclar das linhas do caminho explicativo reflete o entremesclar de racionalidades que compõem a complexa Sociedade em Redes. Formam-se redes de cientistas advindos dos mais diversos campos da ciência. Esta foi uma experiência presente no cotidiano da convivência do mestrando na REDPECT, Rede Cooperativa de Pesquisa e Intervenção em (In)formação, Currículo e Trabalho.

A Sociedade em Redes é composta por redes de relacionamentos humanos, que, por seu turno, são compostas por emaranhados de interesses, pela pluralidade de discursos, e pela multiplicidade das possibilidades de leituras e de releituras destes discursos diante do emaranhado de interesses (LAVIÉ, 1986).

A assinatura digital (REPÚBLICA..., 2001; BENSOUSSAN, 1999; TRUDEL et al, 1997, p. **19**-23 – **19**-33[16]; MENKE, 2005, p. 36-96; MARCACINI, 2002, p. 59-117) vem compor **forma**lmente mais um nível lógico-hierárquico-**forma**l das comunicações **forma**is das *in***forma**ções nas sociedades humanas: a comunicação **forma**l de *in***forma**ções juridicamente validadas, juridicamente válidas ou juridicamente validantes. Trata-se de mais uma justaposição de tecnologias que cria um nível de complexidade mais inescapável, mais entrópico[17].

Não havendo possibilidade lingüística de descrever em termos simples o emaranhado de técnicas, lógicas e tecnologias que mantêm a sociedade em redes 'funcionando', passa-se a usar uma linguagem que fale de cada uma das partes deste emaranhado. Isto sim pode ser feito em linguagem linear, num clima de penumbra menos inabitual, cujo grau de clareza/escuridão possa ser o mais cômodo possível para o leitor.

O objeto da pesquisa é, pois, o aspecto críptico da [jus]validação da *in***forma**ção. A jusvalidação é críptica, em primeiro lugar, porque o direito é um sistema de informações cuja interpretação hermenêutica resulta sempre eivado [ou dotado] de um certo grau de imprevisibilidade e, em segundo lugar porque aplica a [cripto]grafia como elemento validador.

---

[16] Em Trudel (1997) as páginas são numeradas por capítulo: **19**-23 significa página 23 do capítulo 19; **19**-33 significa página 33 do capítulo **19**.

[17] O conceito de entropia nasce na termodinâmica como medida da irreversibilidade de um processo termodinâmico e se espalha pela ciência, como medida de complexidade (RUELLE, 1993, p, [145]-150). Na teoria da informação de Claude Shannon o conceito de informação é "calcado no conceito de entropia", que consiste na "quantidade de acaso presente no sistema" (RUELLE, 1993, p. 181). O físico belga continua e explica que a informação é medida em termos de acaso "[s]implesmente porque, ao escolhermos uma mensagem dentre toda uma classe de mensagens possíveis, livramo-nos da incerteza ou do acaso presente nessa classe." (Idem)

2.3 CONSTRUÇÃO DO OBJETIVO

Numa sociedade em redes em que, cada vez mais, os profissionais trabalham em equipes multidisciplinares, é importante que os profissionais componentes das equipes multidisciplinares se compreendam mutuamente; outrossim vários projetos no sentido de implantar o uso em larga escala da assinatura digital pelo mundo jurídico sofreram reveses ou, no mínimo, atrasos.

O objetivo da pesquisa é criar bases para permitir uma interlocução [pela aplicação de um lastro conceitual comum] entre os profissionais do direito, da *in***forma**ção e da computação ao trabalharem com criptografia, assinatura digital e infra-estruturas de chaves públicas na qualidade de ferramentais de [**jus**]validação da *in***forma**ção

A relação entre um padrão socialmente compartilhado de *in***forma**r (ou seja, uma linguagem) e a concepção de concertação[18] dos padrões de comportamento dos mais diversos seres humanos – para que cada um use padrões de comportamento (WIENER, 1984, p. 48-72) mutuamente modulados pelos [padrões de comportamento] de seus pares, ao ponto que se gere a impressão de que há um único padrão[19] de *in***forma**ção naquele grupo humano – é o objeto deste estudo.

O fluxo juridicamente reconhecido – i.e., validado – de *in***forma**ções jurídicas, algumas de grande interesse para a vida nacional e para as finanças públicas, é hora dificultado, hora obstado, seja pelo não uso, seja pelo uso inadequado de técnicas de assinatura digital e de criptografia assimétrica.

Sem o emprego da assinatura digital, e da criptografia assimétrica, a jusvalidação da *in***forma**ção é inviável, pois os documentos digitais simples – como serão aqui referidos daqui a diante os documentos não assinados, nem criptografados – são extremamente fáceis de se alterar, lembrando o que se dá com os documentos escritos a lápis.

---

[18] Por concertação aqui se quer significar todo e qualquer processo de ajustamento social mediante pactuação que tenha como resultado um concerto, i.e, um ajuste socialmente ajustado [dos acoplamentos estruturais] das condutas dos sujeitos.

[19] No sentido de pattern, não de standard.

2.4 O OBJETO DA PESQUISA E A SUA CIRCUNSTÂNCIA PLURAL E MULTI-REFERENCIAL

A circunstância complexa do objeto deste trabalho é justamente a chamada era da *in***forma**ção[20] (MATTELART, 2004): período da existência humana marcado pela superposição frenética de tecnologias – e, por conseguinte, de lógicas e de técnicas. Estas lógicas e técnicas, bem como as tecnologias plurais – a que, a partir delas, chegou o domínio da mente humana – são parte indissociável de tal circunstância.

2.5 ESTABELECIMENTO DE OBJETIVOS ESPECÍFICOS

O trabalho de pesquisa desenvolveu-se não pelo ponto de vista que parte da encruzilhada entre ciência da *in***forma**ção, ciência jurídica, cibernética, [filosofia da] biologia, e passa pelo ponto de vista da necessária lembrança de que a divisão da ciência em campos (BORDIEU, 2001) é um artifício.

Uma vez que objetivo do trabalho é criar bases para uma intelocução interdisciplinar que se inicie no multi-referencial (ARDOINO, 2000); a própria concepção deste metaponto de vista (MORIN, 1999) é já uma conquista.

Atingir-se a finalidade última da pesquisa aqui relatada não pode ser um esforço monolítico. Ainda que técnica e logicamente os esforços quase sempre se entremesclassem e se co-instituíssem, foi sendo criada, para cada um destes esforços – pela via de sua instituição, que se tornou cada vez mais uma co-instituição recíproca – uma identidade particular para cada um dos esforços.

Os esforços *per se* nada mais são do que caminhos explicativos mais simples, que só são passíveis de uma análise que possa fazer sentido, se forem sempre considerados como uma visão amesquinhada[21] do todo.

O todo, de seu turno, não poderia ser analisado como 'o todo', senão comparativamente, i.e., diante da estipulação de que há, dentro do todo, partes, que somente se podem conceber no todo, pelo todo, mas com algum grau de autonomia

[20] Babin (1989) chama o mesmo período de era da comunicação. Na presente dissertação as expressões são tidas como equivalentes.
[21] Isto não é característica do todo, mas fruto da reduzida capacidade de observação do ser humano.

– não da parte, mas da análise parcial do todo que dá origem e fundamentação ao tratamento da parte como parte.

A composição da busca de um caminho explicativo adequado e uno é então, por necessidade mais metodológica que lógica, fracionada da **forma** que a seguir se descreve.

Primeiramente, estudam-se as relações que foram sendo desenvolvidas entre as tecnologias da escrita e as tecnologias jurídicas. O termo tecnologias da escrita deve ser aqui entendido em sua acepção mais ampla, i. e., o de gravar o universo das percepções humanas: desde os cômputos da pré-história assistidos por pedras, ou ossos, passando pelas pinturas rupestres e pela escrita cuneiforme, até as várias **forma**s de representação indireta que são básicas para a existência dos sistemas sociais humanos hodiernos.

Nas tecnologias de escrita que fazem uso da representação indireta estão todas as línguas européias: a palavra simboliza o objeto e a escrita simboliza a palavra. **Forma**s mais indiretas e mais elaboradas de representação cada vez mais indireta incluem a escrita (ou gravação) em *bits* – pela qual é hoje possível escrever números, palavras, imagens, sons – e a escrita criptográfica que se instala costumeiramente por sobre a escrita em *bits*.

Em segundo lugar, estuda-se a concepção de sistema auto-referente, ou autopoiético. É importante, neste particular, passar-se pela teoria geral dos sistemas e pela cibernética, mas também pela bio*logia*, da qual surgiria, mais tarde, a teoria da auto*poiese*, segundo a qual é autopoiético todo aquele sistema cujos eventos de retro-alimentação produzam os elementos do sistema.

Em terceiro lugar, estuda-se a concepção de sistema jurídico como sistema de interação entre seres humanos para decidir sobre *in***forma**ções de controle sobre o ajuste de comportamentos. Estas interações acontecem no bojo de um discurso que não é literal, e sim, hermenêutico. O discurso hermenêutico é também um meio de representação indireta dos objetos.

O sistema jurídico é considerado como sendo um sistema autopoiético, i.e., auto-referente, mas não como totalmente isolado. A clausura é meramente lógica. Estruturalmente o sistema jurídico é aberto.

É, se calhar, útil um exemplo: Se uma organização empresarial fica sem acesso a recursos financeiros ela deixa de poder pagar seus credores. O não pagamento é um dado econômico que se torna [para o sistema jurídico] uma

*in***forma**ção jurídica: o inadimplemento da obrigação de pagar. O inadimplemento da obrigação de pagar, seguido pelo protesto do título[22], ou pelo fracasso da cobrança judicial da dívida abre as portas para o início de um processo de falência. Este início de processo de falência é uma *in***forma**ção jurídica [para o sistema jurídico], mas é um dado econômico [para o sistema econômico].

Se, de um lado, percebe-se o sistema jurídico[23] como sendo um sistema exclusivamente auto-referente do ponto de vista operacional, i.e., operacionalmente fechado, ele é, de outro lado, percebido como sendo um sistema estruturalmente aberto a processos contratuais [jus-econômicos] e constitucionais [jus-políticos] que são base desta abertura *in***forma**cional radical do sistema jurídico.

Em quarto lugar, analisa-se o que é a criptografia assimétrica, em quinto lugar, como ela pode dar origem à assinatura digital, e como esta última é empregada pelo Estado de Direito brasileiro. Como o sistema jurídico tem seu comportamento modulado pelas capacidades e incapacidades *in***forma**cionais de seus atores, toca-se a tecla da necessidade de que se faça uma gestão jus-*in***forma**cional das organizações – termo pelo qual se faz aqui referência também às instituições – que **forma**m, ou melhor, **formulam** o discurso jurídico.

É de costume, para os textos produzidos pelas áreas especialistas e dirigidos às demais áreas, que os textos considerem que o leitor seja um consumidor de resultados, e não um co-criador. Mas, adotar-se uma visada multidisciplinar implica reconhecer no não-especialista um co-criador, sem o qual o trabalho do especialista não pode fazer sentido.

Assim, ainda que cada um possa se especializar em um domínio específico do conhecimento, todos precisam manter-se generalistas para que possa haver um bom fluxo de *in***forma**ções entre as várias áreas de especialidade.

Não basta – para estudar a questão da importância do emprego em larga escala da criptografia assimétrica e da assinatura digital – participar de equipes compostas quer seja só por juristas, seja só por administradores, seja só por cientistas da *in***forma**ção, ou mesmo só por educadores. É imprescindível que o

[22] Documento jusrepresentativo de uma dívida.

[23] Concebe-se aqui o sistema jurídico como um sistema composto por virtualizações, tanto quanto o é a própria escrita. Para além disto, o sistema jurídico é entendido como sendo um sistema de construção de sentidos. Neste ponto pode-se dizer que o sistema jurídico é um sistema significante, i.e., um sistema *in***forma**cional. Buscou-se, então, o que faz com que a uma *in***forma**ção se possa classificar como sendo uma *in***forma**ção jurídica. Esta questão passa, inexoravelmente, pela ontologia jurídica. Sobre o que seja ontologia jurídica vide Da Maia (1999).

educador seja um pouco jurista, um pouco cientista da *in***forma**ção, que o jurista seja um pouco *in***forma**ta, que o cientista da *in***forma**ção seja um pouco jurista, e assim por diante.

É claro que nem se pretende *trans***forma**r juristas em cientistas da *in***forma**ção, nem vice-versa. O que se pretende criar são bases para um discurso que permita o necessário nível de acoplamento estrutural mórfico, i.e, envolvimento [*trans*]**forma**dor, para que o cientista da *in***forma**ção possa perceber qual é a perspectiva do jurista, e vice-versa, que o administrador possa perceber qual a perspectiva do educador, e vice-versa, e assim, sucessivamente.

O discurso cujas bases aqui se traçam deve, pois, permitir acoplamentos de conhecimentos que permitam aos atores participantes de equipes interdisciplinares gerir mutuamente as aprendizagens recíprocas. A análise mais aprofundada deste aspecto foi, no entanto, deixado para um outro momento da pesquisa, por limitações de tempo e de recursos.

Sem mais, passa-se ao estudo da escrita e do surgimento da prática jurídica a ela associada, num sobrevôo desde a oralidade, até os primórdios da generalização do uso [jus-*in***forma**cional] da assinatura digital e da criptografia assimétrica.

3 **[IN]FORMAÇÃO DOS SISTEMAS JURÍDICOS**

Ante a tudo o que o termo ‘sistema de *in***forma**ção’ pode significar, é importante especificar o que se quer aqui dizer quando se afirma que os sistemas jurídicos são sistemas de *in***forma**ção. Mas, antes mesmo de poder fazê-lo, é mister mostrar o que se entende por direito.

Parte-se aqui do postulado de que os sistemas jurídicos são sistemas [in]formativos das sociedades a que pertencem. Os sistemas jurídicos são dedicados à [in]formação de uma estrutura de controle social (WIENER, 1984, p. 104-110).

Dá-se prosseguimento a este esforço estabelecendo que o conceito mesmo de sistema esta cingido ao de relação, e que este último conceito não é razoável sem o conceito de *in***forma**ção.

3.1 VISÃO DO DIREITO COMO SISTEMA DE INFORMAÇÕES

O direito é aqui visto como um sistema humano de *in***forma**ções. Do ponto de vista da TGS – Teoria Geral dos Sistemas – este sistema é explorado pela via da cibernética, que é uma aplicação da própria TGS (LAVIÉ, 1986, p. 5).

Do ponto de vista da teoria da autopoiese, o mesmo sistema humano de *in***forma**ções, i.e., o direito, é visto como um sistema lingüístico auto-referente que se autonomiza, tornando-se autopoiético.

Dizer que o sistema jurídico – i.e., o sistema auto-referente de *in***forma**ções jurídicas – é um sistema autopoiético significa tão somente dizer que não há *in***forma**ção não-jurídica que possa ser tratada pelo sistema jurídico. Por outro lado, do ponto de vista da jusvalidade toda e qualquer informação social humana é jurídica, i.e., pode ser classificada como lícita ou ilícita.[24]

Antes mesmo disto, vislumbra-se a importância da emergência de uma ciência do direito que seja propriamente uma ciência da norma e da decisão em termos normativos [segundo o código lícito/ilícito] para a evolução da ciência como um todo. Para além disto, vale salientar que, se o direito é visto como sendo um sistema auto-referente de *in***forma**ções jurídicas, a norma jurídica é vista como

---

[24] Vide p. 38-41.

sendo a unidade reprodutiva do sistema jurídico, ou seja, a sua instância *in***forma**cional[25].

3.2 VISÃO WIENERIANA: FLUXOS RETRO-ALIMENTADOS DE *IN***FORMA**ÇÃO JURÍDICA.

Em Cibernética e Sociedade, Wiener (1984) afirma que o direito[26] pode ser definido como:

> [...] o contrôle ético aplicado à comunicação, e à linguagem enquanto[27] (sic) **forma[28]** de comunicação, especialmente quando tal aspecto normativo esteja sob mando de alguma autoridade suficientemente poderosa para dar às suas decisões o caráter de sanção social efetiva. (p. 104)

Para Wiener (1984), o direito seria:

> [...] o processo de ajuste dos <<acoplamentos>> que ligam o comportamento dos diferentes indivíduos de maneira tal que aquilo que chamamos de justiça pode ser levado a cabo, e as disputas evitadas, ou, pelo menos, decididas judicialmente.
> (p. 104)

Dessarte – continua Wiener – "a teoria e a prática [do direito] envolve[m] dois grupos de problemas: os de seu propósito geral, de sua concepção de justiça; e os da técnica pela qual êsses conceitos de justiça possam ser tornados efetivos" (WIENER, 1984, p. 104).

Aos 'problemas de propósito geral' os juristas costumam chamar direito substantivo, ao passo que, aos da técnica de efetivação, os juristas costumam chamar direito adjetivo, ou direito processual.[29]

---

[25] O termo 'informacional' é empregado aqui para significar aquele evento lingüístico de acoplamento de algo que pertence a uma lógica exterior à forma da lógica interna do sistema.

[26] Na tradução para o português o termo original 'Law' é traduzido como 'A lei'. Trata-se de um grave equívoco jurídico. Em inglês, 'law' quer dizer direito, ao passo que 'act' ou 'statute' significa lei, ou seja um documento escrito produzido por um centro de poder público que enuncia normas jurídicas de aplicação geral.

[27] O tradutor quer dizer 'como'. No padrão culto, ou *norma*l, da língua portuguesa a palavra 'enquanto' só deve ser usada no sentido de 'durante um intervalo de tempo' e, portanto, não corresponde à expressão inglesa 'as', nem à expressão espanhola 'em cuanto', que está provavelmente ligada à origem do erro de tradução.

[28] Sem grifo no original.

[29] Isto se conclui da leitura comparativa de Wiener (1984, p. 104) e de Kelsen (1998).

Wiener (1984) se confessa liberal e expõe que não há como determinar o que seja este ideal de justiça. Explica que há tantas noções de justiça quanto há códigos morais e religiões. Acaba por aderir aos três valores básicos da revolução francesa[30].

Kelsen (2000b), de sua parte, tem toda uma obra postumamente publicada voltada a demonstrar que a justiça é uma ilusão. Em português o nome que se deu ao livro foi 'A Ilusão da Justiça'. Em setenta e dois capítulos, divididos em quinhentas e dezenove páginas, refutam-se as noções de justiça de Platão, desde o amor pela justiça e, obviamente, o Eros, sem deixar de passar pelo Kratos, noção grega de governo[31].

A posição, à qual se chegou durante a reflexão que permeou a pesquisa, é que se pode tratar justiça como característica daquilo que se tenha [juridicamente] ajustado. Assim, o ajuste de que fala o conceito de direito de Wiener não dependeria somente do "ajuste dos <<acoplamentos>> que ligam o comportamento dos diferentes indivíduos" (WIENER, 1984, p. 104), mas também do acoplamento entre os ajustes.

Dir-se-á, pois, daqueles 'ajustes de acoplamentos entre comportamento dos indivíduos' que forem ajustadamente acoplados a outro[s] 'ajustes de acoplamentos de comportamentos dos indivíduos' que eles são ajustes ajustados (WIENER, 1984). Daí porque daqui por diante chamar-se-á **justiça** *'a característica de comportamento dos indivíduos que façam parte dos ajustes ajustados [de acoplamentos de comportamentos dos indivíduos]'.*

Dito isto, a justiça será tanto um 'stimvlvs' ou 'input', quanto um 'prodvctvs' ou 'output' do sistema jurídico, se considerado pela ótica da cibernética. A *in***forma**ção que flui nos sistemas jurídicos há que ser, então, do ponto de vista da cibernética, uma [*in]***forma**ção de ajustamento dos ajustes, i.e., uma *in***forma**ção promotora de *justiça*. E, se esta *in***forma**ção é tanto um 'stimvlus', quanto um 'prodvctvs', então é forçoso aceitar que os sistemas jurídicos são sistemas informacionais retro-alimentados.

Isto explica porque – por mais diferentes uns dos outros que pareçam ser dois sistemas jurídicos, i.e., por mais diferente que seja a idéia sobre justiça que

[30] Sobre os valores da revolução francesa ver Hobsbawm (1996).
[31] Χυβερνητιχή (Kybernetiké) é uma noção que os antigos gregos aplicavam tão somente ao governo de embarcações, o que se usava para falar de governo, no sentido da politéia, era Kratos.

cada um desses sistemas proclame como a ‘sua idéia de justiça’ – os sistemas jurídicos são capazes de intercambiar *in***forma**ções jurídicas que capazes de criar, de um e de outro lado, deveres e, por conseguinte, direitos. Há mesmo um sistema jurídico criado entre os vários sistemas jurídicos nacionais para facilitar o intercâmbio inter-sistêmico de tais *in***forma**ções. Trata-se do direito internacional público.

Justiça deixa de ser, pois, um conceito vinculado à moral de cada povo, de cada cultura religiosa. A justiça passa a ser uma característica *in***fo**-relacional dos sistemas jurídicos: quando, numa dada relação jurídica, houver um grande fluxo de [*in*]**forma**ções de ajuste, tenderá a haver um ajustamento, do qual decorre uma relação ajustada, i.e, tornada justa.

Este novo conceito geral de justiça é mais útil à ciência jurídica, na sua atividade de construir pontes na direção das demais ciências, que aquele conceito tradicional e desgastado advindo das religiões, que não pode mais sobreviver num mundo em que impera a diversidade cultural. Sem a cooperação com a ciência da *in***forma**ção, seria impossível talhar-se um tal conceito de justiça, baseado em justeza [*in*]**forma**cional das relações jurídicas.

Sem ajustamentos não será viável sintetizar – mediante pactuação – as redes de ajustamentos necessárias à gênese da justiça, i.e, da justeza jus-*in***forma**cional que torna mais difícil o surgimento de surpresas indesejáveis chamadas na linguagem do senso comum de injustiça. Somente pela aplicação da criptografia torna-se possível a comprovação jurídica da integridade e da autoria dos documentos digitais independente de perícia. Esta comprovação é fundamento de autoridade naquelas situações em que o direito exija forma escrita para a comunicação da vontade ou do consentimento, da validade jurídica da relação jurídica cuja gênese [válida], por imposição jusnormativa, dependa de documento **forma**l.

A criptografia é a cabeça de chegada da meta-ponte destes entrecaminhos metateoréticos justamente porque ela torna possível a jusvalidação de documentos tanto imateriais quanto desmaterializados – i.e., transpostos de suportes materiais aos mais fluídos meta-suportes[32] digitais – que torna comprováveis e verificáveis, do ponto de vista jurídico, os procedimentos de celebração de pactos por intermédio do

[32] Vez que se não concebem suportes digitais propriamente ditos, pois que digital é o nome dado a uma técnica específica para se registrar um constructo em todo e qualquer suporte físico imaginável, do papel, passando por superfícies magnetizáveis, e chegando a materiais sensíveis aos raios ‘laser’.

uso de tecnopontas das info-redes que se estabelecem por sobre as redes de computadores. (BARBAGALO, 2001; SANTOLIM, 1995; CARVALHO, 2001)

3.3 AS TEORIAS DA AUTOPOIESE COMO TEORIAS DOS SISTEMAS

As teorias da autopoiese são teorias dos sistemas específicas (LUSSATO, 1995, p. 105-106). Para bem compreender o que isto quer dizer, i.e., para bem compreender o que seja uma teoria de sistemas é primacial o entendimento do que é uma teoria, para somente depois selecionar dentre as teorias aquelas que se dirijam ao estudo sistêmico ou sistemático.

Para fazê-lo, será inescapável a árdua tarefa de se definir o que seja sistema. Durante tal empreitada metodológica, surge a constatação de que há uma miríade de conceitos para sistema e de que há, por conseguinte, uma nuvem densa de definições para o termo sistema.

Somente apoiados em uma teoria dos sistemas bem definida é que se poderá dizer que todo sistema é um corpo de info-relações que interagem entre si e com o ambiente. A necessidade de uma teoria dos sistemas bem definida é também um dos motivos da adoção da teoria da autopoiese e da teoria da autopoiese jurídica[33] para compor, juntamente com a teoria matemática da informação de Claude Shannon (1949), com a teoria da cibernética de Wiener (1970; 1984) e Ashby (1970), e com a teoria do Caos de Lorenz (1996), Ruelle (1993) e Prigogine (1996) o quadro metodológico da pesquisa.

Na teoria da autopoiese o fluxo de *in***forma**ções será então entendido como fator essencial da enteléquia e da ontologia dos sistemas. Com base neste presente constructo lógico é que se pode postular que todo sistema jurídico é um sistema composto de [*in*]**forma**ções jurídicas. Resta ainda a dúvida sobre como, dentre vários sistemas de [*in*]**forma**ção, se pode distinguir quais são os sistemas de [*in*]**forma**ção jurídicos.

[33] Que pressupõe a teoria pura do direito de Kelsen.

3.4 O CONCEITO AMPLO DE *IN***FORMA**ÇÃO ADOTADO NA PESQUISA E A TEORIA DA AUTOPOIESE

O conceito de *in***forma**ção aqui adotado não pode ser restrito à informação humana. Já em 'A Comunicação Humana', Cherry (1974) não se ateve à *in***forma**ção entendida como um fenômeno exclusivamente humano, mas fala de informação em todas as tecnologias de comunicação criadas pelo ser humano até então. O conceito de *in***forma**ção que se utiliza durante todo o texto de Cherry é, pois, um conceito mais amplo.

O conceito usado no presente documento vai além dos limites traçados por Cherry (1974) e se estende também à *in***forma**ção biológica (JORGE, 1995) que tem a ver com os processos **forma**tivos, compreendidos como acoplamentos estruturais[34] em que o 'a**morfo**', o pré-**forma**l, o in**forma**l[35] e o des**forme**' são estruturalmente acoplados a um outro processo **forma**tivo e sofrem subsunção ao [com]portamento da estrutura em **forma**ção.

Na presente dissertação a *in***forma**ção é considerada sempre, pois, como um processo, e nunca como um produto. A **forma** é o produto [da informação], ou melhor, *a adequação de uma segunda estrutura à* ***forma*** *de uma primeira* estrutura é o produto dos processos **forma**tivos [de estruturas] mediante *intro*jeção aqui chamados de processos *in***forma**tivos.

Para abarcar a *in***forma**ção em toda a plenitude de múltiplas referências[36] teóricas que se buscou guardar durante a pesquisa, recorreu-se à teoria da

---

[34] Acoplamentos eletroquímicos das estruturas bioquímicas que constituem os seres vivos. A vida é, pois, vista como um processo *in***forma**cional.

[35] O prefixo 'in' da palavra informal não tem o mesmo sentido do prefixo homógrafo 'in'da palavra informação. No primeiro caso, trata-se de uma indicação de negação, ao passo que, no segundo caso, trata-se de uma indicação de introjeção, que por si só indica um tipo específico de acoplamento estrutural (LUSSATO, 1995, p. 113-116) dos que dá origem a sistemas. Se uma estrutura é inserida no quadro de comportamento de uma outra estrutura, diz-se que elas passam a ter comportamento homomórfico, ou seja, o comportamento da estrutura inserida passa a ter a mesma forma do comportamento da estrutura que sofrera a introjeção. Vide também Rosenstok-Huessy que argumenta que quando o *in***forma**l "[...] se torna um ideal", o *in***forma**l "passa a parecer normal", embora admita que, uma vez que o in**forma**l "é uma rebelião contra o formal", "[n]unca pode o <<informal>> ser chamado de <<pré-formal>> [...]. É depois de as **formas** terem sido criadas e talvez envelhecido até ficar caducas que podemos tornar-nos in**forma**is" (2002, p. 39).

[36] A intenção inicial da pesquisa era posicionar-se como multi-referencial. Esta postura não foi satisfatória para a construção de um quadro teórico que pudesse abordar e lidar com o objeto pesquisado no sentido de abarcar-lhe a análise provinda do metaponto de vista da pesquisa (Morin, 1999) da análise info-cripto-normativa. Criaram-se, pela via do recurso à teoria da autopoiese, não mais referências múltiplas, mas sim, inter-referencialidades. A partir delas é que se decolou – ou, como diriam os portugueses, a partir delas é que se descolou – para a pesquisa.

autopoiese. A teoria da autopoiese é uma teoria específica dos sistemas, criada para explicar o funcionamento dos seres-vivos como máquinas vivas (MATURANA; VARELA, 1994, p. 68-74).

Para selecionar dentre várias *in***forma**ções aquelas que são jurídicas, é necessário conhecer o que caracteriza uma [*in*]**forma**ção jurídica como tal, i.e, qual é a enteléquia da [*in*]**forma**ção jurídica, ou ainda, o que a faz ser compreendida como [*in*]**forma**ção jurídica.

Note-se que a pergunta 'o que faz uma *in***forma**ção ser compreendida como sendo jurídica?' é diferente de 'o que é a *in***forma**ção jurídica?' e de 'onde está a jurdicidade de toda e qualquer informação humana?'. A segunda pergunta presume que uma *in***forma**ção pode ser em si jurídica, ao passo que a primeira busca saber como um sujeito pode [*re*]**conhecer** uma *in***forma**ção como sendo jurídica. A terceira dirige-se a investigar o aspecto pactual e, portanto, jurídico de toda e qualquer *in***forma**ção nas sociedades humanas.

Para responder a pergunta 'o que é a [*in*]**forma**ção jurídica?' seria necessário saber diferenciar qual [*in*]**forma**ção é jurídica e qual não o é, independentemente de qualquer conhecimento sobre os eventuais leitores e intérpretes da [*in*]**forma**ção. Esta pergunta é, pois, irrespondível. Nenhuma [*in*]**forma**ção, jurídica ou não, é independente de quem a **formula** e/ou de quem a *in*terpreta [nem do contexto social dos atores do processo do fluxo *in***forma**cional].

Já para a pergunta 'o que faz uma [*in*]**forma**ção ser compreendida como sendo jurídica?' vale dizer que o que se busca é que tipo de acoplamento estrutural há entre um ser humano que [*re*]**conhece** uma [*in*]**forma**ção jurídica e essa estrutura lingüística do seu ambiente conhecível que é a [*in*]**forma**ção jurídica. Esta é uma pergunta complexa, cuja resposta será sempre relativa aos sujeitos da [*in*]**forma**ção jurídica; mas não deixa de ser, ainda que relativamente, respondível.

Para a pergunta derradeira, i.e., 'onde está a jurdicidade de toda e qualquer informação humana?' Vale dizer que toda informação social humana é linguajada e, portanto, pactuada e pactual. Toda e qualquer informação social humana será, pois,

---

As inter-referências compuseram as inter-referencialidades que serviram de chão, que serviu de base para o impulso de vôo da pesquisa que passou a se posicionar para além das inter-referencialidades, no ultra-referencial, consubstanciado na adoção teorética do meta-meta ponto de vista inspirado em Varela; Thompson; Rosch (2003), ou seja: a teoria da enação foi o universo pelo qual navegou o observador a analisar – horas com o devido afastamento, horas com o devido engajamento – o encadear das inter-referencialidades no entorno teórico do objeto.

seja jurídica, seja protojurídica, mas sempre juridicisante, i.e., genitora da sistematicidade jurídica que acompanha as sociedades humanas.

3.5 A TEORIA DA AUTOPOIESE JURÍDICA E OS FLUXOS DA *IN***FORMA**ÇÃO JURÍDICA

Além da amplitude do conceito de *in***forma**ção, a teoria da autopoiese tem uma outra vantagem que foi basilar para a sua adoção na [e pela] pesquisa, que é o fato de haver uma transposição dessa teoria para o campo da teoria jurídica. Trata-se da teoria da autopoiese jurídica de Luhmann (1983; 1985), que é bastante retocada, quase metamorfoseada por Teubner (1996).

Segundo a teoria da autopoiese jurídica, o sistema jurídico é encarado como autopoiético, i.e., isomórfico aos sistemas vivos. O sistema jurídico é, pois, **forma**do por um fluxo fechado e recursivo de *in***forma**ções que circula numa estrutura radicalmente aberta. O sistema jurídico é visto como um sistema que se constrói por sobre uma base lingüística[37], mas que se autonomiza da linguagem tanto quanto a linguagem se autonomiza do ser humano, i.e, de maneira radical, mas incompleta.

3.6 DO INFORMACIONAL E DO JURÍDICO AO JUS-INFORMACIONAL: DOS PACTOS INSTITUIDORES DA LINGUAGEM À JURIDICIDADE NA SOCIEDADE DA INFORMAÇÃO

O que se aborda na presente dissertação é o lado oculto da [jus]validação da *in***forma**ção jurídica. Penetra-se no território críptico e movediço da validação dos fluxos de *in***forma**ção que instituem no imaginário social (CASTORIADIS, 2000) aquilo que se costuma a nominar (BADIOU, 1994, p. 45) como direito, ou mais precisamente como sistema jurídico (CANARIS, 1996). Explora-se este sistema pelo que ele tem de sistema de *in***forma**ção.

Interessa perceber que toda *in***forma**ção depende sempre da capacidade humana de instituir (CASTORIADIS, 2000), de pactuar. Isto porque toda *in***forma**ção só pode ser humanamente compreendida quando inserida no meio de uma linguagem, cujos símbolos tanto quanto os seus significados precisam ser

[37] A biologia da linguagem é ricamente trabalhada pela teoria original da autopoiese. A linguagem é vista como sendo o elemento ontogenético do ser humano. (MATURANA, 2001a, p. 123-347)

pactuados. O pacto é visto como uma construção jurídica ou protojurídica que permite aos grupamentos humanos comunicar idéias, criar culturas, gerar fluxos de *in***forma**ção.

Assim, antes de dizer que, na presente dissertação se busca estudar no conjunto das informações, aquela parcela que é um subconjunto seu, e no qual estão contidas as informações jurídicas, mais vale afirmar que na presente dissertação se vê toda *in***forma**ção humana como um constructo que se erige por sobre uma infra-estrutura gramatical que é, nos termos de Saussure (1971), pactuada e contratada. A linguagem humana, na qual fluem as *in***forma**ções, é fruto de um conjunto enorme de concertações cuja natureza [proto]jurídica é inafastável.

Num segundo momento, a *in***forma**ção [jurídica] é usada para [re]produzir o direito. É a partir daí que direito e *in***forma**ção começam um entrelaçamento, que continua pela adoção em larga escala da escrita como **forma** hegemônica de expressão da *in***forma**ção [jus]normativa, e que se consolida pela substituição do soberano humano por um soberano textual: a constituição.

Se, antes, o direito era textual e ditado por um ser humano, o soberano, com o advento das constituições escritas, o direito passa a ser textual e ditado por um texto [ou pelo processo interpretativo hermenêutico que se desenvolve na relação social daqueles que aderem ‘ao texto’]: a constituição soberana. O contexto jurídico deixa de ser reto; passa a ser circular, cíclico. Quando o cidadão vota, ele é hierarquicamente superior ao parlamento, quando a lei é publicada ela está, ao menos em tese, acima de todo cidadão. (KELSEN, 1998)

Desde o advento das constituições escritas, pois, o direito, que já era vinculado à **forma**lidade, passa a vincular-se à *in***forma**ção. Todo o fenômeno jurídico agora cabia numa estrutura *in***forma**cional. Não há mais situação jurídica que seja não-*in***forma**cional: toda e qualquer situação jurídica precisa, pois, ser necessariamente expressa em termos *in***forma**cionais.

Por outro lado, não há informação humana nenhuma que não seja passível de apreciação jurídica, ou seja, de classificação como sendo lícita ou ilícita.

Mais ainda, com o avanço das tecnologias de informação e comunicação, o redigir evolui para criar o código de programação e, nas redes abertas de computadores, os códigos de programação passam a representar códigos de conduta (LESSIG, 1999) que são virtualmente inescapáveis, salvo para os mais

hábeis trabalhadores da computação. Um grande exemplo desta juridicização[38] do código de programação é a aceitação – que pode ser tácita ou explícita –, em todo contrato de conexão a uma rede de computadores, dos protocolos utilizados naquela rede. Assim, quem se conecta à Internet se conecta também ao TCP e ao IP. Esta conexão é tanto informática, quanto jurídica.

Pode-se dizer sobre a sociedade da *in***forma**ção[39] o seguinte:

a) Todo fluxo de informação tem um atributo de juridicidade, i.e., pode ser classificado como lícito ou ilícito;

b) A constituição de um sistema jurídico é um processo que somente se constitui mediante fluxo de *in***forma**ção.

Assim, há um vai-e-vem entre a *in***forma**ção jurídica e a juridicidade de toda e qualquer *in***forma**ção [social humana]. Não interessa, pois, manter-se separados os estudos da validade da informação jurídica nos termos de uma dicotomia radical entre ciência da informação e ciência jurídica, ou, em outras palavras: a validade da *in***forma**ção jurídica só pode ser compreendida como sendo a validade jurídica da *in***forma**ção jurídica. Não cabe, pois, falar em validade meramente informacional da informação jurídica. É por isto que doravante se fala em jusvalidação da informação jurídica e não tão somente em validação da *in***forma**ção jurídica.

3.7 INFORMAÇÃO JURÍDICA E DECISÃO JURÍDICA NAS SOCIEDADES DA INFORMAÇÃO

O advento da[s] sociedade[s] da *in***forma**ção[40] é, para Santos (2003), um localismo globalizado. É o hegemônico modelo ocidental de sociedade que adota o capital, e, depois, a informação como a medida do ser humano, e o ser humano como a medida de todas as coisas. Os sistemas jurídicos desse modelo de sociedade, i.e., os sistemas jurídicos ocidentais contemporâneos, são caracterizados pela instituição (CASTORIADIS, 2000) da assunção [pelo decisor jurídico] do dever [jurídico] (KELSEN, 1998) de fundamentar as suas decisões.

Nos sistemas jurídicos ocidentais contemporâneos, qualquer decisão será rejeitada como antijurídica sempre que estiver desacompanhada de fundamentação

---

[38] Processo pelo qual algo passa a ser considerado juridicamente, i.e., em termos de licitude, ou seja de lícito/ilícito.

[39] Conforme vista por Mattelart (2004, p. 81-107).

[40] Conforme vista por Mattelart (2004, p. 81-107).

em termos de *in***forma**ções jurídicas. Para que as decisões possam ser fundamentadas, é necessário um fluxo de informação jurídica que permita que o intérprete-decisor integre os vazios [discursivos] dos processos de interpretação jus-hermenêutica.

É por este motivo que, nos limites desta dissertação, só se considera *in***forma**ção jurídica aquela que produz efeitos jurídicos, i.e., aquela *in***forma**ção que influa no processo interpretativo hermenêutico que culmina com a tomada de decisão. Se uma lei já não vale mais, por ter sido revogada há mais de duzentos anos e por não haver mais nenhum processo em julgamento que faça referência ao período de tempo anterior ao advento da revogação, esta lei não é mais um documento jurídico, mas meramente um documento histórico. *In***forma**ção jurídica é somente aquela que implica **forma**ção do direito.

Supõe-se nas sociedades ocidentais contemporâneas – que abrigam os sistemas jurídicos que interessam a esta pesquisa – que as decisões jurídicas sejam fundamentadas em *in***forma**ções jurídicas [válidas]. Neste sentido seria a *in***forma**ção jurídica que faria o direito [passar a] ser o que ele é, ou, melhor dizendo, seriam os fluxos de informações jurídicas que impulsionariam o devir dos sistemas jurídicos, aquilo que se costuma chamar de [re]produção do direito.

A vinculação entre fundamentação e decisão é, nesses sistemas, tanto um dogma quanto um pressuposto.

3.8 A MENSAGEM JURÍDICA: A NORMA JURÍDICA COMO *IN***FORMA**ÇÃO [JURÍDICA] E O ENUNCIADO JURÍDICO COMO DADO [JURÍDICO]

A norma [i.e., a *in***forma**ção jurídica] difere do texto normativo [i.e., enunciado normativo ou dado jusnormativo] pois é sempre um fruto da interpretação, ao passo que o texto é algo que carece ser interpretado. A ciência jurídica, como ciência das decisões (FERRAZ JÚNIOR, 1980, p. 87) sobre a interpretação (FERRAZ JÚNIOR, 1980, p. 68) das normas (FERRAZ JÚNIOR, 1980, p. 50), é sempre uma ciência interpretativa tanto quanto uma ciência interpretadora e interpretada (KELSEN, 1998, p. 395).

A **norma** jurídica é, pois, intangível, e tem caráter de *in***forma**ção, ou ainda: é fruto de interpretação. Só o enunciado normativo — textual ou não — é

diretamente percebido pelos sentidos humanos — e mesmo isto só é verdade para aqueles capazes de perceber os enunciados como enunciados[41].

Há uma separação jurídica radical entre o enunciado e a **norma**: a ninguém é dado escusar-se do cumprimento de uma **norma** argumentando ignorá-la. Em outras palavras: a **norma**, uma vez enunciada, autonomiza-se do enunciado e torna-se independente da tomada de conhecimento sobre este último.

Daí em diante o enunciado passa a ser, na argumentação e pela argumentação, referencial dos processos de **alter***ação* **norma**tiva, i.e., o sentido interpretado da **norma** é alterado quando se alteram os processos hermenêuticos.

A **norma** jurídica é informação que se passa de pessoa a pessoa, a pessoa... [no sentido de] (KELSEN, 1998, p. 188 - 212) e assim por diante. Sua passagem se dá — ao menos do ponto de vista **forma**l — pela enunciação da **norma** e subseqüente interpretação dos enunciados **norma**tivos (no sentido de compor-se **nova***mente* a **norma** pela interpretação).

A publicidade é, pois, característica fundamental da norma. E a publicidade consiste na comunicação de algo razoavelmente bem definido. Este algo que se comunica é a *in***forma**ção.

3.9 O SILÊNCIO QUE NÃO CALA: O PARADOXO DE A VALIDADE DA DECISÃO NÃO [PODER] SER CONSEQÜÊNCIA DA VALIDADE DA IN***FORMA***ÇÃO

A validade de um sistema jurídico como sistema discursivo está baseada na validade das normas que o compõem, que, de seu turno, está assentada na validade do processo de validação das decisões jurídicas que está, finalmente, assentado por sobre a assunção de que as informações por cujo emprego se compõe a fundamentação das decisões jurídicas sejam informações válidas.

Ocorre que as decisões jurídicas que, em tese, deveriam se basear em informações jurídicas lícitas e válidas baseiam-se, em grande medida, em uma atividade criativa do decisor, que pode até utilizar informações jurídicas, mas que se baseia no conhecimento jurídico para produzir saber jurídico. Isto pode ser demonstrado pela análise do problema da [im]possibilidade da fundamentação da tomada de decisão jurídica com base na *in***forma**ção jurídica.

---

[41] Eis porque aqueles que pleiteiam o direito de conduzir veículos se submetem a testes na busca de impedimentos visuais, tais como o de daltonismo.

O problema da [im]possibilidade da fundamentação da tomada de decisão jurídica com base na *in***forma**ção jurídica se pode resumir nos seguintes termos:

Diante de qualquer questionamento formulado por qualquer jurisdicionado, que pode ser tanto uma pessoa natural quanto uma pessoa moral, ao decisor se impõe o dever jurídico de formular uma resposta que, segundo Luhmann (1983;1985b) precisa estar enquadrada no código binário lícito/ilícito[42]. Assim não há quantidade nenhuma de *in***forma**ção jurídica que o decisor possa evocar para justificar a não tomada de decisão.

O evento (BADIOU, 1994, p. 44) que constitui (CASTORIADIS, 2000) o sujeito decisor como sujeito decisor é precisamente sua sujeição ao sistema jurídico que o impele a decidir, mesmo sem base para decidir. A falta de base jus-informacional não equivale, pois, à falta de fundamento, já que o próprio sistema jurídico prescreve imperativamente a tomada da decisão e, mais ainda, prescreve como o decisor deve agir quando não haja base para decidir.[43]

Se um sistema jurídico for desprovido de bases para validar as decisões jurídicas ele não será um sistema jurídico-estatal rigorosamente constitucional. O decisor não precisaria, pois, sentir-se impelido a decidir, vez que o sistema estaria se constituindo como a antítese do que ele deveria ser. O decisor deveria deixar de sentir-se pertencente ao sistema, e assim, desobrigar-se-ia. Mas o decisor age na precariedade e, para superá-la, decide tornar possível o que até então era impossível: ele decide, i.e., [re]afirma a sua crença[44] em que o sistema jurídico é válido e, *moto continuo*, preenche a lacuna semântica do sistema jurídico, proferindo sua decisão fundamentada.

É o "fato de que o evento seja indecidível [que] faz com que apareça um sujeito do evento" (BADIOU, 1994, p. 45). Ainda segundo Badiou (1994, p.45), o potencial de sujeito se torna um sujeito quando faz uma aposta e decide este conflito que, para Badiou é indecidível. A aposta, para Badiou (1945), consiste em dizer que um determinado evento ocorreu. Nesta dissertação a indecidibilidade é vista como aparente, a partir do fato de que há uma possibilidade de que seja decidida. Se, no entanto se optar por dizer que não há tomada de decisão, mas sim a criação de uma

---

[42] Também chamado jurídico/anti-jurídico.

[43] O exemplo mais vulgarizado de decisão fundamentada, embora **de***s**in***forma**da é, quiçá, o que se formulou já na Roma Antiga: *In dubio pro réu*. Na dúvida, a decisão é considerar não provada a acusação.

[44] Que não tem qualquer base racional.

reação arbitrária que substitua a decisão, sem jamais recompor a cisão original, apenas passando a agir como se ela jamais houvesse existido, pode-se compreender porque Badiou (1945) fala em decidir o indecidível nos seguintes termos: não é a indecidibilidade que é aparente, mas sim a reação à necessidade de um tomada de decisão impossível que é uma aparente decisão.

Assim, no discurso jurídico, o silêncio informacional não equivale a um silêncio semântico, já que o silêncio tem, inegavelmente, um significado. Não cabe dizer que a ausência de *in***forma**ções é, no discurso jurídico, um vazio discursivo, pois esta ausência é cheia, ou melhor, preenchida, de significado, mediante a ação do decisor-intérprete.

Um sujeito da *in***forma**ção jurídica, ou sujeito jus-*in***forma**cional é, pois, sempre um decisor diante de uma aparente[?] inviabilidade de decisão. E, se é a decisão jurídica o evento pelo qual se [re]produz a *in***forma**ção jurídica, é pelo vazio jus-informacional que se introduz, mediante o evento da decisão-interpretação, o impulso [re]produtor dos sistemas jurídicos de *in***forma**ção.

3.10 O FLUXO DE IN**FORMA**ÇÃO JURÍDICA COMO REGULAÇÃO SOCIAL: A INFORMAÇÃO É BASE PARA A CONDUTA

Com Wiener (1984, p. 104-110) se estabelece que a *in***forma**ção que flui no sistema jurídico é voltada para o controle social, mediante o ajuste entre os sujeitos daquilo que Wiener (1984, p. 48-72) mesmo chama de padrões de comportamento comunicativo.

O sistema jurídico passa, portanto, a ser compreendido como uma máquina (ASHBY, 1970, p. 28-84) isomorfa (ASHBY, 1970, p. 109-128) voltada para a regulação e controle (ASHBY, 1970, p. 229-320) de padrões de comportamento comunicativo (WIENER, 1984, p. 48-72).

Desde ASHBY (1970, p. 286-310) se passara a entender que o sistema jurídico é um sistema de informação do tipo sistema muito grande. É em ASHBY também, que, para entender a regulação dos sistemas muito grandes, abrem-se as portas da pesquisa para a noção de que a regulação dos sistemas muito grandes dependem de uma amplificação da regulação (ASHBY, 1970, p. 311-320).

É no estudo da amplificação da regulação que se encontra a noção de amplificação da regulação no cérebro, no ser vivo. É da noção de amplificação da

regulação nos seres vivos – i.e, nas máquinas vivas (MATURANA; VARELA, 1994, p. 67-74) – que se encontram as noções de autopoiese e de homeostase. Este salto em nada é criativo, pois apenas repete o que vários autores sistêmicos já fizeram: a passagem da cibernética para a autopoiese.

O imbricamento pesquisador-problema[45] passa da autopoiese para teoria da autopoiese jurídica (LUHMANN, 1983; 1985b), segundo a qual os sistemas jurídicos são máquinas autopoiéticas, i.e., máquinas vivas (MATURANA; VARELA, 1994).

Mas, se os sistemas jurídicos, na condição de sistemas de *in***forma**ção, são máquinas autopoiéticas, como é que tais máquinas podem se alimentar? De onde vêm as 'proteínas essenciais' que fazem com que o sistema jurídico não seja só um sistema retro-alimentado. Esta pergunta leva à descoberta de [Quiroga] Lavié (1986, p. 7-15; 17-72; 243-357) que demonstra a estreita ligação entre sistemas jurídicos e sistemas políticos por um canal específico de interligação, ou de transmissão de variedade (ASHBY, 1970, p. 141-225) de um sistema para o outro.

Mas há inegavelmente uma outra fonte de alimentação essencial para o sistema jurídico [como sistema de *in***forma**ção] que provém de outro sistema de regulação da sociedade ativa (LAVIÉ, 1986, p.141-204) e autopoiética (LUHMANN, 1983; 1985a). Trata-se da alimentação [do sistema de *in***forma**ção chamado sistema jurídico] a partir de elementos essenciais advindos do sistema de *in***forma**ção chamado sistema econômico.

Teubner (1996) demonstra que tanto a *in***forma**ção política quanto a *in***forma**ção econômica alimentam o fluxo das *in***forma**ções jurídicas mediante um processo de interferência no [funcionamento do] sistema jurídico por canais de contato específicos. A tais eventos de hetero-alimentação Teubner (1996, p. 163-170) chama de ultraciclos, ao passo que aos eventos de retro-alimentação do sistema jurídico são chamados de hiperciclos.

Há ligações estreitas entre os três grandes sistemas de *in***forma**ção que compõe a estrutura básica da regulação social. Para Teubner (1996) a ligação entre sistemas jurídicos e sistemas políticos se dá pela via da constituição – ou processo de interpretação chamado processo constitucional –, ao passo que a ligação entre

[45] O pesquisador não é aquele que pesquisa o problema, nem é o problema [tudo] aquilo que o pesquisador pesquisa. Não há pesquisador em si, muito menos há problema em si. O que ocorre é uma relação potencial de pesquisador ←→ indecidibilidade do problema. Esta relação, uma vez decidida arbitrariamente, constitui tanto o sujeito quanto o objeto da pesquisa.

sistemas jurídicos e sistemas econômicos se dá pela via dos contratos[46] – ou processo de pactuação e interpretação das relações contratuais.

Uma vez situada a *in***forma**ção jurídica no quadro maior da *in***forma**ção de regulação [e controle] social, pode-se afirmar o seguinte: nem toda a *in***forma**ção de regulação social é jurídica, mas toda *in***forma**ção de regulação [e controle] social tem um quê de jurídica, ou seja, toda *in***forma**ção de regulação [e controle] social é, ao menos em parte, jurídica. Para além disto, fica evidente que toda *in***forma**ção jurídica é *in***forma**ção de regulação [e controle] social.

É somente deste emaranhado de constatações e perplexidades que se pode vislumbrar a importância mítica (GROSSI, 2004) da validação da *in***forma**ção jurídica para a sociedade.

Os processos de *in***forma**ção entre seres humanos são caracterizados por sua imersão em relações sociais [humanas] cada vez mais complexas – ainda que, eventualmente, haja busca por simplicidade no uso da linguagem. Mesmo ante esta complexidade das relações humanas (MATURANA, 2001a; 2001b, passim), não há *in***forma**ção sem padrões (CUNHA; BURNHAM, 2004). Nem mesmo há padronização qualquer que seja, do ponto de vista de seu estabelecimento e de sua manutenção, independente de trocas de *in***forma**ção (CUNHA; BURNHAM, 2004).

Não há, na vida social humana, padrões desatrelados de um enquadramento *in***forma**cional, nem mesmo de um conjunto de circunstâncias que contextualizem os fluxos de *in***forma**ção (CASTELLS, 1999; 2003) entre seres humanos. Cada vez mais estes padrões, bem como os processos de padronização que os precedem e que, por vezes, os sucedem, são complexos (CUNHA; FRÓES, 2004).

3.11 DA HOMEOSTASE À LINGUAGEM: A FALA, A ESCRITA, A IMPRENSA E A INTERNET

A homeostase (MATURANA; VARELA, 1994; MATURANA, 2001; 2001a) é um processo pelo qual a vida passou a carregar consigo certas características que antes dependiam exclusivamente do meio, tal como a temperatura entre as células que, nos seres homeotermos, é controlada. A homeostase permite aos mamíferos [e às aves][47] sobreviver em lugares que, em tese, seriam inabitáveis. Foi a

[46] Que Lévy (2003) entende como sendo virtualizações da violência.
[47] Mas essas não importam à linha de argumentação aqui construída.

homeostase, em última análise, que permitiu ao gênero *homo* suas grandes migrações.

O *homo sapiens* é – até o momento – a epítome dos mamíferos, a epítome dos seres capazes [e dependentes] da homeostase. E o é porque a linguagem humana (MATURANA 2001; CASTORIADIS, 2000) chegou a um ponto que permite a um ser humano comunicar uma *in***forma**ção a um seu semelhante, mesmo após a morte do emissor da mensagem. Isto se verificou, primeiro, pela tradição oral, e depois, pela escrita, mais tarde pela escrita digital certificada. A linguagem é um passo a mais em direção à sobrevivência que os seres humanos só puderam dar graças à homeostase. A linguagem coloca os seres humanos em situação mais vantajosa na competição pela sobrevivência. A regulação vai além das células e se espalha pelas sociedades de seres multicelulares.

Não se pode deixar de falar que, para o ser humano, os eventos *in***forma**cionais precedem o próprio nascimento, e acontecem tão cedo quanto a reprodução de seus pais. Não é, contudo, sobre todo o espectro das *in***forma**ções humanas que se debruça a presente dissertação, mas somente sobre uma pequena parte das *in***forma**ções linguajadas, que é o conjunto das *in***forma**ções jurídicas orais e escritas, tradicional ou digitalmente. A escrita digital permite escrever genomas. E escrever genomas pode ser classificado hora como lícito, hora como ilícito.

Na oralidade, esta validação é sensível, vê-se e ouve-se o ancião, ou chefe da tribo, o pajé, o guarda de trânsito. Já nos escritos, a validação das *in***forma**ções precisará assumir outras **formas**, que serão especificadas adiante, e que constituem o objeto da presente dissertação.

Com a escrita mecanizada [e depois *in***forma**tizada, sobretudo com o advento da Internet] surgiu a necessidade de validar a *in***forma**ção de uma maneira diversa da análise da caligrafia, pois seres humanos têm muitas vezes interesses divergentes dos de outros seres humanos. É, pois, plenamente cogitável a criação de ardis para que um ser humano seja [juridicamente] submetido ao poder[48] (LUHMANN, 1985; LEITE, 2001) dum outro. A validação das comunicações de *in***forma**ções humanas linguajadas é, pois, uma necessidade biológica de cada indivíduo da espécie *homo sapiens*, pois é uma necessidade que tem a ver com a sobrevida das sociedades humanas.

[48] Hobbes (2001) já trabalhava a relação entre forma, poder e Estado.

4 **ASPECTOS {JUS[IN]}FORMAIS DAS *IN*FORMAÇÕES JURÍDICAS NA ORALIDADE E NA ESCRITA**

As sociedades humanas intercambiam informações jurídicas pela via tácita – i.e., por gestos ou silêncios cujos significados tenham sido previamente ajustados –, pela oralidade – i.e., pelo uso articulado da fala – e pelos símbolos visuais, escritos ou não.

Gestos e sons pouco **forma**lizados que foram decerto usados para a demarcação de território – e, mais tarde, de propriedade territorial privada – logicamente antecedem a autoconsciência humana. O ser humano já era territorialista antes mesmo que pudesse conceituar território, antes mesmo de que se pudesse chamar o humanóide de humano. Os lobos, as abelhas e mesmo alguns vegetais têm condutas padrão[49] de estabelecimento de prevalências nos processos de ajuste de território.

Se de um lado é claro que os pinheiros da América do Norte não negociam o seu território, de outro é claro que as negociações humanas sobre territorialidade exercem nos ecossistemas função semelhante à dispersão pelos pinheiros de substâncias nocivas sobre o solo.

O que aqui é chamado de *in***forma**ção jurídica é todo processo em que fluem impulsos de infinitas classes [isomórficas]: os primários, ou **forma**dores de acoplamentos [entre condutas humanas]; os secundários, ou os **forma**dores de ajustamentos entre acoplamentos [entre condutas humanas]; os terciários, ou **forma**dores de acoplamentos entre os ajustamentos [entre acoplamentos entre condutas humanas], e assim sucessivamente.

Toda *in***forma**ção jurídica é, pois, um elemento de ajuste entre acoplamentos de condutas humanas ou um evento de acoplamento entre ajustes [de acoplamentos] de condutas humanas.

4.1 PACTOS: NATUREZA [JUS]-*IN***FORMA**CIONAL

Há um tipo evento básico de acoplamento que, daqui por diante, será chamado de pacto. É necessário que haja fluxo[s] de *in***forma**ção jurídica para que

[49] As condutas padrão de controle de território de pinheiros norte-americanos envolvem a dispersão no solo de uma substância que inviabiliza o crescimento de uma vasta quantidade de vida vegetal.

se forme um pacto. Os pactos se dão sempre em um ambiente de *in***forma**ção jurídica que precisa envolver certos acoplamentos básicos, que tornem possível a interação entre as duas partes do pacto; os acoplamentos estruturais entre [os padrões de comportamento d]os atores que estabelecem o pacto são genéticos e experienciais.

Genéticos[50] porque os seres humanos não aceitam a criação de vínculos com outras espécies de vida como pacto, i.e., não importa a natureza afetiva do vínculo que possa haver entre um cão e um ser humano, os seres humanos não aceitam como válido chamar de pacto qualquer coisa que surja de tal relação.

Experienciais porque os seres humanos são incapazes de fazer fluir as *in***forma**ções jurídicas necessárias para o estabelecimento de pactos desde o momento de seu nascimento. A vivência é de fundamental importância para que se possa considerar um ser humano capaz de pactuar.

Para ser [re]conhecido (MORIN, 1999) como pactuador válido, o ser humano precisa primeiro sujeitar-se ao padrão de fluxo[s] de *in***forma**ções jurídicas necessário à participação nos processos de pactuação da comunidade que [re]conhecerá[51] o pacto. Cada comunidade cultural humana tem suas normas [jurídicas] – costumeiras ou escritas – para controlar o [re]conhecimento de novos sujeitados [ao padrão de fluxo{s} de *in***forma**ções jurídicas]. Em ciência jurídica dá-se a esta capacidade de pactuar o nome de capacidade jurídica.

Os pactos são sempre ajustamentos pluripessoais e têm, pois, natureza de relações inter-humanos. Estas relações – os pactos – podem ser estudadas pela sociologia, mas também pela lingüística, pela biologia [da linguagem], pela economia, pelo direito; enfim, não há limites para o tipo de reflexões possíveis sobre os pactos. O que interessa aqui não é nenhuma dessas abordagens clássicas consagradas, mas, tendo em vista que toda a visão de sistema depende de uma visão *in***forma**cional, compreender, mediante uma investigação em ciência da *in***forma**ção, como os pactos influenciam o devir dos meios de jusvalidação da *in***forma**ção [jurídica].

Os pactos, para além do que já se disse, são a base do estabelecimento da linguagem e da língua, como se vê no capítulo que trata especificamente desta

[50] Sobre a gênese do sistema de normas ver Alexy (2001, p. 125-129).

[51] A relação entre cognição e recognição é largamente analisada por Cherry (1974, p. 389-451) que questiona o conceito de realidade do senso comum, perguntando-se “Realidade – Para quem?” (Idem, p. 395-399). A noção de realidade é esmiuçada por Maturana (2001a).

matéria. O que interessa agora é saber que os pactos dão origem aos contratos, bem como aos esquemas de comunicação da *in***forma**ção que tornam possível as comunicações das *in***forma**ções de celebração contratual (BARBAGALO, 2001; SANTOLIM, 1995; CARVALHO, 2001; TUCCI, 2000).

Cada contrato resulta de um acoplamento entre pactos. Um pacto, que é um ajustamento[52] de acoplamentos[53] de condutas [humanas], gera meramente uma obrigação[54] para os seus partícipes; o acoplamento sinalagmático entre as obrigações dá origem aos contratos.

Os contratos se dão mediante arranjos linguajados[55] e, como tais, carecem de interpretação. Quando há desavenças em excesso entre as interpretações dos participes de um contrato, por exemplo, sobre como deve ser satisfeita uma determinada obrigação, gera-se um vazio. É este vazio que relações de maior prevalência tendem a preencher.

4.2 PREENCHIMENTO DO VAZIO INFORMACIONAL DOS PACTOS PELO EVENTO SANEADOR DA DECISÃO

Da necessidade de preenchimento de vazios interpretativos decorre um espaço discursivo[56] jurídico em que autoridades instituídas e/ou constituídas debatem não só sobre o contrato que deu análise à disputa, mas também sobre o seu ajuste ao padrão de contratação[57] que tenha sido adotada pela comunidade de que participem os contratantes. Nas sociedades ocidentais espera-se que este vazio seja logo recomposto mediante a produção de um remendo para este evento de micro-ruptura do sistema jurídico. Tal remendo é chamado de decisão.

A decisão é, pois, um evento de ajustamento entre acoplamentos [fraturados] de ajustamento de acoplamentos entre condutas humanas. Há em todas as culturas registros de como as decisões jurídicas baseadas unicamente na

---

[52] Mediante o fluxo de informações jurígenas.
[53] Idem.
[54] Que corresponde ao termo latino obligatio, que quer dizer literalmente uma subligação, o que, em termos mais práticos quer dizer uma ligação virtual, não material, mas sim lingüística entre os partícipes do pacto.
[55] Mesmo celebrados tacitamente, pois, num sistema jurídico, todo silêncio é *in***forma**tivo, devido ao postulado de que o que não é expressamente proibido é implicitamente permitido.
[56] Um espaço discursivo é aqui entendido como toda e qualquer infra-estrutura que possibilite direta ou indiretamente o fluxo de informações entre os seres humanos.
[57] I.e., de fluxo de informações jurídicas voltadas à criação de um vínculo contratual.

prevalência juspolítico-econômica do decisor sobre os partícipes de pactos levam ao descontrole social. Um tal desajuste leva não raro à perda de poder[58] e de prestígio do decisor, sem que a sociedade deixe de necessitar que alguém desempenhe o papel de decisor.

Para reajustar sua relação com a sociedade, os decisores precisam [re]criar esquemas de validação de suas decisões perante a sociedade. É aí que surge o discurso jurídico, com ele a *in***forma**ção jurídica passa de originária e linear a cíclica e recursiva, sobretudo graças à criação de um meio de justificação perante a sociedade das decisões atuais pelo precedente. Decisões jurídicas passadas passam a ser, pela via da *in***forma**ção jurídica primeiramente dita tradicional, e, depois, jurisprudencial, modelos para as decisões futuras.

A tradição e a jurisprudência são, pois, esquemas de conservação social da *in***forma**ção jurídica. O baixo nível de variância, i.e., a conservação das características, da *in***forma**ção jurídica não implica necessariamente uma conservação quantitativa. Se doze querelas são levadas à instância decisória e todas são decididas de acordo com os precedentes, o procedimento aumenta a força dos precedentes. Já se houver choque entre as interpretações de vários precedentes que se vislumbre aplicáveis a um caso prático, um precedente ou mais podem perder âmbito de aplicabilidade. A repetição é, pois, reforço jus-*in***forma**cional, ao passo que a não-repetição é um esmorecimento jus-*in***forma**cional.

Com o surgimento da escrita, a tradição passa por uma metamorfose que dá origem à jurisprudência, ou seja, ao estudo de documentos escritos que descrevem decisões precedentes. Não seria então necessário ter vivenciado ou presenciado decisões passadas, nem ter estado aprendendo com alguém que as tivesse presenciado ou vivenciado. Bastaria ler o registro das decisões. Daí porque a biblioteca, o arquivo e, mais tarde, os sítios de internet são tão relevantes no dia-a-dia do profissional do direito.

Mas, antes de mais nada, é necessário analisar, dentro dos limites do que é viável diante das restrições de forma e de temática do presente texto, como se dá o fluxo das *in***forma**ções jurídicas nas sociedades sem escrita. É o que se faz a seguir.

---

[58] A expressão poder (BOBBIO, 2001a) é aqui empregada no sentido de elemento constitutivo do mundo jurídico (BOBBIO, 2001b).

4.3 INFORMAÇÃO JURÍDICA EM SOCIEDADES SEM ESCRITA

A constatação de que certas sociedades sejam [ou tenham sido] desprovidas da escrita – ou mesmo desinteressadas pela escrita – não implica que estas sociedades não tenham [tido] alguma espécie de cultura jurídica. Shirley (1987, p. 43) conceitua cultura jurídica como sendo **forma**da pelo menos por "uma [?] opinião sobre o que é uma [?] conduta apropriada e uma [?] idéia [?] de justiça."

Por exemplo, os inuítas – a quem Shirley (1987, p. 40-41) incorretamente chama de esquimós[59] – têm um conjunto [juridicamente][60] articulado de sanções sociais[61] que vão do *escárnio*, exposição repetida e consistente do infrator ao ridículo, evoluem para as *disputas constantes* [, semelhantes ao desafio da cultura do repentista do Nordeste brasileiro e dos cantautores de Portugal], passa pelo *recurso a um ancião*, pela *destruição das armas e das provisões de alimento do contendor*, pelo *desafio para duelo por esmurramento* ***forma****l e sucessivo*, em que cada um dos contendores esmurra tão somente uma vez o seu adversário que, de seu turno, esmurrará em revide, e chega, por fim, ao direito de matar o contendor, que Shirley (1987, p. 41) chama de homicídio.[62]

Em que pese constatar o anarquismo político do povo inuíta, o próprio Shirley também afirma que sua cultura jurídica é composta de "leis (s.i.c.)[[63]] muito bem elaboradas". (1987, p. 40).

Duas coisas ficam evidentes após a análise do texto de Shirley:

a) O nível de **forma**lização dos sistemas jurídicos de *in***forma**ção não é diretamente vinculado ao nível de **forma**lização dos sistemas políticos de *in***forma**ção. [Isto dá mais sentido à leitura do trabalho do jus-constitucionalista argentino Quiroga Lavié (1986), em que se estuda a capacidade de acúmulo de

---

[59] Quando residiu no Canadá – vide Capítulo II – o pesquisador aprendeu que o termo 'esquimó', que significa 'os comedores de carne', é uma ofensa aos inuítas cunhada por povos rivais que habitam áreas logo ao sul dos territórios inuítas. Acredita o pesquisador que o uso imotivado e infundado de linguagem agressiva em literatura científica deve ser evitado. Reproduz-se o termo 'esquimó' apenas para fins de verificabilidade da citação.

[60] No sentido de cultura jurídica que o próprio Shirley (1987, p. 43) apresenta para cultura jurídica.

[61] O termo 'sanção social', embora similar, distingue-se do termo 'sanção jurídica', vide Kelsen (1998, p. 121-124)

[62] Chamar o direito auto-tutelado, mas formalizado, solenizado e regulado pela cultura jurídica inuíta só seria adequado se o autor também se referisse às 'execuções de pena de morte' [das ditas democracias ocidentais] como homicídio.

[63] O uso da palavra lei não foi feliz. Shirley, embora seja professor no Brasil, não é lusófono de nascimento. Usa a palavra leis como se usaria a palavra laws em inglês. O termo jurídico adequado seria dispositivos.

*in***forma**ção política nos sistemas jus-constitucionais. Sob o título 'Cibernética y Política', Lavié (1986) demonstra, usando o método da cibernética, que, quando a quantidade de *in***forma**ção política rompe o limite de capacidade de acúmulo de informação dos sistemas jus-constitucionais, o sistema jus-constitucional como um todo rompe, i.e., torna-se incapaz de operar. O hiato de regulação cria solo fértil para o surgimento de revoluções jurídicas.[64]

b) Não é necessário escrever para **forma**lizar dispositivos jurídicos. A *in***forma**ção jurídica pode, portanto, ser oral e ainda assim ser **forma**l. Na comunicação da *in***forma**ção jurídica a oralidade não implica necessariamente *in***forma**lidade. O povo inuíta **forma**lizou juridicamente seus procedimentos de aplicação de sanção social sem, para tanto, ter sido necessário escrever os dispositivos em **forma** de lei [jurídica escrita][65].

Pode-se extrapolar este resultado para o caso inverso, i.e, nem toda *in***forma**ção jurídica escrita seria necessariamente **forma**l. Um exemplo muito claro do que aqui se propõe, i.e., que há *in***forma**ções jurídicas escritas *in***forma**is é o fato de que tanto os cientistas do direito, quanto os tecnólogos jurídicos[66], consideram os textos escritos que compõem as campanhas publicitárias como sendo parte integrante do conjunto de *in***forma**ções, chamado conjunto probatório, i.e., aquelas *in***forma**ções que documentam a relação jurídica [que, no caso é uma relação contratual[67] de consumo].

---

[64] O termo revolução aqui é aplicado no sentido jurídica, i.e, no sentido de ruptura da ordem jurídico-constitucional.

[65] Toda lei jurídica é um documento escrito. Toda lei jurídica moderna é um documento impresso. O digital permite a criação de documentos fracionários e interligáveis. A legislação já começa, graças aos motores de busca e à capacidade intrínseca de busca dos editores de texto, a ser hiper-lida: o que se espera daqui por diante é que ela comece a ser hiper-escrita.

[66] O termo faz referência aos profissionais do direito, àqueles que não [só] estudam o direito, mas desenvolvem atividades profissionais jurídicas práticas.

[67] Vale explicar, em teoria jurídica diz-se que os contratos não são documentos, mas sim relações [jurídicas]. Os documentos, inclusive o texto escrito chamado 'instrumento de contrato' são comprovações das relações entre as pessoas.

O termo pessoa, na teoria jurídica, não significa o ser humano, mas, guardando fidelidade à etimologia da palavra, a máscara que aparece no cenário jurídico. A metáfora do teatro é, mais que uma metáfora, um elemento constitutivo do próprio vocabulário da teoria [e da prática] jurídica. Esta máscara, para Kelsen (1998, p.188-213), seria, como tudo em direito, composta por normas e por relações entre normas.

5 **FORMA COMO NORMA E NORMA COMO FORMA: INFORMAÇÃO JURÍGENA E JURÍDICA COMO NORMATIVIDADE**

Este capítulo é essencialmente o relato de um trabalho epistemológico que objetivou demonstrar a falta em teoria da ciência da construção de pontes teóricas entre a ciência jurídica e a ciência da informação no que concerne ao conceito de liberdade informacional.

Trata-se de um esforço de pesquisa básica que envolveu aspectos da metodologia científica, da ciência da *in***forma**ção e da teoria geral do direito (FERRAZ JUNIOR, 2000).

Demonstra-se, no curso do capítulo, que a falta de critério no uso de expressões tais como *direito informacional* e *liberdade de informação* seria evitada pela adoção de um campo de significados mais precisamente construído para a palavra *in***forma**ção.

Da imprecisão atual no emprego destes termos resulta que a liberdade *in***forma**cional do autor de logicais é mitigada pela comunidade GNU e pela fiscalidade[68] tributária (CORRÊA, 2000; ARENO; ZUFFO, 2004; BORGES, 1984). Resulta necessário aprofundar o estudo da norma como forma básica da informação jurídica.

A demonstração da ocorrência de vínculos históricos, lógicos, metodológicos e epistemológicos entre o conceito de **norma**, o de **forma** e o de *in***forma**ção é, concluiu-se, fato relevante para a ciência da informação e para a ciência jurídica, mas, sobretudo, para as suas áreas de confluência — dentre as quais convém destacar o direito informático (BAUZA REILLY, 2001a), a informática jurídica (BAUZA REILLY, 2001; PIMENTEL, 2000; BIELSA, 1987; GARCIA, 1976; GUIBOURG; ALENDE; CAMPANELLA, 1996; LOSANO, 2001) e a doutrina dos direitos humanos ou fundamentais (BONAVIDES, 2004)

5.1 TERMINOLOGIA

Para os fins deste capítulo, admitam-se as seguintes definições para os termos a seguir inspirados no trabalho de Maturana (2001):

---

[68] Fiscalidade refere-se à potencialidade de manter-se fiscalizável.

a) I**nformar-se** é dar forma ao [por si] percebido e, por conseguinte, estabelecer-se como forma perante o que se é [por acaso] dado a perceber. Informar-se é interpretar o perceber [o que ainda não se sabe pelo ponto de vista do que já se sabe];

b) I**nterpretar** é um configurar-se diante de si mesmo condicionado [pelo acaso] e pela natureza do si próprio. Interpretar é acoplar-se ao [acaso]. O *mundo exterior* é, pois, fruto sempre da configuração de percepções humanas diante do acoplamento do percebido ao acaso ao que *já se sabia;*

*c) S***aber** é o nome que se dá a estados do conhecer-se [o mundo como experiência própria] cujo processo de alteração percebemos como [quase] estáveis. Estes estados do conhecer-se [o mundo] quase estáveis servem como a **forma** a ser por cada um de nós integrada ao processo do *in***forma**r-se.

Respeitadas estas condições, resulta que *in***forma**r-se é um processo reflexivo pelo qual o sujeito [às condições de sua própria existência, dentre as quais a língua] submete tudo o que aprende à crítica perante o repertório de **formas** [ou **fórm**ul**a**s] do saber de que o sujeito dispõe, ou melhor, pelas quais o sujeito se *in***forma**.

As **formas de saber** são ao mesmo tempo *patrimônio* de cada um de nós, e condicionantes do que podemos ser – e, por conseguinte, do que podemos fazer. O observar[-se] propriamente dito é inviável: como é do senso comum que a ninguém é dado ver sua própria face.

A melhor aproximação ao observar[-se] é o espelho. O estado do sujeito é sempre condicionante da *in***forma**ção, tanto quanto da *per***cepção**. E ainda: toda *in***forma**ção e toda *per***cepção** são *alter***ações** condicionantes do estado do sujeito. Não se pode, pois, de fato observar qualquer estado de si mesmo.

É possível somente observar a transitoriedade dos processos que compõem a própria vida. O estado de si mesmo é fruto da *in***forma**ção, é um saber [adequado às **formas**, ou estruturas configuradas do ser em si]. O estado é um distanciamento [ou falseamento] da própria transitoriedade visando a comunicação.

A **comunicação reflexiva é** também, pois, necessariamente, **um falseamento** de *si* perante *si mesmo*, pelo qual um estado de si é posto à crítica perante a transitoriedade de ser-se, ou melhor, do devir-se. Assim, na transitoriedade da vida do indivíduo: Saber e ser são formas. As formas são, na mesma medida, saberes do ser.

Portanto: Saber[es], ser[es] e forma[s] são sempre condicionadas, tanto mutuamente quanto pela transitoriedade. E ainda: saber, ser e formas [do saber, do ser e do saber-se do ser] são mutuamente condicionantes na transitoriedade do viver[-se] a vida.

5.2 FORMA-NORMA: DA PRÉ-HISTÓRIA AO DIREITO DO ESPAÇO CIBERNÉTICO:

Tratar da origem comum dos conceitos de forma e norma pode ser uma empreitada desconfortável. O desconforto está presente tanto para os juristas quanto para os cientistas da informação. Isto ocorre porque tal tratamento — a um só tempo etimológico e epistemológico — põe em xeque o fechamento dos dois campos da ciência[69]. Sendo o fechamento de campo uma característica paradigmática, (KUHN, 1997) dos ramos da ciência (e normal!) (KUHN, 1997, p. 225) é natural que a reação inicial seja negativa.

Os cientistas filiados à ciência normal dependem do paradigma para conceberem *o método* e *o objeto* de seus *campos científicos fechados*. O paradigma, ao conformar as atividades dos cientistas, conforma tanto *o objeto* quanto *o método* de cada ramo da ciência: daí se pode afirmar que tanto o método da ciência é formal quanto o é seu objeto — e mais: esta característica formal do objeto e do método de uma ciência é fruto do caráter normativo (KUNH, 1997, p. 225) — de um paradigma.

Mas o pior ainda está por ser dito: tanto os juristas quanto os cientistas da informação trabalham de ordinário dentro do ambiente lingüístico (e isto é inevitável!)

---

[69] O fechamento de campo é o que isola um ramo da ciência dos demais. Assim aquilo que é objeto do estudo da física não é objeto de estudo da química nem da sociologia. Mesmo que as três ciências estudem "bancos, cadeiras e poltronas" cada uma terá sua abordagem. O físico estudará os vetores de força que tornam tais móveis resistentes. O químico estudará as características químicas dos materiais de que tais móveis são compostos. O sociólogo estudará sua função social. Conforme o paradigma clássico da ciência, interferir com o fechamento de campo é interferir com a harmonia e com a autonomia funcional (e metodológica) dos diversos ramos da ciência. Quando aqui se prega que norma e forma são dois lados da mesma moeda, a princípio os juristas e cientistas da informação podem reagir em defesa de seu território científico (os seus campos fechados de atuação científica). O que se busca aqui, contudo, não é obliterar as diferenças entre forma e norma, e menos ainda, entre as ciências jurídicas e da informação. Visa-se tão somente demonstrar que os campos de atuação dos partícipes das duas comunidades científicas é fronteiriço. Mais ainda: busca-se demonstrar as vantagens a que ambas as ciências terão acesso se forem construídas boas pontes epistemológicas entre estes campos do conhecimento humano. Este capítulo se propõe a ser um esforço na direção da intensificação da construção destas pontes metodológicas.

(CASTORIADIS, 2000, p. 291). De um lado os juristas costumam pensar no direito como algo que se desenvolve pela língua e na língua; por outro os cientistas da informação costumam trabalhar com a informação como algo que surge também no ambiente lingüístico.

Não obstante estes comportamentos paradigmáticos serem de grande utilidade no dia-a-dia, impõe-se um olhar mais aprofundado. O que parece evidente aos lingüistas, e filólogos, e mesmo aos hermeneutas é que a língua pressupõe forma e norma. Por outro lado forma e norma são incompreensíveis sem língua. (CASTORIADIS, 2000, p.291)

Sendo **forma** e **norma** pressupostos práticos ao surgimento da língua, ou ainda: sendo a língua impossível sem morfologia [i.e., **forma-norma**] e sintaxe [i.e., **norma-forma**] comuns, há que se deduzir que a **forma**lidade e a **norma**tividade instituem-se — e são instituídas — com a língua e na língua. [70]

A relação da palavra com a classe de objetos que ela designe (CASTORIADIS, 2000, p. 277-284) será, pois, sempre fruto de uma convenção (SAUSSURE, 1971, p. 82) entre seres humanos: certo nível de **forma**lidade é, portanto, indispensável (CASTORIADIS, 2000, p. 291) para que os seres humanos se *re***conheçam** mutuamente como sujeitos válidos (MATURANA, 2001a, p. 146-147) da convenção, a que Maturana chama de consenso.

Para além disto, um certo nível de **norma***tividade* é necessário para que a convenção seja útil: a palavra não pode mudar de significado a cada trinta segundos. A comunicação seria inviável (SAUSSURE, 1971, p. 85-93). Por outro lado, nada impede que a palavra vá tendo seu sentido lentamente alterado em períodos mais dilatados, de trinta anos, por exemplo (SAUSSURE, 1971, p. 85-93).

Afirma-se aqui que os primeiros contratos entre os seres humanos não foram redigidos, e sim tácitos — os contratos tácitos, de origem, não são simplificações elípticas dos contratos verbais, mas seus antecedentes lógico-temporais.

Contrariamente ao que indicaria o senso comum, as nossas primeiras redações [ainda na oralidade primitiva] só foram possíveis porque houve convenções — ou, como diria Saussure (1971, p. 22; 85-86), contratos — sobre as

[70] Em outras palavras: quando um ser humano chama algo de garrafa, ele presume que (ao menos) um outro ser humano associará a palavra garrafa a uma determinada classe de objetos. Um outro par de seres humano (enólogos) poderia concordar em chamar de decantador aquilo que os seus desconhecidos companheiros de humanidade chamam meramente de garrafa.

relações entre símbolos e classes de objetos [por eles daí em diante designados] no seio das comunidades humanas do nosso passado mais remoto.

A primeira instituição é a língua – aí incluídas a imagem e a figura, ou melhor, a capacidade figurativa). A sociedade humana é, pois, a sociedade da língua (CASTORIADIS, 2000, p. 259-313). As representações do mundo pela língua são o patrimônio intelectual desta sociedade. Só pela aplicação e pelo uso da língua a família pode deixar de ser um fato natural e passar a ser uma instituição. Só pela aplicação e uso da linguagem jurídica (BITTAR, 2001; WARAT, 1995) o nascimento de um ser humano pode ser mais do que um fato natural. Só pela aplicação do direito, o nascimento de alguém gera o surgimento de uma figura jurídica [: a pessoa] capaz [i.e., **forma**lmente implicada], com direitos e deveres perante a **norma**. O recém-nascido já é mais que filho: é legítimo herdeiro.

Curiosamente, a proposição de Lessig (1999) — segundo a qual o código binário [dos logicais que compõem a estrutura lógica da rede mundial de computadores] desempenha um papel normativo — leva o observador a considerar que, mais uma vez, os conceitos de forma e norma voltam a ser mais que interdependentes e passam a ser convergentes, ainda que não-idênticos. A *in***forma**ção da organização lógica [pelos logicais e protocolos] da *Internet* é também seu primeiro quadro **norma**tivo e **forma**lizador.

Todos escolhemos permanecer conectados de acordo com tais padrões de configuração de logicais e de materiais [para adequar nossos computadores aos protocolos e os logicais aos materiais e vice-versa pelos protocolos]. O novo contrato social – aquele que sucede ao que deu origem à língua – é este pelo qual aderimos à rede das redes. Como aquelas primeiras convenções que estabeleceram **formas-normas** de comunicação (FERRAZ JUNIOR, 2000; FOUCAULT, 2002), estes contratos de adesão que são instrumentos ontogênicos da *Internet*, são reflexivos e recursivos.

Quando aqui se diz reflexivos não se nega a *ultraciclicidade* (TEUBNER, 1996) que consiste no *fato* de que os objetos a que os contratos se referem [não obstante a *auto-referencialidade recursiva do direito*] são [em última, ou em primeira análise] seres não-jurídicos [ou, como se diz na dogmática jurídica: meta-jurídicos].

Não é o direito que define o significado da expressão *processador novo* no contrato pelo qual se compra o tal *processador*. Um contrato de compra e venda de um *processador* tem por objeto *o processador*, e não cabe ao direito definir

primariamente o que quer dizer *processador*, mas apenas secundariamente estabelecer, com maior precisão, que tipo de móvel pode ser classificado [– aí sim secundária e juridicamente –] como sendo conforme a definição juridicamente [– i.e., pela doutrina, pelo contrato, pela jurisprudência ou pela legislação –] atribuída a*o processador*.

Para se entender a instituição da *Internet* há que se somar à noção de que os objetos dos contratos são diferentes do direito — ainda que envoltos pelo direito — a noção de que o objeto de um acordo de conexão à *Internet* qualquer [– aí incluídos os contratos de provimento de acesso e os contratos de interconexão de redes –] não é propriamente a conexão do computador do usuário à rede de computadores do provedor de acesso.[71]

A própria natureza da *Internet* gera a necessidade da possibilidade de acesso [– via computadores do provedor de acesso –] a outros computadores, aos quais, por meio da rede do provedor de acesso [— e de outras redes a que esta rede esteja, ainda que indiretamente, interligada —] o usuário deve ser capaz de acessar.

Impõe-se assim ao provedor de acesso o ônus de celebrar e manter outros acordos [ou contratos] de conexão que permitam a seus clientes acessarem [ainda que indiretamente] redes de terceiros pela via da rede do provedor.[72]

Em outras palavras: o objeto de um contrato de conexão à *Internet* é um ou mais contratos diversos de acesso à *Internet*.

Pode-se, portanto, dizer que cada contrato de conexão à *Internet* se refere mútua e ciclicamente a um grande número de contratos de conexão à *Internet* e que, por fim, este grande número de contratos de conexão à *Internet* se refere mútua e ciclicamente à totalidade dos contratos de conexão à *Internet*.

Eis, pois, como — de uma massa de convenções diversificada — gera-se algo tão diversificado quanto uno: a *Internet*.

Mas isto só é possível porque todas estas convenções pressupõem que, pelo uso da palavra *Internet*, estejam representadas todas as **formas-normas** – i.e.,

---

[71] Não se cumpre o fim do contrato de provimento de acesso à Internet se o usuário é apenas capaz de acessar computadores da rede do provedor.

[72] Na vasta maioria dos países, o acesso à porção estrangeira da Internet pode se dar por variados caminhos (variadas interconexões de redes nacionais a redes estrangeiras). Em outros países, a situação é muito diversa: para manter o controle sobre o fluxo de informações estes países estabelecem um ponto único e estatal de conexão da porção nacional da Internet com as redes estrangeiras. (YURCIK; TAN, 1996).

os protocolos, dentre os quais o TCP e o IP – necessárias ao funcionamento da grande rede mundial.

Esta nova rede de acordos de conexão mútua e ciclicamente auto-referente é o que constitui a *Internet* como espaço de interação social, que, no entanto, independe dos acordos individuais de conexão para permanecer existindo, i.e., a perda de uns poucos usuários não é capaz de descaracterizar a *Internet*.[73] Está, pois, constituído um ser autônomo, cuja natureza jurídica precisa ser cientificamente explicada.

Contudo, a idéia fundamental da Internet não é interligar e sim permitir [pela interligação] o fluxo (CASTELLS, 1999, p. 435-441), e o acoplamento (MATURANA, 2001, p. 146 - 147) de fluxos, que constituem o processo complexo do intercâmbio de informações.

É este intercâmbio de informações que deve possibilitar o bom exercício da *liberdade como autonomia recíproca de acesso à informação* (FERRAZ JÚNIOR, 2001), o que, de seu turno, é essencial para que a democracia não se dissolva em uma sociedade que passa a se comportar como uma sociedade da informação[74]. Também por isso, é logicamente necessário proteger a informação como direito humano [para cada indivíduo] e como direito fundamental [para a sociedade e para o Estado de Direito].

A *Internet* é tão fundamental para o surgimento e crescimento da sociedade da informação quanto é para o seu funcionamento [adequado]. A *Internet* é meramente a *ágor@*, mas ter-se a *ágor@* é já um passo importante no sentido de se possibilitar o diálogo e o discurso democráticos.

Assim, se o discurso democrático deve ser transparentemente regulado para que se mantenha a *autonomia recíproca de acesso à informação*, cumpre que os seus protocolos sejam mantidos livres e acessíveis para que a democracia informacional não se decomponha numa caixa-preta composta de **formas-normas** ou protocolos de comunicação cujo conteúdo seja inacessível ao cidadão.

Tanto liberdade de expressão, quanto liberdades de acesso, geração e dispersão de informações dependem desta disponibilidade para o acesso público aos protocolos básicos da Internet. O progresso da Internet deve então se manter — pelo menos neste aspecto — ligado ao logical e aos protocolos em código aberto.

---

[73] E é por isso que se deve chamar a *Internet* de ser complexo.
[74] Sobre o conceito de sociedade da informação em direito ver Ascensão (2002).

5.3 CONTRIBUTOS DA CIÊNCIA DA INFORMAÇÃO PARA A CIÊNCIA JURÍDICA

Os variados ramos da ciência normal (KUHN, 1997) identificam-se — por meio da operação metodológica chamada fechamento de campo — porque cada um é formal e normalmente competente para tratar, em caráter primário, da delimitação de certos conceitos. Assim, os leigos em ciência sentem que nem cabe ao físico definir o que seja sociedade, nem ao biólogo definir o que seja contrato. Esta sensação geral dos leigos é fruto do paradigma que regia a ciência no Século XIX.

Reconhece-se, pois, a competência da ciência da informação para primariamente traçar esquemas científicos de aproximação do conceito de informação. Quando o faz, a ciência da informação cumpre o imperativo metodológico de delimitação de seu objeto. É devido ao império de normas (BOBBIO, 2001a) como esta que a ciência moderna é chamada de ciência normal.

Seguindo as mesmas normas da atividade científica, deve o cientista do direito recorrer à ciência da informação sempre que buscar delimitar o que venha a significar informação no bojo de uma *démarche* juscientífica qualquer.

Aqui a ciência da informação fornece conteúdo zetético às investigações juscientíficas. [Sempre que se reconhecer *ciência do direito* como ciência dogmática, há que se inferir forçosamente que às demais *ciências* cabem o preenchimento de seu vazio zetético].

Ninguém na comunidade daqueles que lidam com as expressões *direito informacional*, *direito informático*, *direito da informática*, *informática jurídica*, *direito à informação*, *direito sobre a informação*, *liberdade de informação* e, por conseguinte, *habeas data*, ousa negar seu patente caráter zetético. O conteúdo do conceito de informação inegavelmente transcende o campo de aplicação da dogmática jurídica.

5.4 NORMA COMO MENSAGEM PRESCRITIVA DE CONDUTA, E/OU COMO INFORMAÇÃO

Retoma-se aqui a discussão da Seção 4 do Capítulo 0, que consiste, em síntese em [co/i]nstituir a publicidade [da *in***forma**ção normativa] como fundamento de validade da norma.

A norma [i.e., a *in***forma**ção jurídica] difere do texto normativo [i.e., enunciado normativo ou dado jusnormativo], pois a primeira cabe sempre em uma fórmula interpretativa que, segundo Kelsen (1998), é a seguinte:

a) Dada uma **H**ipótese **deve ser** uma **P**restação[75]

b) Dada uma **N**ão-Prestação **deve ser** [a aplicação de] uma **S**anção[76]

O texto **norma**tivo — conquanto seja **norma**tizante e **forma**lizante — não costuma aparecer tão bem **forma**lizado. Assim, diz-se aqui, com o apoio de termos da lingüística (SAUSSURE, 1971), que a **norma** é significado enquanto que o texto **norma**tivo é significante.

Para além disto, poder-se-ia dizer que, para quem a profira, a **norma** é aquilo que se quer dizer pelo texto normativo, ao passo que, para aquele a quem ela se dirija, a **norma** se constitui como o produto da compreensão do texto ouvido ou lido, ou melhor: interpretado.

A **norma** jurídica é, pois, sempre um fruto da interpretação. E, a ciência jurídica, como ciência das decisões (FERRAZ JÚNIOR, 1980, p. 87) sobre a interpretação (FERRAZ JÚNIOR, 1980, p. 68) das normas (FERRAZ JÚNIOR, 1980, p. 50), é sempre uma ciência interpretativa tanto quanto uma ciência interpretadora e interpretada (KELSEN, 1998, p. 395).

A **norma** jurídica é, pois, intangível, e tem caráter de *in***forma**ção, ou ainda: é fruto de interpretação. Só o enunciado normativo — textual ou não — é diretamente percebido pelos sentidos humanos — e mesmo isto só é verdade para aqueles capazes de perceber os enunciados como enunciados[77].

Resiste, ainda, uma separação jurídica entre o enunciado e a **norma**: a ninguém é dado escusar-se do cumprimento de uma **norma** argumentando ignorá-la. Em outras palavras: a **norma**, uma vez enunciada, autonomiza-se do enunciado e torna-se independente da tomada de conhecimento sobre este último.

Daí em diante o enunciado passa a ser [, na argumentação e pela argumentação, referencial dos processos de **alter***ação* **norma**tiva,] i.e., o sentido interpretado da **norma** é alterado quando se alteram os processos hermenêuticos.

---

[75] Kelsen (1998) chama esta parte da fórmula da norma jurídica de norma primária.

[76] Kelsen (1998) chama esta parte da fórmula da norma jurídica de norma secundária, que ele destaca como sendo o núcleo duro da norma jurídica.

[77] Eis porque aqueles que pleiteiam o direito de conduzir veículos se submetem a testes na busca de impedimentos visuais, tais como o de daltonismo.

A **norma** jurídica é *in***forma**ção que se passa de pessoa a pessoa a pessoa [no sentido de] (KELSEN, 1998, p. 188 - 212) e assim por diante. Sua passagem — ao menos do ponto de vista **forma**l — dá-se pela enunciação da **norma** e subseqüente interpretação dos enunciados **norma**tivos (no sentido de compor-se *nova*mente a **norma** pela interpretação).

Esta *in***forma**ção propõe-se a condicionar e influenciar as condutas de complexos pólos lingüísticos de produção, interpretação e aplicação de **normas** que são as pessoas que se submetem à ordem jurídica, mas também supra-ordenam-se (KELSEN, 1998, p.182 - 188) a ela no exercício do poder constituinte e pelo voto.

5.5 SISTEMAS JUSNORMATIVOS COMO SISTEMAS DE INFORMAÇÃO

É de fundamental importância estar-se atento para o fato de que os sistemas jurídicos são sistemas *in***forma**cionais instituídos. Explica-se: os sistemas jurídicos democráticos dependem da publicação dos enunciados de suas **normas** para se reproduzirem no seio das sociedades.

Salvo o costume, que é uma norma não enunciada e pública *ab ovo*, não há **norma** cujo enunciado não haja sido publicado: **norma** cujo enunciado não tenha sido publicado é mera proposta de norma, *ipso facto* da deficiência do pré-requisito da comunicação da norma, o que se cumpre pela publicação formal do enunciado.

5.6 O TERMO INFORMAÇÃO NA LINGUAGEM JUSCIENTÍFICA

Não há maiores esforços, na generalidade dos textos de informática jurídica e de direito informático, produzidos pela comunidade juscientífica brasileira, no sentido de uma conceituação seja mais delimitada, seja mais aprofundada, do termo informação. Uma rara exceção é a doutrina de Alexandre Pimentel (2000).

Em contrapartida — mesmo se abstendo de uma análise minimamente precisa e profunda do conceito de *in***forma**ção — Ferraz Júnior (2001) já busca redefinir o conceito jus-científico de liberdade, quando, num trabalho curto, mas potencialmente revolucionário na agregação de valor heurístico ao conceito de liberdade. E fá-lo assim: “Liberdade [na Sociedade da Informação] é autonomia recíproca de acesso à informação”.

Eis que o conceito em si de liberdade está em xeque e a correr riscos de erosão conceitual plena, caso não se construam pontes teóricas sólidas e abundantes para ligar juscientificamente o conceito de liberdade ao de *in***forma**ção. Há que se proteger juridicamente aquela liberdade que é relevante para a sociedade da *in***forma**ção, sobre a qual discorre Ferraz Júnior (2001).

Faz-se mister — para que se possa bem compreender o conceito proposto por Ferraz Júnior para *liberdade* — explorar aquilo em que consiste o significado da autonomia recíproca, ou seja, há que se buscar um mínimo campo de determinabilidade significacional do que venha a representar para a sociedade e para o direito brasileiros uma *autonomia recíproca de acesso à informação*.

Uma vez que o *direito à informação* goza de um reconhecimento cada vez maior do seu *statvs* de direito humano (BONAVIDES, 2004, p. 356-367), preocupa o pesquisador o fato de que este será sempre um direito deserto sempre que o conceito de informação seja um vazio.

5.7 POLÍTICA DE DIREITOS HUMANOS COMO POLÍTICA DE SUSTENTAÇÃO DO ESTADO DE DIREITO

Bonavides (2004, p. 356-367) promove o direito à informação à condição de pilar do exercício tecnológico (LÉVY, 2000, p.158) da democracia participativa (BONAVIDES, 2003), necessário à sobrevivência do direito na Sociedade da Informação (BONAVIDES, 2004, p. 356-367). Quer-se lembrar que, na doutrina de Bonavides, os direitos fundamentais são aqueles que dão base de sustentação (em outras palavras, fundamento) à existência mesma do sistema jusnormativo.

Ou seja, sem direitos fundamentais, o sistema jurídico pode ser ditatorial e, por conseguinte, transformar-se no oposto do que deveria ser, num arremedo de direito à serventia dos tiranos.

Um sistema que tenha meramente as características formais do direito não será necessariamente um sistema jurídico[78]. Ou isso, ou o direito nazista e as leis da escravatura não eram aberrações. [Vale reler *O Processo* de Franz Kafka]

[78] Por isto mesmo Hans Kelsen se deu ao trabalho de escrever a segunda edição de sua *Reine Rechtslehre* (Teoria Pura do Direito). Isto fica claro pela leitura do prefácio à segunda edição, bem como, pela visão monista a partir da qual o direito de qualquer Estado só vale porque os demais Estados da Comunidade Internacional o reconhecem como Estado legítimo.

Eis que é se levado a crer que, para que um sistema normativo se possa chamar de direito, é importante que tenha fundamentos jurídicos. Eis a importância dos direitos fundamentais: são eles a base dos sistemas normativos corretamente chamados de direito.

A quarta dimensão dos direitos fundamentais[79] implica, pois, não meramente uma melhoria dos fundamentos dos sistemas jurídicos, mas sim uma revisão (BONAVIDES, 2004, p.356-367) de todos os esquemas interpretativos e aplicativos. Esta revisão — ou revolução — de uma hermenêutica em crise (STRECK, 2003), partindo do fundamental, determina uma metamorfose do sistema jurídico como um todo.

5.8 EFEITOS INFORMACIONAIS DA POLÍTICA PARAFISCAL GERANDO RESTRIÇÕES À PRIVACIDADE E À LIBERDADE INFORMACIONAL DO AUTOR DE LOGICAIS

Há dois tipos distorcidos de Estados-Nacionais que estão a emergir nos ‘novos tempos’: o Estado exacerbadamente fraco e o Estado exacerbadamente forte. Nunca a diferença entre Estado[s] dominante[s] e Estado[s] dominado[s] foi tão forte (DUPAS, 2001, p. 37 - 48).

Há indícios de que o primeiro tipo de Estado seria enfraquecido pelo neoliberalismo, e perderia a capacidade de financiamento e de bom aproveitamento da informação *para*-fiscal; o segundo, fortalecido pelo capitalismo, ampliaria grandemente suas capacidades de informação sobre a sociedade, julgamento de indivíduos e aplicação de sanções (DUPAS, 2001, p. 37 - 48).

Em ambos os casos há indícios de impacto sobre a atividade interpretativa das normas que compõem o sistema jurídico. A atividade de interpretação é fundamental para o bom andamento da dinâmica jurídica. Indícios também há de que este impacto vá ser sentido na interpretação das reflexões sobre a interpretação jurídica, ou seja, na hermenêutica jurídica.

Enfim, admitindo-se a proposição (KELSEN, 1998, p. 352 - 353) pela qual se nega a separabilidade entre Estado moderno e Direito moderno em prol do reconhecimento do sistema complexo[80] — fruto da auto-obrigação (KELSEN, 1998,

[79] Sobre a situação dos direitos fundamentais nas infovias ver Cella (2001).
[80] O conceito de complexidade é trabalhado no Capítulo 1 e o conceito de sistema, no Capítulo 3.

p. 345 - 346) do Estado, que assume o ônus de cumprir as normas por ele mesmo postas — a que se chama Estado de Direito.

Não é mais plausível se falar em Estado produzindo direito, mas agora tão somente de uma [auto-][re-]produção do Estado de Direito. Não há, pois, produção de normas, mas reprodução de um ente, o Estado de Direito, cuja informação gênica é, ao menos em parte, a informação jurígena, ou jus-estado-gênica [por falta de melhor expressão].

Os Estados dominantes usam mui habilmente a tributação com fins para-fiscais ou meta-fiscais. Assim, vem novamente à baila a problemática da privacidade (SILVA NETO, 2001). Emerge, diante disto, a necessidade de aprimoramento jus-teórico do conceito de direito à privacidade.

Propõe-se aqui a investigação futura do seguinte caminho teórico para a delimitação do significado do direito à privacidade na sociedade da informação que adira à proposição de Ferraz Júnior (2001), segundo a qual, a liberdade seria uma "autonomia recíproca de acesso à informação": O direito à privacidade deve ser visto como sendo o direito reflexo do direito à informação. Mais uma vez há que se trilhar este caminho em esforço próprio. O direito à privacidade seria, pois, tanto limite ao direito à informação quanto seu fundamento.

5.9 SÓCIOS NA INFORMAÇÃO, O MODELO GNU/GPL

A indústria desempenha um papel de base no entendimento da evolução do capitalismo, do metalismo[81] até a gênese do capitalismo financeiro. Alguns autores adotam o termo Sociedade da Informação para designar o tipo de organização e de organicidade sociais que sucedem à sociedade industrial, que funciona por sobre a estrutura do sistema capitalista. (CASTELLS, 2001, p. 38; 225 – 2; DUPAS, 2001, p. 27 - 35)

Não se deve, contudo, concluir que o capitalismo tenha chegado ao fim. Pelo contrário, o capital revigorou-se, transmutado em *in***forma**ção financeira. Mais ainda: a moeda transformou-se, com o fim do padrão ouro, em *in***forma**ção sobre a saúde financeira de um país ou bloco econômico. Hoje, o *mercado* do capitalismo financeiro depende de um fluxo crescente de *in***forma**ções (CASTELLS, 2001, p.

[81] Este termo refere-se à fase da evolução da economia pré-mercantilista quando o acumulo de metais era reconhecido como forma de constituição da riqueza.

112; 497 - 501) para realizar suas especulações, muitas vezes descritas em termos emocionais.

As relações jurídico-patrimoniais — que, diferentemente das descrições [baseadas em emoções] do comportamento de mercado, ainda são compostas quase que exclusivamente segundo modelos racionalistas — refletem ultraciclicamente (TEUBNER, 1996, p. 158) as alterações das relações econômicas: é o caso dos logicais GNU. (FREE SOFTWARE FOUNDATION, 1991).

O conjunto de logicais que integram o patrimônio intelectual da comunidade GNU — aquela que se submete ao contrato de cessão mútua de direitos de autor GNU/GPL (FREE SOFTWARE FOUNDATION, 1991; DIAMANTAS, 2003) — só pode ser integrado a novos programas por quem consulte a base GNU de conhecimento tecnológico caso o autor da novel obra intelectual se sujeite às regras da comunidade GNU, o que envolve a obrigatoriedade de manter o seu programa aberto e disponível para telecarga (*download*) no sítio da comunidade GNU. Eis o disposto pela Licença GNU:

> GNU GENERAL PUBLIC LICENSE
> Version 2, June 1991
> **1.** You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. [...]. (FREE SOFTWARE FOUNDATION, 1991)

Este é um evento não propriamente de gratuidade, mas do exercício de uma nova modalidade de acúmulo de informação que dispensa a intermediação dos sistemas específicos de informação sobre valor agregado [, ou sistemas monetários], ao que acompanha uma prática de retribuição via concessão obrigatória a toda a comunidade GNU da parcela patrimonial dos direitos intelectuais do autor do programa de computador. Trata-se de um evento de retribuição nos moldes comunitários ou, se calhar, comunistas — e também da concretização do lema *svvm cviqve tribvere*[82].

Note-se que este não é um comunismo para todos, como gostariam os ideólogos socialistas, mas sim um comunismo por adesão [i.e., por meio de

[82] Contribuir cada um com a parte que lhe cabe.

contratos de adesão como a GNU/GPL] que se constitui em um dos processos econômicos em sociedades cujo modelo é o capitalismo financeiro e cujo direito é ainda hegemonicamente patrimonialista.

Demonstrou-se aqui o surgimento dum [info-]comunismo de elite, que usa a infra-estrutura jurídica do Estado capitalista para sustentar seu modelo contratual.

5.10 ESCAPE DOS PRODUTORES DE LOGICAIS GNU DA FORÇA [TRIBUTÁRIA] DO ESTADO PELO ABANDONO DO USO DA MOEDA

Uma vez que não há fluxo financeiro no esquema [de retribuição em termos de *in***forma**ção chamado] GNU/GPL e, considerando que o valor da informação é de difícil precificação, os Estados têm seus poderes tributário e parafiscal efetivamente mitigados pelo esquema de retribuição da comunidade GNU/GPL.

Caberia aos Estados *fiscal*izadores o ônus de avaliar o preço das *in***forma***ções* e de estruturar sistemas tributários que fossem capazes de fazer incidir tributos sobre esta comunidade, cujos membros ao menos possuem computadores capazes de acesso à internet. No Brasil, isto por si é prova de capacidade contributiva (REPÚBLICA..., 2005, Art.145 § 1º). Hoje, os Estados não têm meios tecnológicos adequados para impor tributos a essa elite. O que parece ocorrer é a liberação da esfera de poder dos Estados de uma comunidade determinada a partir da fuga da moeda estatal [como instrumento informacional antes necessário à retribuição econômica].

Os sócios em *in***forma**ção superam em liberdade *eco***nômica** e *in***forma**cional os sócios em capital, pois os primeiros libertam-se da moeda e, conseqüentemente, dos tributos e da parafiscalidade estatais.

Isto se dá porque a grande maioria dos Estados ainda é de Estados-Nacionais capitalistas, que não atingiram o *statvs* de participes efetivos da sociedade da *in***forma**ção (BURNHAM, 2000). Usando o jargão mais simplista, poder-se-ia afirmar que há que se promover uma inclusão digital (SILVEIRA, 2003) dos agentes do Estado.

A solução que parece mais próxima — e que talvez se consolide no silêncio de alguns Estados — é o reconhecimento da possibilidade do uso de logicais livres como contribuição econômica, substituta da tributação tradicional. Isto se dá — como era de se prever — de **forma** tácita.

A conduta de agentes estatais já parece indicar que, no Brasil, este será o caminho escolhido (RIO GRANDE DO SUL, 2002). Uma vez que não há valor monetário estabelecido para as relações econômicas de cooperação envolvendo logicais gratuitos, não é necessário que o Estado abra mão expressamente de competência tributária ou de receita.

Fenômeno jurídico-tributário diverso ocorrerá quando algum Estado-Nacional venha a classificar a prática da gratuidade de logicais como prática comercial abusiva [do tipo *dumping*]. Neste caso o Estado em questão passaria a arrecadar e a fiscalizar as atividades de produção, distribuição e anexação de logicais.[83]

5.11 CONCLUSÕES PARCIAIS

Conclui-se a esta altura do relato da pesquisa que a já realizada demonstração [dos estreitos vínculos históricos, lógicos, metodológicos e epistemológicos entre os conceitos de norma, de forma e de informação] é, *per se*, um fato relevante seja para a ciência da informação, seja para a ciência jurídica, e, sobretudo, para as suas áreas de confluência — dentre as quais convém destacar o direito informático, a informática jurídica e a doutrina dos direitos humanos, devido à enorme importância que presentemente por ela é dada ao direito à informação.

Há, para além disto, muitos outros aspectos relevantes que poderiam ser já levantados da análise aqui apresentada, mas que não poderão ser abordados neste trabalho por limites de forma e de temática. Eles são os seguintes:

a) O Aprofundamento do Estudo da Norma como Unidade Básica da Informação Jurídica;

b) O Aprofundamento Teórico das Conseqüências da Classificação dos Sistemas Jusnormativos como Sistemas Informacionais;

c) O Estudo do Conjunto de Enunciados do Direito Objetivo como Hipertexto;

d) O Estudo das Conseqüências Hermenêuticas de Entender-se que o Conjunto de Enunciados do Direito Objetivo como Hipertexto;

e) As Conseqüências de uma Visão Monista (que não separa direito internacional de direito nacional, nem direito de Estado) Kelseniana para a Concepção Hipertextual do Conjunto de Enunciados do Direito Objetivo;

---

[83] Esta linha de pensamento é hoje defendida nos Estados Unidos da América por setores radicais do partido republicano, mais ligados ao executivo.

f) As Conseqüências da Adoção da Concepção Hipertextual do Conjunto de Enunciados do Direito Objetivo sobre o Leitor de Normas Jurídicas e sobre o Ensino de Informática Jurídica e de Hermenêutica Jurídica;

g) As Implicações Práticas dos Aspectos já Tratados e dos Aqui Elencados sobre A Criação de Sistemas Especialistas em Informática Jurídica;

h) A Questão da Classificação do Direito à Privacidade como Direito Reflexo ao Direito à Informação.

Há que se reconhecer que a contribuição da pesquisa aqui relatada abre mais perguntas do que fornece respostas, isto devido à própria dimensão dos aspectos abordáveis da inter-conceitualidade: norma – forma – informação – normatização – normalização – normatividade – validade – validação – [re]conhecimento - [não [poder]] saber - tecnologia.

6 **BASES CONCEITUAIS: ASSINATURA E DA CRIPTOGRAFIA**

Este capítulo tem por objetivo a exposição das bases conceituais para que o leitor possa acompanhar os passos da pesquisa no sentido de analisar as novas formas de jusvalidação da *in***forma**ção jurídica. Para tanto, levantam-se quais são as características de uma assinatura convencional que a criptografia precisará emular para tornar possíveis as técnicas de assinatura digital.

Para além disto, exploram-se os desafios que residem na necessidade de validar a assinatura de um desconhecido e, por conseguinte as *in***forma**ções que este desconhecido haja validado com sua assinatura. Exploram-se, portanto, os procedimentos tradicionais de reconhecimento de firma.

Somente feito isto, pode-se avançar para buscar compreender a e as bases da criptografia. Isto se faz para principiar a compreensão dos mecanismos de validação e de garantia de integridade *in***forma**cional que, somente mediante a adoção da criptografia, penetraram o mundo dos documentos digitais e das comunicações telemáticas.

6.1 REQUISITOS [JURÍDICOS] PARA A ADOÇÃO DO USO DA CRIPTOGRAFIA NA VALIDAÇÃO DE FLUXOS DE INFORMAÇÃO JURÍDICA NÃO-MILITAR

Na vida civil, costuma-se confiar na integralidade e originalidade de documentos produzidos por terceiros desconhecidos. Para tanto, é necessário que haja uma autoridade juridicamente competente para validar o tal documento.

Daí se pode inferir que o documento, no âmbito de um sistema jurídico, é da emissão de alguém qualificado por um interveniente reconhecido – dotado de autoridade pelo próprio sistema jurídico.

6.2 DEMONSTRAÇÃO DOS REQUISITOS [JURÍDICOS] PARA A ADOÇÃO DO USO DA CRIPTOGRAFIA NA VALIDAÇÃO DE FLUXOS DE *IN*FORMAÇÃO JURÍDICA NÃO-MILITAR

Observe-se os seguintes exemplos hipotéticos que visam a demonstrar como nos sistemas jurídicos as pessoas se identificam [mutuamente]:

Entre cidadãos, i.e., sem hierarquia jurídica:

Dado que em um sistema jurídico qualquer:

Rita, Graça e Jadson sejam cidadãos;

Rita e Graça não se conhecem;

Jadson conhece Rita; e

Jadson [também] conhece Graça.

E que:

O sistema jurídico autoriza Rita a confiar em pessoas que desconheça, contanto que ela tenha um pacto com um conhecido seu [no caso, Jadson], por meio do qual este último se responsabilize em identificar, perante Rita, terceiros que ele [Jadson] conheça.

Considere-se que:

No presente exemplo, Jadson afirmaria contratualmente perante Rita que Graça é quem diz ser, e que a assinatura que Rita apresenta a Graça é mesmo a de Rita;

Analogamente, uma vez que Graça também não conhece Rita, mas somente a Jadson, a identidade de Rita e a validade de sua assinatura pode também ser garantida por Jadson.

Sendo assim:

A garantia de Jadson para Rita pode ser lida da seguinte maneira: "Rita, existe alguém que se chama Graça, e esta assinatura aposta nesse documento é mesmo a de Graça";

Analogamente, a garantia de Jadson para Graça pode ser lida da seguinte maneira: "Graça, existe alguém que se chama Rita, e a assinatura aposta nesse documento é a de Rita".

É graças a fluxos de *in***forma**ção jurídica como o desta demonstração que Graça e Rita podem confiar reciprocamente em suas assinaturas.

Com hierarquia, i.e., sob os auspícios de uma autoridade jurídica:

Imagine-se agora que Jadson não seja um terceiro qualquer, mas uma autoridade estabelecida pelo sistema jurídico: Jadson pode imputar a Rita e a Graça a obrigatoriedade do reconhecimento mútuo de suas assinaturas, uma vez certificadas pela autoridade competente.

Note-se ainda que:

Caso Jadson escreva um documento do qual constem a identificação e a assinatura de Graça terá sido criado um certificado da identidade de Graça garantido por Jadson;

O documento emitido por Jadson para garantir a aceitação da identidade e da assinatura de Graça por terceiros [por Rita, inclusive] é um certificado, e o processo de criação desse documento é chamado de certificação;

O certificado funciona como um documento de identidade para Graça e como documento de identificação de Graça para Jadson.

Processos como estes são bastante freqüentes desde que haja o uso disseminado do papel e da escrita indelével. Eles se tornaram obrigatórios em vários países a partir da disseminação de imprensa[84].

Mas há limitações à eficácia deste sistema:

As legislações de alguns países, como o Canadá, por exemplo, não adotaram documentos de identificação emitidos pelo Estado, como forma de preservar a privacidade (BENYEKHLEF, 1992; 1994) *do indivíduo;*

Os documentos padrão de identificação costumam ter valor somente perante os países que os emitiram.

Para que se identificasse um cidadão de um país perante as autoridades de um outro país foi necessária a criação de um outro tipo de documento, que os vários países do mundo pudessem aceitar. Com muitas dificuldades políticas e justecnológicas pelo caminho [que não interessam à pesquisa em tela], o processo de identificação por um país do cidadão – ou súdito – de um outro país acabou gerando um documento razoavelmente bem padronizado que é o passaporte.

Demonstra-se pelo modelo acima que há um claro estabelecimento de requisitos à certificação da identidade e da assinatura de um indivíduo que em muito precedem a criação da assinatura e da certificação digitais[85].

O que ocorre é que, durante muito tempo, foi matemática e computacionalmente inviável a criação de documentos digitais não-voláteis, ou ao menos pouco voláteis. Isto se deveu ao fato de que a tecnologia da criptografia convencional não era capaz de conferir garantias técnicas de integridade do

[84] Que permitiu a confecção em larga escala de formulários típicos, conformes às normas jurídicas, que instrumentalizaram a produção de documentos de identificação/identidade. Sobre o advento da imprensa e seu reflexo na história do conhecimento ocidental ver Burke (2003).

[85] Sobre assinatura e certificação digital ver: Barreto (2002); Bensoussan; Le Roux (1999); Marcacini (2002); Menke (2005).

documento digital, que permaneceu, até o posterior advento da criptografia assimétrica, equiparável, no que tange à sua volatilidade, aos documentos escritos a lápis.

6.3 INTRODUÇÃO À CRIPTOGRAFIA

Nesta seção, explora-se o processo histórico de formação das bases matemáticas e computacionais para a construção da tecnologia empregada nos processos de assinatura e de certificação digitais. Uma vez que as tecnologias para assinatura e certificação digitais precisaram ser matematicamente desenvolvidas, a pesquisa se debruçou sobre a história da evolução do conhecimento matemático da criptografia neste capítulo. Com isto, demonstrou-se que tal evolução dependeu, ao menos em parte, do investimento realizado por Estados de direito. Sobre o Estado de direito britânico relatou-se o seu interesse em manter sigilosa a evolução do conhecimento matemático sobre criptografia.

Num primeiro momento, a criptografia servia apenas de ferramenta voltada à garantia de sigilo dos comandos militares [respaldados, no caso dos Estados de direito, no sistema jurídico]. Mais tarde, com a criptografia assimétrica disponível para os civis, a assinatura digital se tornaria uma ferramenta de validação da integridade [informacional], bem como da 'originalidade' dos documentos.

Originalidade [relação do documento com o autor] e integridade [da informação no documento] são requisitos para o [re]conhecimento jurídico[86] de sua autenticidade[87].

Fiel ao caráter interdisciplinar da pesquisa, o pesquisador aceita penetrar no universo da matemática, visando a compreender como se forma uma [in]*forma*ção jurídica [e juridicamente validável][88] ante à característica de volatilidade da 'escrita' digital ordinária.

A relevância deste capítulo para o corpo da dissertação provém, portanto, do fato de a criptografia assimétrica possibilitar tecnologicamente uma escrita digital

---

[86] Sobre conhecimento jurídico ver Aftalión; Vilanova (1988).

[87] Que é uma consideração jurídica quanto à validade do documento que repercute sobre a informação que ele expresse validando-a formalmente.

[88] A [in]formação jurídica de expressão digital precisa, portanto, adequar-se às demandas da cultura jurídica sobre as características que um documento [digital] precisa ter para ser validado juridicamente. A [in]formação para ser considerada válida do ponto de vista jurídico precisa, regra geral, estar expressa num documento que não tenha sido [juridicamente] invalidado.

que pode ser sigilosa ou indelével, segundo as necessidades do utente e do sistema jurídico. Para que se compreenda o funcionamento da criptografia assimétrica é necessário antes compreender o funcionamento da criptografia convencional.

Tanto o caráter sigiloso, quanto o caráter indelével de um documento, têm influência sobre a [re]conhecimento jurídico da validade da informação que um tal documento 'contenha'[89].

Do ponto de vista da ciência da informação, é importante explorar este acoplamento entre matemática e direito, pois ele é justamente um provável fator desbloqueador do aprofundamento e da aceleração da 'revolução da informação'[90]. É plausível traçar o seguinte paralelo entre a revolução industrial e a revolução da informação:

A primeira fase da revolução industrial nem foi a mais profunda, nem a mais rápida. Isto se deveu à incapacidade das instituições de dar forma às novas dinâmicas sociais. Foi possível à sociedade empreender uma fase nova e mais profunda da revolução industrial, uma vez que houve uma reforma jurídica e institucional;

A primeira fase da revolução da informação, a atual, não terá sido a mais profunda, nem a mais veloz. Uma vez que o direito – e, com ele, as instituições – se tenha adaptado à nova dinâmica tecnológica das relações sociais, haverá espaço para uma nova fase mais profunda e mais acelerada dos processos sociais que compõem o que se costuma chamar revolução da informação.

Em se aceitando os termos deste paralelo, haverá de se concluir que a sociedade brasileira ainda não entrou propriamente na 'era da informação' (GERMAN, 2000) e que a sociedade ainda não está tão 'organizada em redes' quanto ela poderá estar após uma revolução da cultura jurídico-institucional.

É, portanto, essencial analisar tanto teórica quanto pragmaticamente este acoplamento inter-tecnológico que reúne eletrônica, matemática, computação digital e direito para validar certos fluxos de informação que são essenciais para a 'economia da informação' da 'sociedade em redes' (CASTELLS, 2001, p. 87-172; 2003, p. 56-97; ALMEIDA, 2000).

---

[89] Usa-se a palavra conter por falta de alternativa. Considera-se que a [in]formação é um processo da dinâmica bio-sócio-cognitiva humana, e, portanto não há documento qualquer que possa conter a [in]formação.

[90] Processo a que Burroughs (1994) chama de "revolução electrónica".

O encadeamento lógico das idéias apresentadas na seção é disposto da seguinte maneira: noções gerais de criptografia e de esteganografia; noções gerais criptografia convencional ou simétrica; noções gerais sobre a transição tecnológica da criptografia convencional para a criptografia assimétrica; noções gerais sobre criptografia assimétrica. No capítulo seguinte tratar-se-á da função digestora e assinatura digital; certificação digital e infraestruturas de chaves públicas.

6.4 NOÇÕES GERAIS

Durante a história da humanidade, desenvolveram-se duas formas de se ocultar uma mensagem: a criptografia e a esteganografia, sendo que cada uma dessas modalidades se manifesta por múltiplas técnicas.

Para que o leitor não tenha uma percepção demasiado ampla do objeto de pesquisa – que é a criptografia –, é necessário definir com exatidão o que é criptografia e o que é esteganografia para que não se confundam. Ressalte-se, portanto, que se tratará sobre a esteganografia nas linhas abaixo apenas como expediente elucidativo para o objeto pesquisado.

Tanto a criptografia quanto a esteganografia ocultam a informação. Ocorre que nas técnicas existentes de esteganografia a própria existência da mensagem é dissimulada, seja pela inserção dessa mensagem em outra maior, como, por exemplo, o uso de tinta “invisível”[91]; enquanto na criptografia o que se pretende é tornar ilegível a mensagem para a grande maioria dos leitores em potencial.

6.5 ESTEGANOGRAFIA

Para CUNHA (2005, p. 329), o termo esteganografia significa “escrita em cifra ou caracteres convencionais” e provém do latim moderno *steganographia,* que por sua vez deriva do grego *steganós*, que quer dizer coberto, encoberto.

[91] Substâncias que deixam no papel uma marca que não é imediatamente visível ao ‘olho nu’, necessitando que se coloque o papel contra uma fonte de luz para que a mensagem possa ser visualizada. Na antiguidade, fazia-se um concentrado a partir do limão, que era utilizado com “tinta” para deixar marcas imediatamente invisíveis a ‘olho nu’.
A invisibilidade nunca foi e nem é uma necessidade absoluta. Hoje em dia ocorre a integração – ‘incentivada pelo governo estadunidense’ – de pequeníssimos pontos amarelos em todas as páginas impressas por um grande número de impressoras. O padrão da distribuição desses pontos na página permite, por meio do uso de um código, identificar o número de série da impressora e a data e o horário preciso da impressão do documento (ELECTRONIC..., 2005).

Esteganografia, assim, é toda técnica de dissimulação da existência de mensagens pela alteração de seus suportes físicos (materiais e imateriais).

Na antiguidade, uma simples tatuagem na cabeça raspada de um escravo podia ser utilizada como recurso esteganográfico para transmitir uma informação; bastava para isso aguardar o crescimento do cabelo, que ocultaria a mensagem, e, por conseguinte, a informação.

Outro exemplo clássico é o uso de tiras de papiro enroladas horizontalmente em volta de um cilindro. Uma vez enrolada a tira – até que se cobrisse integralmente a superfície do cilindro – a mensagem deveria ser escrita normalmente em sentido vertical. Depois de realizado o procedimento técnico, as tiras eram desenroladas e armazenadas, e somente quem tivesse conhecimento da existência da mensagem e do diâmetro exato do cilindro utilizado na esteganografia poderia recuperar a informação original.

Por fim, mais modernamente, tem-se a ocultação de textos escritos em fotos ou em mapa de bits – que se traduz pela formação de imagens por meio de arquivos que informam quais dos muitos pontos potencialmente luminosos que compõem o ecrã do computador devem ser ativados.

6.6 CRIPTOGRAFIA X ESTEGANOGRAFIA

Na criptografia, contrariamente ao que se dá na esteganografia, não é dissimulada a existência da mensagem, o que se faz é tornar ilegível o seu conteúdo para a quase totalidade dos potenciais leitores.

A criptografia surgiu, inicialmente, como arte ou técnica de cifrar mensagens. Hoje se entende também por criptografia um ramo da criptologia, que, de seu turno, é o ramo da matemática que se ocupa do estudo da criptografia e criptanálise[92], sendo criptanálise a disciplina matemática – com um alto grau de transdisciplinariedade com a lingüística – que tem como finalidade a remoção da obscuridade gerada pela criptografia, ou seja, a busca por caminhos matemáticos para produzir métodos e meios de decifrar o código sem que se conheça a chave e/ou o algoritmo (MEL; BAKER, 2001, p. 5).

[92] Sobre criptanálise vide Gaines (1956?) e Gardner (1984).

A palavra portuguesa criptografia deriva do francês *cryptographie* e apareceu pela primeira vez em língua vernácula em 1844, grafada da seguinte maneira *cryptographia* (CUNHA 2005, p. 228).

Para Cunha (2005, p. 228; 392), o termo criptografia deriva da junção dos elementos compostos *cript(o)* e *–graf(o).* O primeiro elemento deriva do grego *kryptós,* que significa “escondido, oculto, secreto” e deu origem a muitos vocábulos “[...] introduzidos, a partir do séc. XIX, na linguagem científica internacional [...]”. O elemento composto *–graf(o)* deriva do grego *gráphein*, que significa “escrever, descrever, desenhar”.

“Há indícios de que, na Antiguidade, [a criptografia] foi conhecida no Egito, Mesopotâmia, Índia e China, mas não se sabe bem qual foi sua origem, e pouco se sabe acerca de seu uso nos primórdios da História” (MARCACINI, 2002, p. 10).

O que é certo, do ponto de vista civil, é que até 1976 só havia um tipo de criptografia. Nesse ano, a criptografia de chaves públicas foi inventada por Whitfield Diffie e Martin Hellman (MORENO; PEREIRA; CHIARAMONTE, 2005, p. 37). A partir desta data é que faz sentido classificar a criptografia em duas grandes vertentes de desenvolvimento tecnológico. Assim, diz-se grosso modo que a criptografia está dividida em criptografia convencional – também chamada simétrica – e criptografia de chaves públicas – também chamada assimétrica.

7 **ASSINATURAS: VALIDAÇÃO DA *IN*FORMAÇÃO JURÍDICA**

Este capítulo tem por objetivo demonstrar como a assinatura digital passa a ser adotada como procedimento de validação jurídica da *in***forma**ção. Para cumpri-lo, é necessário descrever como a assinatura, que consiste em um processo de aposição de signo pessoal, foi adotada pelo direito juntamente com a escrita.

7.1 DAS MARCAS PESSOAIS PRIMITIVAS À ASSINATURA CURSIVA

Desde os primórdios da escrita[93], muito antes do surgimento do alfabeto, os seres humanos têm aposto marcas ou sinais próprios nos registros escritos. De primeiro estas os escritos eram artefatos tridimensionais em argila, e as marcas eram feitas sobre os ditos artefatos (BURKE; ORNSTEIN, 1998, p. 61).

Os 'envelopes de argila' nada mais eram que invólucros arredondados e fechados em que os símbolos tridimensionais eram depositados. Para se acessar o conteúdo era necessário quebrar o 'envelope'. Daí porque se optou por gravar a marca dos artefatos tridimensionais correspondentes ao conteúdo pelo lado externo do envelope. Algum dia notou-se que bastava a gravação exterior e, pois, que o conteúdo do envelope era desnecessário (BURKE; ORNSTEIN, 1998, p. 62-63).

Dos envelopes de argila passou-se às tábuas de argila (PIMENTEL, 2000, p.5). Deu-se aí a bidimensionalização da escrita. Note-se que a bidimensionalização da escrita é primordial, melhor dizendo, é uma *conditio sine qua non* para a linearização da escrita e, por conseguinte, da linguagem verbal como um todo.

A linearidade da linguagem verbal implica a linearização do pensamento lingüístico (VYGOTSKY, 1998; CHOMSKY, 1971). Como o direito, a ciência – e, portanto, inequivocamente, a ciência do direito – *per***fazem**-se na e pela linguagem (CASTORIADIS, 2000, p. 259-313), pode-se afirmar que a ciência, o direito e – reitera-se – inequivocamente, a ciência do direito – vêm-se linearizando.

O trabalho metódico de Descartes (19??) é a epítome da linearização e estruturou o método científico. Daí por diante, a padronização da linearidade levou a vislumbrar a existência de não uma, mas de várias linearidades que se entrecruzavam, entrecortavam e entremesclavam. A percepção do entrecruzar, do

[93] Na época em que a escrita ainda era a mera representação de um objeto por um outro menor, tridimensional e artefatual.

entrecortar e do entremesclar a esmo das linearidades levaria à superação do pensamento estruturalista – i.e., das múltiplas linearidades – pelo pensamento sistêmico, que consiste em se notar que na deriva de entrecortes, entrecruzamentos e entremesclas, as estruturas acabavam por se acoplar umas às outras (LUSSATO, 1995, p. 105-116).

Voltando aos primórdios da história[94] da cultura ocidental, a criação fenícia de símbolos imagéticos padronizados que representavam os sons, em vez de representarem objetos, uma vez adaptada pelos gregos, e recebendo símbolos para os sons vogais, fez surgir o alfabeto.

A adoção do alfabeto implicou uma radical diminuição dos símbolos disponíveis. A assinatura continuou, contudo, a depender de símbolos específicos. Estes símbolos específicos se aproximavam cada vez mais dos símbolos-padrão alfabéticos. A escrita cursiva, no entanto, permitia a criação de marcas que, apesar de terem referenciais alfabéticos, podiam ser ainda marcas pessoais.

Houve também o uso de símbolos para um grupo ou comunidade. Ou ainda símbolos de um certo posto hierárquico na sociedade, tal como os relevos dos anéis dos reis que podiam ser passados de soberano a soberano.

7.2 A IMPRENSA CHINESA SOMA-SE AO ALFABETO OCIDENTAL: OS TIPOS MÓVEIS DE GUTENBERG

Presume-se que a milenar arte chinesa de imprimir tenha tido relativamente pouca utilidade *in***forma**cional até o advento da transposição do alfabeto padrão ocidental para o universo da impressão mediante a criação dos tipos móveis. A invenção atribuída a Gutenberg virtualmente eliminava os erros de copistas, o que importava em uma garantia de integridade do texto que até então jamais se vira.

Conquanto a justaposição tecnológica da imprensa chinesa aos tipos móveis de Gutenberg provesse – pela padronização de todas as cópias, sem que o original fosse, do ponto de vista do conteúdo, em nada diferente de seus milhares de cópias – garantia de integridade do texto, bem como, ao menos nos primeiros anos, em que as prensas eram raras, garantia de origem do texto, pouco ou nada se garantia da efetiva autoria dos textos.

---

[94] Ou seja, à época em que tinha início a escrita.

Em geral, para o direito não importa a autoria dos documentos, meramente a sua autoridade. A lei vale não porque o príncipe a cria, mas porque primeiro o príncipe, depois a constituição – que é um soberano virtual, i.e., um processo (LUHMANN, 1985b) no qual se deposita a soberania[95] – validara a sua imposição. A validade de uma lei tem a ver com a origem do comando e não com a sua autoria.

Já para o direito dos contratos e para o direito autoral – no último caso exclusivamente para os países cujos sistemas jurídicos não pertençam à família jurídica européia insular – a autoria é de suma relevância. No primeiro caso porque os contratos, diferentemente das leis, não valem para a generalidade das pessoas, mas sim para uma pequena comunidade de signatários. No segundo, porque o autor deve ser remunerado pelo número de cópias que se imprimam das suas obras.

7.3 A IMPRENSA NO BRASIL: EXCLUSIVIDADE DE ACESSO ÀS PRENSAS COMO FUNDAMENTO DA GARANTIA DE ORIGEM DOS DOCUMENTOS

A assinatura de primeiro não acompanha a revolução da imprensa. Os papéis impressos se multiplicam, padronizam a escrita e são, de início, difíceis de fraudar. A dificuldade de fraudar os documentos impressos decorre da escassez de prensas. Se o documento fosse impresso, poder-se-ia dizer, com uma relativa certeza em que casa de prensa ele tivera sido composto.

Em tempos de Brasil colônia foi muito comum destruírem-se prensas particulares no território colonial, vez que não interessava à metrópole a manutenção de prensas por particulares.

Durante muito tempo a expressão ‘imprensa oficial’ não faria, pois, sentido; todo impresso era régio, i.e., oficial. Não havia imprensa que não a oficial. Os documentos impressos prescindiam, portanto, de assinatura. Nem por isso se deixou de usar os símbolos heráldicos como reforço da originalidade do documento, ante a possibilidade de que tipografias mais simplórias pudessem operar na clandestinidade. A aposição de símbolos heráldicos não deixava de ser uma **forma** de assinatura.

---

[95] O conceito de soberania deriva da virtualização das características de poder do soberano, que dele se separam para dar origem a um conceito jurídico-político. O soberano deixa de ser uma pessoa e passa a ser um conceito que pode, por exemplo, ser exercido por um órgão colegiado. É por isso que Rousseau (1996, p. 7) pode se dizer um ‘cidadão de um Estado livre e membro do soberano’.

Quando da transferência da casa real portuguesa para o que é hoje território brasileiro foi aberta a imprensa régia no Rio de Janeiro. (IMPRENSA..., 2005). O poder do Estado-Nação sempre foi acompanhado da tecnologia de *in***forma**ção que caracterizara a sua emersão: a imprensa. No Brasil, não poderia ter sido diferente.

Retornada a Casa Real Lusitana à porção européia do então 'Reino Unido de Portugal, Brasil e Algarve', restou no território do Brasil uma imprensa oficial estabelecida e um príncipe herdeiro. As estruturas de comando e de *in***forma**ção estavam então prontas para que surgisse em terras brasileiras um Estado [de Direito] Soberano.

Não teria sido possível organizar o exercício do poder imperial no vasto território de maneira centralizada sem que se contasse com a Imprensa Régia, que foi fundamental para a impressão em grande escala dos documentos mais importantes para o funcionamento de um sistema jurídico estatal, i.e., constituição e leis. Por ora os contratos poderiam permanecer manuscritos.

7.4 COPYRIGHT E DIREITO AUTORAL: SITUAÇÕES EXCEPCIONAIS

O direito autoral é uma criação francesa e surgiu – somente após o advento da imprensa – porque em França se percebia como injusta a remuneração exclusiva dos editores por cada cópia, em detrimento dos autores, que até então recebiam apenas um pagamento inicial.

O *copyright*, diferentemente do direito autoral, era um direito que se conferia ao autor sempre que ele concedesse a um editor qualquer o direito de reproduzir-lhe uma obra. No arcaico sistema de *copyright*, hoje abandonado mesmo pelos estadunidenses, o autor não recebia nenhuma remuneração proporcional ao número de impressões de seu trabalho, apenas fazia jus a uma remuneração inicial: o direito de cópia, ou *copyright*.

Não fazendo os temas de direito autoral e de *copyright* parte do objeto da pesquisa esta constatação há de ser o bastante para a presente *démarche*

.

7.5 A IMPORTÂNCIA DAS ASSINATURAS PARA A JUSVALIAÇÃO DAS INFORMAÇÕES JURÍDICAS MEDIANTE ESCRITOS COMUNICANTES DE DECLARAÇÕES PESSOAIS DE VONTADE

Não faz parte do objeto da pesquisa definir o que seja vontade; muito menos o que seja poder. Mas vale definir suas relações com o direito, como sistema *in***forma**cional de controle social.

É de se ressaltar que a própria abordagem sistêmica desconstitui a discrição. Elementos não perfeitamente discretos, i.e., não absolutamente separáveis, não são tão bem definidos seja pela atribuição de fronteiras entre os conceitos, seja pela descrição dos limites [dos campos de validade] que tais fronteiras geram para a aplicação dos conceitos na ciência normal (KUHN, 1997).

Cabe aqui, contudo, estabelecer que, ainda que imprecisos no uso do dia-a-dia, seja do uso do senso comum, seja no da linguagem (WARAT, 1995) da *in***forma**ção juscientífica – mais precisamente justeorética – os conceitos de poder, de controle, de informação, de direito, de vontade e de consentimento se articulam numa rede de intrincadas relações.

O imbricamento é tanto que não se concebe poder sem controle, controle sem poder, controle sem *in***forma**ção, controle sem vontade, direito sem controle da vontade, consentimento sem controle jurídico da vontade, poder político-econômico sem *in***forma**ção jurídica, e assim, sucessivamente.

Nos escritos em que se façam declarações de vontade[96], sejam as unipessoais, que surtem efeitos jurídicos perante o declarante e outrem [que é o caso das declarações testamentárias], sejam as pluripessoais **sinal**agmáticas cujo intercâmbio dá origem aos **contra***tos*[97], a assinatura desempenha um papel maior que a de mero identificador do autor da *in***forma**ção. Nestes casos a assinatura é

---

[96] Leite (2001, p. 73), de seu turno [in]define poder, num contexto juscibernético – i.e., de análise do direito pelo método da cibernética – como sendo parte da própria acepção teórica da ontogênese do direito: "**As teorias jurídicas são** teorias normativas ou **cripto-normativas**, reconhecem o fato do poder e lhe atribuem uma propriedade misteriosa que é sua duração e lhe conferem um ascendente fora da razão. Partem do pressuposto de que o que existe é a crença humana na legitimidade do poder [...]" o poder portanto abrange, para Leite (2001, p. 73), "o elemento vontade". (Sem grifo no original)

[97] Contratos são aqui entendidos como relações jurídicas, i.e., relações normóticas e normativas e **forma**tivas de deveres e direitos, em que ao menos duas partes contraem deveres e, por conseguinte, direitos, uma(s) da(s) outra(s). Os contratos não são, pois, documentos. Para se fazer prova dos contratos é horas dispensável, horas habitual, e horas obrigatório se recorrer à documentação. É freqüente nesses casos que a lei ou o contrato exijam assinatura.

representativa da expressão de vontade ou de consentimento e, portanto, jusvalidante; de resto a assinatura é, nestes casos, jusvalidante também da integridade das *in***forma**ções registradas no documento jurídico.

A *in***forma**ção pela qual se expressa vontade, em alguns casos, e mero consentimento, em outros, é juridicamente interpretada como sendo um elemento de validação jurídica de um engajamento, i.e., da assunção de deveres ou ônus. No caso das relações plurilaterais a assunção de um dever para uma parte gera um direito para as demais.[98] Mas, para que se produzam efeitos jurídicos não basta a *in***forma**ção sobre a assunção de deveres para que direitos se produzam; uma tal *in***forma**ção há que fluir. Sem fluxo de *in***forma**ção jurídica não há a constituição de deveres e, por conseguinte, de direitos para as pessoas, i.e., de deveres subjetivos e direitos subjetivos.

O fluxo da *in***forma**ção jurídica é, pois, elemento basilar do processo ontogenético dos direitos subjetivos. Uma vez que é na constituição de deveres [jurídicos] subjetivos e de direitos [jurídicos] subjetivos que o sistema *in***forma**cional de controle social [que é o direito] se reproduz, pode-se dizer que o elemento básico da ontogênese do direito é a *in***forma**ção jurídica, ao passo que o evento ontogenético básico do direito é o fluxo [juridicamente validado] da *in***forma**ção jurídica.

O fluxo de *in***forma**ção jurídica é, pois, sempre jurígeno[99], i.e., originador, em primeira análise, de direitos [jurídicos] e de deveres [jurídicos] e, em última análise, reprodutor do próprio sistema jurídico, em sua condição de sistema *in***forma**cional de controle social.

Ocorre que, para validar juridicamente os fluxos de *in***forma**ção jurídica, os sistemas jurídicos estabelecem critérios [que podem variar de sistema para sistema] mediante os quais – e para cada finalidade específica – possa ser exigível [ou mesmo proibida] uma determinada **forma** de expressão da *in***forma**ção jurídica. Em alguns casos, nem mesmo uma palavra é necessária: bastam os gestos; em outros, os sistemas estabelecem **formas formais** ou **formas** solenes seja para a documentação, seja para a comunicação, seja para o registro das *in***forma**ções jurídicas.

---

[98] Ou seja, se uma pessoa reconhece que deve cinco reais, uma outra será credora, pois é inconcebível que se deva cinco reais ao *nihil*.

[99] Vide Capítulo 8, item 4.

Muita vez, escritos assinados são juridicamente exigíveis. Não é objeto da pesquisa determinar quais são os eventos em que se exige assinatura no sistema jurídico brasileiro em particular. Basta saber que, como em todos os demais sistemas jurídicos ocidentais, no caso do sistema jurídico-estatal brasileiro, há certas exigências de registro **forma**l e/ou solene de *in***forma**ções jurídicas que demandam a produção e a guarda de documentos escritos e assinados.

8 **CRIPTOGRAFIA CONVENCIONAL OU SIMÉTRICA**

A criptografia convencional é composta de duas classes de técnicas básicas: a transposição (GARDNER, 1972, p. 11-20) e a substituição (GARDNER, 1972, p. 21-33). Há dois tipos de substituição: a cíclica, também chamada de rotação, e a substituição baseada em tabelas aleatórias conveniadas, i.e., compartilhadas.

Alguns povos conheceram primeiro a técnica da substituição por rotação, enquanto outros, a técnica da substituição por tabelas, ou por outro alfabeto, ou ainda a da transposição. Na pesquisa ainda não se conseguiu precisar a razão disso. Pode-se, contudo, especular que a natureza dos sistemas de simbolização – seja pela via da representação dos fonemas, seja pela via da representação das idéias – deve ter influenciado o avanço das técnicas de criptografia e de esteganografia em cada cultura.

Em mandarim, por exemplo, não há alfabeto, e sim símbolos ideográficos: os grafemas não representam fonemas, mas apresentam idéias. Isto torna muito mais difícil a aplicação da técnica da substituição, pelo simples fato de ser extremamente grande a quantidade de símbolos que compõem o sistema gráfico do idioma mandarim, e que, portanto precisariam compor a[s] tabela[s] de substituição.[100]

Para além deste fato, vale salientar que é muito mais difícil para quem trabalha com o ciframento conhecer o número de ordem dos grafemas no conjunto do sistema simbólico do mandarim do que o é para aqueles que trabalham com um alfabeto curto como o latino, o cirílico e o hebraico.

Em termos históricos, existe uma impropriedade em se chamar a criptografia convencional de simétrica. Prova disso é que vários povos que utilizaram a criptografia ‘convencional’ desconheciam a noção de número negativo, fundamental para a construção da idéia de que há duas chaves neste tipo de criptografia, cujos valores matemáticos seriam contrários[101], portanto, simétricos.

---

[100] Note-se que o tamanho das tabelas de substituição depende diretamente da quantidade de símbolos que compõem o sistema de simbolização.

[101] O contrário de um número positivo tem o mesmo valor, mas é negativo. Assim, o contrário de +5 é –5, o contrário de +20 é –20. Não confundir com inverso: o inverso de 2, por exemplo, é ½.

8.1 E O PODER USA CRIPTOGRAFIA: CÆSAR, A CIFRA E O DIREITO ROMANO

Para um melhor entendimento do que acaba de ser exposto, traz-se o seguinte exemplo, baseado no primeiro uso relevante da criptografia com fins claramente jurídicos (MEL; BAKER, 2001, p. 8), que é uma técnica criptográfica simples e rudimentar, conhecida por criptografia de César, porque era usada para comunicação entre Caivs Ivlivs Cæsar, primeiro imperador romano, e seus generais. No exemplo dado, foi utilizada a criptografia de Cæsar com chave[102] três.

É importante salientar que a Roma antiga já contava com a padronização do alfabeto[103] e com o latim, uma língua cuja estrutura gramatical era bastante organizada para a época, no concerne à morfologia e à sintaxe. Os romanos, como os hebreus, usavam o alfabeto para simbolizar tanto fonemas quanto números. Não havia sistema simbólico específico dedicado exclusivamente à matemática. Também não havia o sistema de pontuação, que só foi incorporado ao latim muito depois. O sistema de ciframento de Cæsar podia, portanto, trabalhar com um único sistema de representação padrão, isto é, o alfabeto de vinte e uma letras.

A criptografia de Cæsar utiliza apenas um procedimento criptográfico, denominado de rotação (ou substituição cíclica), que consiste no deslocamento dos caracteres que simbolizam a mensagem em um número “x” de casas[104] num sistema padronizado e ordenado de simbolização, tais quais o alfabeto, os números de 0 a 9, as tabelas alfa-numéricas [de 0 a z] ou as tabelas de caracteres utilizadas pelos atuais equipamentos digitais, como impressoras e computadores.

Quadro 1

MENSAGEM	D	O	M	V	S
ROTAÇÃO I	E	P	N	X	T
ROTAÇÃO II	F	Q	O	Z	V
CIFRA (Rotação III)	G	R	P	A	X

[102] Chave é um número utilizado para cifrar a mensagem.

[103] O alfabeto em Roma sofreu algumas alterações no decorrer do tempo, por exemplo, o U e o J passaram num determinado período histórico a fazer parte do alfabeto (ALMENDRA; FIGUEIREDO, 1977, p. 13-19).

[104] Nesse exemplo “X” é igual a três, por ter sido este o número de rotações escolhido.

No Quadro 1, acima, a palavra DOMVS, que em latim significa lar, é a mensagem[105]. GRPAX é a cifra[106]. E a criptografia utilizada tem chave três, ou seja, é de acordo com o número de rotações que se determina o valor da chave.

Segundo Marcacini (2002, p.[9]) a criptografia pode ser "[...] definida como a arte de escrever em cifra ou em código, de modo a permitir que somente quem conheça o código possa ler a mensagem; essa é uma definição que remonta às suas origens artesanais".

Marcacini se equivoca em sua definição de criptografia, porque "cifra e código" (2002, p.[9]) não "é (sic) maneira de escrever", e sim um resultado de uma operação [matemática] de alteração de texto. Tal alteração de texto gera inacessibilidade de informação, todavia não gera sua perda, já que, em tese, ela pode ser 'transportada'e/ou 'armazenada' tanto em sua expressão comum, quanto em sua expressão cifrada.[107]

Na época de Cæsar, avançavam-se três casas no alfabeto para cifrar, e regridiriam-se três casas no alfabeto para fazer a operação inversa, ou seja, o deciframento. Os matemáticos mais modernos, por trabalharem muito confortavelmente com o conceito matemático de números positivos e negativos, ao invés de dizer que se regridem em três casas, dizem que se avançam três casas negativas.

Esta nova maneira de constituir um caminho explicativo [a dos números negativos] para demonstrar o funcionamento da criptografia convencional permitiu àqueles matemáticos dizer que os sistemas criptográficos convencionais também dependem de um par de chaves.

No exemplo da cifra de Cæsar, são combinados uma seqüência ordenada de procedimentos – chamado, na matemática, de um algoritmo – e uma chave. O método é 'somar', e a chave (quantas vezes fazê-lo) é três (MEL; BAKER, 2001, p. 8-9).

---

[105] O texto no padrão normal da língua convencional.

[106] Texto', a seqüência de grafemas ou caracteres (ALMENDRA; FIGUEIREDO, 1977, p. 13) que é [derivada] da mensagem a partir da aplicação do procedimento criptográfico.

[107] É óbvio que em tese, pois se a forma de transmissão for oral ou relacionada à oralidade (rádio, fonograma, teledifusão vocal, etc) a transmissão do código torna-se muito mais difícil do que da mensagem. No exemplo dado, é muito mais difícil pronunciar GRPAX do que DOMVS, o que também chamaria a atenção dos ouvintes para a idéia de se tratar de um código, o que vai de encontro à finalidade da criptografia, que é de dificultar o mais possível o acesso à informação.

> O algoritmo de criptografia é uma seqüência de procedimento[s] que envolve uma matemática capaz de cifrar e decifrar dados[...] Além do algoritmo, utiliza-se uma chave. A chave na criptografia [...] é um número ou um conjunto de números[...] Para decifrar o texto cifrado, o algoritmo deve ser alimentado com a chave correta, que é única" (MORENO; PEREIRA; CHIARAMONTE, 2005, p.27).

8.2 TRANSIÇÃO: PRECURSORES DA CRIPTOGRAFIA ASSIMÉTRICA NA CRIPTOGRAFIA CONVENCIONAL

Em meados do séc. XIX, o telégrafo trouxe o código Morse bem como outros códigos não secretos para encurtar e baratear as comunicações comerciais.

O ciframento das escritas criptográficas manuais e dos sistemas mistos – ou criptoestenográficos – tornou-se facilmente decodificável com o tempo, cujo maior exemplo é a 'nomenclatura'[108]. Essa facilidade de deciframento gerou uma pressão pela adoção de equipamentos computacionais, primeiramente mecânicos e depois eletromecânicos, para [de]cifrar as mensagens secretas. Os militares precisavam de maneiras seguras de comunicar com rapidez e acuidade as informações secretas de segurança militar. Os militares, no entanto, nem sempre sabiam qual técnica era segura para o ciframento.

Na década de 1860, no contexto da guerra civil estadunidense, o exército confederado confiou seus segredos a um sistema criptográfico que se acreditava seguro, com base numa tabela criada por Vigenére. Acontece que vários criptanalistas conhecidos sabiam da falibilidade do sistema da tabela de Vigenére. De maneira incompreensível, o exército estadunidense continuou a utilizar a tabela de Vigenére até 1914, o que fez com que o exército da União obtivesse vantagens militares da fraqueza deste sistema criptográfico. (MEL; BAKER, 2001, p.47-48)

A esteganografia era muito mais comum que a criptografia na Primeira Guerra Mundial, pois não havia ainda um grande desenvolvimento tecnológico das máquinas [computacionais] de ciframento. Os alemães conheciam a técnica da tinta

---

[108] A nomenclatura é a mescla do uso da criptografia convencional com a esteganografia durante a Renascença para mascarar as comunicações entre Papas, a realeza e os grandes comerciantes. A nomenclatura tem como característica a realização manual de cálculos matemáticos.
No contexto da nomenclatura, código e cifras tinham significados bem diferentes. Cifra era o resultado da operação de ciframento e código tinha um significado bem específico, que era de um símbolo não convencional para representar apenas no contexto da nomenclatura uma pessoa ou uma instituição, i.e., um "P" com a base cortada sinalizava, em alguns sistemas de nomenclatura, o Papa.

‘invisível’, e a utilizavam para destacar em textos de jornais aquelas letras que compunham a mensagem. Os espiões alemães analisavam um jornal “destacado” e assim decifravam a mensagem. (MEL; BAKER, 2001, p.47).

Os E.U.A. também utilizaram a codificação para transmitir informações militares na Primeira Grande Guerra. Os estadunidenses utilizaram as línguas nativas dos índios (Navaho) como código para passar mensagens pelo rádio por serem línguas de difícil compreensão por seus inimigos (japoneses, italianos e alemães) (MEL; BAKER, 2001, p.46).

O uso de códigos desse tipo continua majoritário até a década de 1930, em que a criptografia passa a ganhar terreno em relação aos métodos esteganográficos. Apesar do novo *status* militar conferido à criptografia havia deficiências na gestão de seu uso estratégico. Em 1931, por exemplo, tornou-se disponível a informação de que os estadunidenses detinham conhecimento dos códigos japoneses, por meio da publicação do livro, *The American Black Chamber*, de Herbert Yardley. (MEL; BAKER, 2001, p.46-47).

A reação japonesa foi no sentido de criar uma nova geração mais evoluída de códigos. No final da década de 1930, os japoneses criaram um sistema chamado máquina de escrever alfabética 97, cujo codinome era Roxa, para substituir uma máquina denominada Vermelha. Os japoneses tinham a crença de que a cifra resultante do uso da máquina Roxa era indecifrável pelos inimigos. Mas estavam enganados. Os americanos conseguiram criptanalisar o novo sistema de cifra, utilizando-se do conhecimento que detinham da máquina vermelha, para criar uma máquina análoga à Roxa. Desta feita, tal informação não chegou ao conhecimento dos japoneses[109]. (MEL; BAKER, 2001, p.48).

A versão estadunidense da máquina Roxa era composta por comutadores telefônicos e já se constituía em um pequeno engenho mecânico computacional[110].

---

[109] O que se quer destacar com a narração dessa seqüência de eventos históricos é que a vantagem estratégica militar – que se atinge pelo emprego da criptanálise – é relativa ou parcial, porque não basta saber decifrar a mensagem criptografada do inimigo, mas é fundamental que o seu oponente desconheça essa capacidade de deciframento. Caso o oponente venha a conhecer o sistema criptográfico a ponto de saber [de]cifrar as suas mensagens secretas são três as prováveis conseqüências: 1) o envio de mensagens falsas com o intuito de induzir a erro; 2) o emprego de uma solução de contingência, por meio da alteração mais constante do valor das chaves com o intuito de dificultar o deciframento; e, 3) o desenvolvimento de uma nova geração de sistemas criptográficos.

[110] A história da computação é mais antiga do que a própria história da escrita das palavras. Os primeiros símbolos gráficos foram “símbolos aritméticos, na forma de signos de quantidade” (BURKE; ORNSTEIN, 1999, p.63). O número estava decerto presente nas primeiras mensagens

Resta claro, portanto, que os computadores eletrônicos não foram somente aplicados para realizar cálculos criptográficos, mas sim especialmente desenvolvidos para cálculos, dentre os quais, os de criptografia [e os de balística][111], porque tinham destacada importância na estratégia militar. Em suma: o computador moderno não foi simplesmente **usado** para decifrar, e sim **criado (ou idealizado)** para decifrar as cifras usadas por inimigos.

Os trabalhos de quatro matemáticos americanos foram fundamentais para elevar a criptologia da condição de arte para a de ciência matemática (MEL; BAKER, 2001, p.49). O casal Elisabeth[112] e William[113] Friedman, o prof. Universitário de matemática Lester Hill e o matemático e engenheiro Claude Elwood Shannon.

William Friedman, que decriptara cifras para os E.U.A. antes da Primeira Guerra Mundial, e que, posteriormente, tornara-se desenvolvedor de um programa de treinamento para o governo federal [estadunidense], publicou um ensaio que ligava a criptografia à matemática. O ensaio apresentava a distribuição das letras como uma curva que tinha características que podiam ser estatisticamente[114] quantificadas. Mais tarde, desenvolveu um teste matemático bem definido denominado de teste kappa[115], o que permitiu aplicar os estudos de probabilidade para co-relacionar textos legíveis e suas cifras. Nos anos de 1960, Friedman testemunhou o uso de seu teste kappa para criptanalisar cifras com extrema velocidade em computadores.

Já Elisabeth Friedman trabalhava para o exército estadunidense e também fazia criptanálise para a Marinha e para o Departamento de Estado Estadunidenses.

---

criptografadas. Dada a criação de máquinas eletromecânicas e depois eletrônicas, foi absolutamente natural o seu emprego para a realização de operações matemáticas complexas necessárias à criptografia.

[111] Que não interessam à pesquisa em tela.

[112] Bacharela em inglês, o que equivaleria atualmente a um bacharelado em letras, o que decerto contribuiu para o potencial criptoanalítico do casal, uma vez que grande parte de criptoanálise depende de conhecimentos lingüísticos, i.e., depende do conhecimento das regularidades da língua (MEL; BAKER, 2001, p. 14-15).

[113] Geneticista.

[114] Mais a diante fala-se do equipamento computacional eletrônico Colossus; a importância do trabalho de William Friedman é que ele tornou matematicamente possível relacionar estatisticamente texto aberto a texto cifrado. Esta inovação era a base do funcionamento da Colossus.

[115] A letra kappa no alfabeto grego corresponde à letra K na versão inglesa do alfabeto latino. Em inglês, a letra K se pronuncia ‘KEY’. A palavra ‘KEY’, traduzindo-se para português, significa chave. Logo, o nome dado ao teste kappa faz menção a idéia de chave criptográfica.

Durante a ‘Lei Seca’ nos anos de 1920, ela ajudara a guarda costeira a decifrar mensagens dos contrabandistas[116] de bebidas alcoólicas.

Lester Hill publicou um ensaio que demonstrava como usar equações algébricas em criptografia no ano de 1929. A sua teoria foi fundamental para que outros matemáticos empreendessem estudos sobre a criptografia, dentre eles, Claude Elwood Shannon.

Claude Elwood Shannon usou da sua teoria da informação para descrever em termos matemáticos a criptologia na década de 1940, explicando que as línguas usam muito mais símbolos do que o necessário na transmissão de significados. Este fenômeno é chamado de redundância. Shannon concluiu que, na maioria das cifras, “só a existência de redundância nas mensagens originais torna possível a sua quebra” (MEL; BAKER, 2001, p.50).

Tal análise matemática permitiu que os computadores fossem usados para realizar operações, que antes constituiam um árduo trabalho mental para os criptanalistas.

Paralelamente aos estudos matemáticos da criptologia nos EE.UU., o britânico Alan Turing desenvolveu teses matemáticas, cujas expressões fundamentais foram: 1) um tratado matemático sobre a máquina alemã enigma[117]; 2) a ‘máquina de Turing’ – que não era propriamente uma máquina, porque sua construção era fisicamente impossível, na medida em que dependia de elementos infinitos para funcionar – e constituiu-se em uma ferramenta teórico matemática que possibilitou a criação da Bombe[118] e da Colossus[119], primeiro computador eletrônico.[120]

Os trabalhos existentes nos EE.UU. e Grã-Bretanha confluíram com o advento da Segunda Guerra Mundial, quando estes dois países uniram esforços para enfrentar inimigos comuns.

---

[116] Note-se que os criminosos também fazem uso da criptografia.

[117] Máquina eletromecânica utilizada pelos alemães para cifrar mensagens, inicialmente comerciais e posteriormente militares. (NATIONAL..., 2004). Vide figura 5.

[118] Máquina eletromecânica utilizada para encontrar as chaves que permitiriam decriptar as comunicações alemãs assistidas pela máquina enigma. (CHENERY, 2004). Vide figura 1.

[119] Primeiro computador eletrônico utilizado para decifrar fitas perfuradas frutos da interceptação mediante escuta de rádio das mensagens de teletipo cifradas com as máquinas de cifrar alemãs Enigma. As máquinas preenchiam salas inteiras (BRITISH..., 2004). Vide figura 3,4 e 5.

[120] É comum se apresentar o ENIAC, Electronic Numerical Integrator and Calculator, como primeiro computador eletrônico. É o que faz Pimentel (2000, p. 12). Este equívoco é justificável, pois a maioria das obras que são referência na história da computação se referem ao fato de a existência do ENIAC ter sido pública. A existência do Colossus foi secreta até os anos 1970 (BRITISH..., 2004).

Na base militar britânica de Bletchley Park, formou-se uma equipe multidisciplinar – composta por vários profissionais de diversas áreas, tanto de origem civil quanto militar, destacando-se matemáticos, criptanalistas, bibliotecários, arquivistas, profissionais de telecomunicações, pessoal do serviço secreto e um corpo de suporte. O objetivo daquele laboratório tecnológico militar era desenvolver técnicas de criptanálise para decifrar as cifras da máquina alemã enigma, o que só foi possível com o trabalho multidisciplinar e com o acesso de todos às máquinas capturadas dos alemães pelo exército aliado[121].

[121] Sobre o novo papel das forças armadas na resolução de conflitos na era da *in***forma**ção ver Baquer (2000).

Fig. 1
Máquina Enigma, apreendida dos alemães e usada na base naval britânica de Bletchley Park durante a Segunda Guerra Mundial para decodificar as mensagens alemãs. Este banner é hoje usado na pagina do Centro Nacional de Codificação da Grã-Bretanha (NATIONAL..., 2005)

Fig. 2
Máquina Bombe, usada na base naval britânica de Bletchley Park durante a Segunda Guerra Mundial para determinar o valor numérico das chaves utilizadas pelos alemães para configurar o funcionamento das máquinas de cifrar Enigma. (CHENERY, 2004)

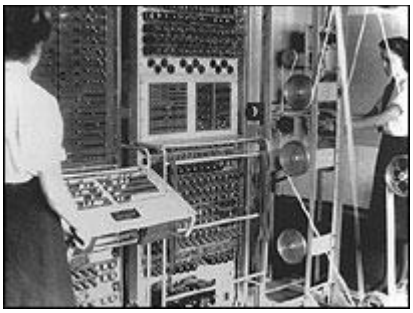

Fig. 3

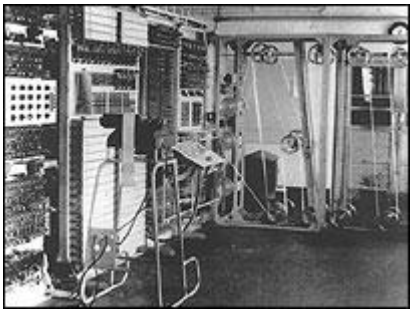

Fig. 4

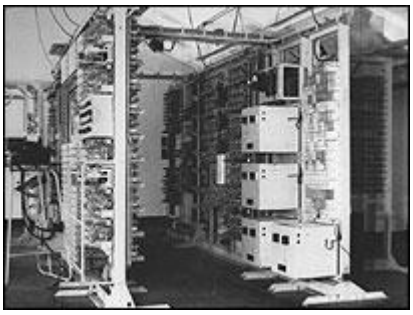

Fig. 5

Figuras 3,4 e 5. Diversos ângulos da máquina Colossus, usada na base naval britânica de Bletchley Park durante a Segunda Guerra Mundial (BRITISH..., 2004).

Um dos procedimentos de deciframento desenvolvidos em Bletchley Park era o *rodding*[122] – primeiro método utilizado para quebrar códigos e decifrar mensagens compostas pela máquina Enigma. Uma vez determinado o valor da chave por meio do *rodding*, configuravam-se os rotores de uma máquina chamada

[122] O Rodding foi desenvolvido com base no Tratado sobre a Enigma de Alan Turing (SALE, 2005) e o vocábulo inglês significa, na língua portuguesa, um castigo físico com um bastão ou vareta (rod), muito usado para disciplinar as crianças na Inglaterra daquela época. A metáfora foi empregada para evidenciar o trabalho de "castigar o texto" com repetidas tentativas matemáticas de decodificação.

Typex[123], e, posteriormente, com o avanço da tecnologia da máquina Enigma, tais chaves eram utilizadas na máquina Colossus.[124]

Para o desenvolvimento desta pesquisa o que interessa é saber que os computadores[125] daquela época ainda não eram programáveis, mas tão-somente grandes máquinas de calcular, o que, no entanto, já foi suficiente para possibilitar incorporação de matemática cada vez mais complexa nos procedimentos criptográficos.

O incremento da capacidade dos equipamentos foi primordial para a adoção da criptografia assimétrica, já que ela requer grande capacidade computacional, sendo que os cálculos de ciframento e de deciframento seriam impossíveis de realizar exclusivamente por humanos.

Com o advento do crescimento continuado da capacidade computacional, deixa de haver somente chaves grupais compartilhadas e passa a haver também chaves individuais e secretas. A adoção de chaves individuais garantiu um certo grau de segurança aos utentes de computador[126]. Cada qual teria uma única chave para realizar as cifras e deciframentos por meio de computadores. A questão era saber como se daria a comunicação, já que ninguém estava disposto a compartilhar a sua chave privativa com os demais, em razão daqueles dois motivos acima já relatados.

Por tudo quanto foi dito, depreende-se que a estrutura computacional necessária para o desenvolvimento da criptografia assimétrica só foi possível devido ao alto investimento financeiro e tecnológico empreendido por Estados de direito.

---

[123] Typex era uma máquina mecânica baseada na versão comercial da máquina enigma alemã dos anos de 1920, utilizada em conjunto com outras máquinas para simular o funcionamento da enigma militar dos anos de 1940.

[124] A máquina Colossus não tinha rotores, já que era uma máquina completamente eletrônica, mas que, para o pleno funcionamento da comutação eletrônica, precisava da informação sobre qual chave utilizar.

[125] Computar significa “contar, calcular, orçar”, enquanto que cômputo significa “contagem, cálculo” (CUNHA, 1986, p. 202).

[126] A escrita digital ordinária é volátil, pois não há diferença entre o documento original e o copiado. Por mais seguro que seja um suporte, sempre será possível se fazer uma cópia digital idêntica ao documento expresso naquele suporte supostamente seguro, bastando para isso que o documento ‘original’seja lido uma única vez. Nesta nova cópia, em tese idêntica à original, pode-se escrever quaisquer alterações que se deseje. Os documentos digitais não gozam, portanto, de qualquer garantia intrínseca de integridade. Essa impossibilidade de determinar a integridade do conteúdo de um documento digital convencional é que o torna indesejável para a grande maioria das comunicações de informação jurídica. A integridade que a pricípio era impossível só veio a ser atribuída ao documento digital com a adoção da assinatura digital.
Sobre a [im]possibilidade da segurança da *in***forma**ção na internet, ver Concernino (2000).

8.3 EFEITOS JUS-[IN]FORMACIONAIS DO USO DA CRIPTOGRAFIA CONVENCIONAL

O emprego da criptografia convencional tem os seguintes efeitos jus-*in***forma**cionais[127]:

a) Sigilo grupal - Só quem conhece a chave e o método pode escrever textos cifrados (cifrar) ou ler textos cifrados (decifrar). Por conseguinte, pode-se presumir que terceiros não deverão ter acesso ao conteúdo da mensagem;

b) Presunção ivris tantvm[128] de pertinência legítima de autor da mensagem ao grupo de pessoas autorizadas a conhecer a chave e o método de ciframento:

Os destinatários da mensagem codificada podem presumir que o autor é alguém legitimamente pertencente ao seu grupo de confiança, na medida em que partilham a mesma chave e o mesmo algoritmo, sendo isso uma conseqüência de acordos ou determinações com valor jurídico. No exemplo dado acima, o fato de o código, ao ser decifrado, produzir uma mensagem legível, indica que o seu autor é proveniente de alguém do grupo de Cæsar, que pode ser o próprio Cæsar ou um de seus generais de confiança.

c) Relegação das mensagens não cifradas à condição [jurídica] de documento cujo valor hierárquico é nulo ou inferior àqueles cifrados:

No caso da cifra de Cæsar é muito claro; quem escreve texto não cifrado não faz parte do grupo de confiança e, portanto, não tem legitimidade para dar ordens ou informações como aqueles que fazem parte do grupo de confiança. Seria o caso de alguém com patente abaixo a de general ou de um general excluído do processo político pelo próprio Cæsar.

Note-se que não há como garantir no nível individual a identidade nem do Autor, nem do destinatário, da mensagem. Do ponto de vista técnico, o emprego da criptografia convencional garante os três efeitos listados acima. Já do ponto de vista jurídico, essas garantias técnicas são acolhidas pelo sistema jurídico brasileiro – desde que não contrariem nenhum dispositivo legal ou princípio moral ou de ordem pública – e servem como meio de produção de prova entre as partes – aqui

---

[127] Por efeitos jus-[in]formacionais se quer significar as alterações na forma da [in]formação jurídica que alteram, do ponto de vista jurídico, a qualidade daquela informação.

[128] Em direito diz-se presunção *ivris tantvm* toda aquela que admite prova em contrário. É a presunção mais comum na produção de provas. Outro tipo de presunção é a *ivre et de ivre*, conseqüência direta de um imperativo do legislador, segundo a qual o que o legislador manda se considerar provado não pode ser desconstituído por nenhuma prova em processo.

entendidas como partes em um contrato de estabelecimento de sigilo. Se, por exemplo, um grupo de pessoas resolver estabelecer uma chave criptográfica convencional e compartilhá-la com vistas a planejar um crime, esta conduta caracteriza a prática do delito de formação de bando ou quadrilha. Não é o fato, portanto, de se criar a chave que constitui um crime, e sim a criação da chave para finalidade delituosa.

8.4 INTERCÂMBIO PÚBLICO DE CHAVES SECRETAS: UM PROGRESSO NA APLICAÇÃO PRÁTICA DA CRIPTOGRAFIA CONVENCIONAL

A partir dos anos 1970, inicia-se uma busca por um padrão criptográfico que pudesse garantir a não-volatilidade [ou, ao menos, um baixo grau de volatilidade] aos documentos digitais. O primeiro passo era garantir a segurança da integridade dos dados gravados em um determinado sistema de computação. Para tanto, passou-se a utilizar uma chave exclusiva e secreta para cada equipamento computacional.

A adoção de uma chave única para cada computador tornaria a comunicação por redes menos segura, não fora a adoção, por cada par de computadores interligados, de uma chave secreta. Para que fosse viável o estabelecimento destas chaves [secretas] compartilhadas por pares de computadores era fundamental que se resolvesse a problemática da entrega a partir do primeiro computador desta chave via rede insegura para o segundo computador que faria parte da relação de comunicação. A informação sobre a chave secreta [compartilhada apenas entre dois sujeitos da relação informacional] não poderia vazar.

O problema da entrega de chave secreta – que já incomodava criptógrafos, governos e reis há milhares de anos (MEL; BAKER, 2001, p. 77) – pode ser enunciado da seguinte maneira: “Como se pode entregar com segurança uma chave secreta a um parceiro confiável usando-se para tanto linhas públicas, e, portanto, inseguras, de comunicação?” (MEL; BAKER, 2001, p. 77)

Trata-se de um problema complicado. Sua solução passa pela resposta à seguinte pergunta: ‘Que vantagem [tecnológica] tem o remetente da chave perante o seu portador que possa ser explorada, no sentido de tornar o portador incapaz de conhecer o valor da chave?’ (MEL; BAKER, 2001, p. 77)

Foi Ralph Merkle o responsável pela solução[129] deste problema. A solução criada por Merkle para o problema do portador não-confiável depende de vários fatores (MEL; BAKER, 2001, p. 77-81):

a) A criação pelo remetente, não de uma única chave para ser secretamente compartilhada, mas sim de (1.000.000) um milhão de chaves;

b) A criação de uma tabela em que para cada chave é atribuído um número de série único e aleatório. A essa tabela chama-se base de dados de pares chave/número de série [da chave];

c) A criação de uma chave secreta para cada par chave/número de série [da chave];

d) A numeração ordenada dos pares que compõem a tabela com os pares chave/número de série [da chave] cifrados individualmente;

e) A seleção pelo destinatário de um único par numerado chave/número de série [da chave];

f) O deciframento no computador do destinatário do par numerado [chave/número de série da chave] selecionado (que demora algo em torno de uma hora);

g) A informação pelo destinatário da chave ao remetente [via portador não confiável] que usará a chave secreta associada ao número serial 553.987 [, mas não diz o número de ordem do par chave/número de série da chave];

h) A seleção pelo remetente da chave secreta apropriada para usá-la como chave secreta compartilhada com o destinatário.

A qualidade da estratégia de Merkle deriva do fato de que, ignorando o número de ordem do par chave/número serial [da chave], o portador estatisticamente teria que decriptar pouco mais de meio milhão de cifras contendo pares chave/número serial [da chave] para topar com o par correto e para, por conseguinte, poder determinar qual fora a chave selecionada pelo destinatário. Pode-se logo dizer estatisticamente que o portador demoraria por volta de 500.000 (meio milhão de) horas, i.e., aproximadamente cinqüenta anos, para determinar a chave secreta compartilhada estabelecida entre remetente e destinatário. (MEL; BAKER, 2001, p. 82-83)

[129] O que só veio a acontecer no princípio da década de 1970. (MEL; BAKER, 2001, p. 77)

Embora a vantagem de tempo de sigilo cinqüenta anos versus uma hora que remetente e destinatário têm em relação ao portador possa *prima facie* parecer elevada, não se levou em conta para esse cálculo uma possível – e até mesmo provável – vantagem computacional que o portador tenha sobre eles. Se o computador do portador for 10.000 vezes mais rápido que o dos compartilhadores de chave secreta, o tempo estimado de solução do problema de Merkle cai de 50 anos para 50 horas. (MEL; BAKER, 2001, p. 83)

Uma vez que a história da criptologia está repleta de eventos em que o avanços tecnológicos anularam vantagens criptográficas, os criptologistas hoje preferem uma vantagem criptográfica da ordem de quinhentos milhões a um, i.e., mais ou menos a relação numérica entre mil anos e um minuto. Exercer tal nível de vantagem criptográfica pelo método de Merkle seria ineficiente em redes telemáticas, devido ao tamanho das tabelas de pares chave/número de série [da chave].

Merkle só conseguiria garantir este grau de vantagem criptográfica a partir de seu trabalho coletivo na Universidade de Stanford com Martin Hellman e Whitfield Diffie. Após dois anos de trabalho incessante com foco em aritmética modular e funções sem retorno, eles desenvolveram a primeira solução pública[130] para o convênio de estabelecimento de chaves: o esquema patenteado Diffie-Hellman-Merkle de acordo de chaves, mais conhecido como Diffie-Hellman, ou DH. Este sistema é utilizado ainda por logicais como o PGP e análogos, tais como o OpenPGP, bem como é extensamente utilizados nos protocolos adotados pelos navegadores de internet, tais como o IPSec e o SSL. (MEL; BAKER, 2001, p. 85)

Mas nada é perfeito, e isto, decerto, inclui o esquema Diffie-Hellman. Há duas fraquezas fundamentais no DH que têm a ver com a sua própria concepção (MEL; BAKER, 2001, p. 85):

1) Inexiste no esquema módulo de autenticação [da identidade] do usuário;

2) Método de intercâmbio de chave secreta não é versátil, é necessário o intercâmbio em linha dos valores DH. Para certas tecnologias de comunicação estáticas, como o correio eletrônico, por exemplo, isto é um sério inconveniente.

[130] Referência à característica do regime jurídico estabelecido para os direitos de uso, alteração e cópia do sistema criptográfico. Em direito autoral classifica-se o sistema Diffie-Hellman-Merkle como um sistema que está no domínio público.

8.5 CRIPTOGRA FIA ASSIMÉTRICA

Por criptografia assimétrica, ou de chave pública se entende toda técnica criptográfica que envolva o uso de uma chave para cifrar as mensagens e outra chave para decifrar o código. Esta é uma classe de técnicas extremamente recente, se comparada com a criptografia convencional.

8.5.1 **Privacidade: direito, sigilo e criptografia assimétrica**

É a criptografia assimétrica que torna possíveis os fluxos privados e sigilosos de informações em espaços de fluxos públicos. Esta possibilidade transforma a relação entre a telemática e o direito.

O ônus de sigilo que, de ordinário, o direito impõe a certas relações *in***forma**cionais deixa de ser inviável de suportar nas redes telemáticas abertas. Além do sigilo, se adequadamente associada à função digestora, a criptografia assimétrica permite a criação de um digesto cifrado da mensagem original que – por ter equivalência funcional com a assinatura cursiva nos documentos em papel – recebe o nome de assinatura digital da mensagem.

O sigilo, e a possibilidade de autenticação individualizada de documento capaz de exprimir concordância, ciência ou verificação das informações documentadas, são as características da tecnologia da criptografia assimétrica que mais interessam ao direito e, portanto à ciência jurídica.

8.5.2 **Validade e validação jurídicas das *in*formações, mediante aplicação da criptografia assimétrica**

Conquanto haja inúmeras análises práticas do processo de acoplamento estrutural inter-tecnológico que reúne eletrônica, matemática, computação digital e direito para validar certos fluxos de informação que são essenciais para a ‘economia da informação’ da ‘sociedade em redes’. (CASTELLS, 2001; 2003), há no mínimo poucos esforços teóricos neste sentido.

Durante a pesquisa não se localizou um só trabalho neste sentido que desça ao nível mais elementar da teoria jurídica, e, a um só tempo, debruce-se sobre a

matemática necessária para constituir um suporte tecnológico à validação [jurídica] dos documentos digitais. Não é outro o objetivo deste item senão o de explorar, de forma que os profissionais da [in]*forma*ção jurídica possam compreender, a matemática necessária para o estabelecimento da assinatura digital.

8.6 SURGE UM NOVO PARADIGMA EM CRIPTOLOGIA [ENTRE OS MILITARES DA GRÃ-BRETANHA E OS CIVIS ESTADUNIDENSES**]**

Em 1969 requisitou-se ao GCHQ[131] que investigasse um problema específico relativo à comunicação militar segura. Sabia-se que a miniaturização dos equipamentos de rádio viria a propiciar que todo soldado estivesse continuamente ao alcance pelo rádio. Mas, ante o paradigma então vigente da criptografia de chaves secretas, seria necessário distribuir chaves para todos os soldados, o que era um problema avassalador.

Este problema foi entregue a James Ellis, um dos mais destacados criptógrafos da Grã-Bretanha que imaginou que poderia se aplicar ruído propositadamente às comunicações. Desde que um ruído fosse adicionado pelo receptor, ao menos em teoria, o próprio receptor poderia subtraí-lo da mensagem recebida – devido ao fato de que o receptor conheceria a fundo as características daquele ruído adicionado.

Ellis, infelizmente, não tinha o ferramental matemático necessário para resolver o problema da remoção do ruído. Foi um novato na GCHQ, que à época pouco sabia de criptografia, mas que acabara de se tornar especialista em teoria dos números pela Universidade de Cambridge, Clifford Cocks que resolveu matematicamente o problema da remoção do ruído, aplicando para tanto um emaranhado de procedimentos que envolviam fatoração e números primos. A solução de Cocks tinha as mesmas características de um sistema civil que em breve seria criado, o RSA[132]. À época o modelo de Cocks não foi implementado, pois faltava capacidade computacional para pô-lo em prática.

Ainda no GCHQ – mas agora em 1974 – Malcolm Williamson, ao tentar provar que Cocks se enganara, acabou descobrindo aquilo que seria em breve

---

[131] General Code Head Quarters, órgão do governo de sua majestade britânica.

[132] Sistema criptográfico assimétrico criado por Rivest, Shamir, Adleman. A sigla RSA faz referência às iniciais dos últimos sobrenomes dos criadores do sistema.

conhecido pelo mundo civil como o intercâmbio de chaves Diffie-Hellman. Em 1975 os militares e os participantes do serviço secreto britânicos já conheciam todos os elementos básicos da criptografia de chave pública, mas tudo era mantido em absoluto sigilo.

O crédito pela criação da criptografia de chave pública foi, então, completamente dispensado aos civis estadunidenses que [re][133]criaram independentemente a criptografia de chave pública.

Além do método DH, Whitfield Diffie, Martin Hellman e Ralph Merkle teriam criado[134] as bases conceituais para a criptografia assimétrica. Visavam a contornar o problema referente à distribuição da chave da criptografia simétrica, que gerara, até então, dois sérios riscos para aqueles que buscavam sigilo:

1) a demora para que se estabeleça o fluxo da informação, porque todas as pessoas da comunidade de confiança precisam primeiramente receber a chave, o que leva tempo;

2) Quanto maior o número de integrantes da comunidade de confiança, mais provável se torna o vazamento do segredo da chave (MORENO; PEREIRA; CHIARAMONTE, 2005, p. 37).

O artigo, datado de 1976, em que Whitfield Diffie discorria sobre o ainda teórico sistema criptográfico assimétrico foi lido por Ronald Rivest, que conseguiu a parceria de Adi Shamir e Leonard Adleman – todos do MIT – para buscar as bases matemáticas para a concretização de um sistema criptográfico assimétrico.

Demonstrou-se no Apêndice 1 como funciona a criptografia ‘assimétrica’, ou seja, como fazer uma chave pública parecer assimétrica a uma chave privada perante quem desconheça o algoritmo, ou a chave privada.

[133] Embora nada soubessem do trabalho britânico.
[134] Foi nisso que se acreditou durante muito tempo, até que o segredo britânico fosse desclassificado e, por conseguinte, revelado ao mundo civil.

9 **ASSINATURA DIGITAL: VALIDAÇÃO DA *IN*FORMAÇÃO JURÍDICA**

Este capítulo como objetivo demonstrar como a assinatura digital passa a ser adotada como procedimento de validação jurídica da *in***forma**ção. Para cumpri-lo, é necessário demonstrar como o direito, em particular o direito da República Federativa do Brasil, passou a reconhecer a técnica chamada de assinatura digital como uma nova **forma** de validar juridicamente as *in***forma**ções.

9.1 CONCEITO DE ASSINATURA DIGITAL

Antes de mais nada, cabe alertar ao leitor que a técnica comumente chamada de assinatura digital não é, nem do ponto de vista formal, nem do ponto de vista essencial, uma assinatura. Pela técnica da assinatura digital não se apõe sinal algum seja à mensagem, seja ao seu suporte, seja ao seu invólucro.

9.1.1 **Assinatura eletrônica não é o mesmo que assinatura digital**

É comum encontrar na literatura uma sinonímia entre os termos ‘assinatura digital’ e assinatura eletrônica’. Isto serve ao objetivo comercial de facilitar a venda dos livros, mas não ao de facilitar a compreensão dos mesmos pelos leitores. Busca-se aqui demonstrar em poucas linhas as enormes diferenças conceituais entre ‘assinatura digital’ e ‘assinatura eletrônica’.

Por assinatura eletrônica entende-se a aposição por meios [parcialmente] eletrônicos de símbolos às mensagens sejam elas ou não eletronicamente transmitidas.

A primeira espécie do gênero assinatura eletrônica é a assinatura eletromecânica. Em geral a assinatura eletromecânica consiste na aposição mecânica movida por eletricidade de símbolos que identifiquem o signatário, seja ele pessoa natural ou pessoa moral. As chancelas eletromecânicas são largamente difundidas no Brasil e são usadas pelo público em geral para autenticação da efetuação de pagamentos de títulos de compensação bancária.

A segunda espécie de assinatura eletrônica é o conjunto ‘nome de usuário’ mais ‘senha’. Este é mais um método de identificação do usuário que propriamente uma assinatura validadora de mensagens. Porém, nada impede que as pessoas

celebrem contratos pelos quais se estabeleça que o conjunto ‘nome de usuário’ mais senha possa ser um elemento validador das *in***forma**ções intercambiadas pelos contratantes.

A terceira espécie de assinatura eletrônica é o conjunto cartão de identificação eletronicamente identificável mais senha [, mais contra-senha]. Este é o sistema de assinatura eletrônica mais conhecido pelos brasileiros. A vasta maioria da população que tem acesso ao sistema bancário[135] se autentica perante as instituições financeiras mediante este tipo de sistema. Os cartões em geral contam com uma banda magnética, que nada mais é que um pedaço de fita magnética. Alguns contam com chips de memória.

A quarta espécie do gênero assinatura eletrônica é o uso de identificação biométrica do signatário. Este tipo de assinatura é aplicado em geral para a mesma finalidade do sistema ‘nome do usuário’ mais senha. Consiste em usar equipamentos [parcialmente] eletrônicos para medir seja as características vocais, faciais e de desenho digital[136], ou mesmo o reconhecimento da palma da mão ou da íris de alguém para controlar, permitindo ou negando, o acesso do identificando a um sistema ou a uma área física, ou a ambos.

9.2 O QUE É UMA ASSINATURA DIGITAL

Não sendo uma técnica de assinatura propriamente dita, a técnica da assinatura digital é chamada de assinatura porque a sua aplicação gera os mesmos efeitos práticos de uma assinatura cursiva [e mais outros que a aposição da assinatura comum é incapaz de produzir]. Esta equivalência de efeitos gerados entre assinatura cursiva e assinatura digital é tecnicamente chamada de equivalência funcional.

Em tese a tecnologia é independente de sistemas eletromecânicos, pois consiste em:

a) aplicar algoritmos[137] matemáticos ao conteúdo [matematicamente valorado[138]] de uma mensagem;

---

[135] Sobre o fluxo telemático de *in***forma**ções financeiras no mercado bancário, ver COSTA (2001).
[136] Refere-se aqui ao desenho da pele do dedo do identificando.
[137] Sobre o conceito de algoritmos, ver Terada; Setzer (1992).
[138] Como já se viu, graças ao trabalho de Claude Elwood Shannon.

b) anexar o resultado das operações matemáticas, i.e., fazê-los circular juntamente com a mensagem, ou apor, i.e., incluir o resultado das operações matemáticas no próprio texto da mensagem.

Isto pode em tese, ao menos ser calculado manualmente, ou com instrumentos que independam de eletricidade. Para, além disto, assim como no caso da assinatura eletromecânica o resultado de uma assinatura digital pode circular em papel. Uma vez que o suporte em papel possa ser conferido, seja, em tese, manualmente, seja, na prática, com o uso de digitalizadores de imagem ou leitores de códigos de barra, a assinatura digital pode ser conferida.

Mas, sem dúvida a maior diferença entre assinatura digital e assinatura eletrônica é justamente o fato de que os processos classificados como sendo processos de assinatura digital geram para cada texto um resultado matemático diverso. Ou seja, para cada documento assinado por um signatário específico, haverá uma assinatura digital distinta.

Isto se justifica, pois a assinatura digital é uma função tanto da chave privada do signatário quanto do texto que se assina. Assim, para cada signatário haverá tantas assinaturas digitais quanto houver textos assinados. É por isto que não se pode dizer que a assinatura digital consista em aposição de signo identificador do signatário. Somente da posse da chave pública de alguém é que se pode verificar se uma assinatura digital é ou não de sua lavra.

9.3 ENTRE DIREITO E MATEMÁTICA: A QUEM PERTENCE ESTA CHAVE? AUTORIDADES CERTIFICADORAS E INFRA-ESTRUTURAS DE CHAVES PÚBLICAS

O grande problema dos sistemas de assinatura digital é a questão do titular da chave. A chave pública corresponde a uma chave privada. Como já se demonstrou, isto é uma propriedade matemática do par de chaves. Mas, como se pode afirmar que um par de números identifica uma pessoa?

Este é um problema sem solução matemática. As soluções para o problema da falta de vinculação entre um par de chaves e uma pessoa natural ou moral são todas jurídicas.

A primeira espécie de solução, e a que sempre acontece primeiro é a solução de direito privado, i.e., a solução contratual. Assim, se dois agentes

*in***forma**cionais concordam em usar os respectivos pares de chave para identificação mútua, eles poderão confiar na autenticidade e na integridade mensagens por eles intercambiadas. É de praxe que o acordo de aceitação recíproca das chaves públicas seja documentado, pois é desse acordo que deriva a validação jurídica das chaves.

Esta espécie de solução não só é útil entre agentes *in***forma**cionais que já se conheciam, mas também, entre aqueles que conheçam alguém em comum e que, com base na confiança naquela terceira pessoa, tenham aceitado mediante contrato, reconhecer todas as chaves validadas por este terceiro de confiança. Isto ocorre conforme o demonstrado no Apêndice. A este terceiro se chama Autoridade Certificadora, pois ele certifica entre si os vários usuários da rede de confiança.

Por fim, várias autoridades certificadoras podem-se organizar mediante acordos de certificação cruzada, ou mediante o estabelecimento de uma autoridade certificadora que sirva somente para certificar as várias autoridades certificadoras. A esta nova meta-autoridade certificadora se convencionou chamar autoridade certificadora raiz, ao passo que, a todo o sistema de múltiplas autoridades certificadoras validadas por uma autoridade certificadora central, se costuma chamar infra-estrutura de chaves públicas, ou simplesmente ICP.

Ocorre que as soluções de direito privado têm uma séria limitação que é o não reconhecimento estatal das assinaturas digitais. As assinaturas digitais serão somente aceitáveis na função jurisdicional, como conteúdo de uma relação contratual, mas não serão aceitas nas relações Estado-cidadão ou Estado-empresa.

A segunda espécie de solução consiste na criação seja por lei[139], seja pela constituição[140] de um sistema público de validação [e de reconhecimento da validade] dos pares de chave da Autoridade Certificadora Raiz de uma Infra-Estrutura de Chaves Públicas. Nele, a validade de todos os pares de chave dependem da validade de um único par de chaves que ocupa o topo de uma longa e articulada pirâmide de validação. A validade do par de chaves de maior valor hierárquico é um problema sem solução matemática que é, pois, resolvido pela

[139] Aqui se faz referência a todo documento que tenha o statvs hierárquico de lei: lei complementar, lei federal ordinária, lei delegada, medida provisória, lei estadual, medida provisória estadual, lei municipal e medida provisória municipal. É claro que o âmbito de validade da lei depende de seu nível de aplicação: uma lei federal ordinária brasileira vale para todo o território nacional, mas não vincula estados e municípios; uma lei complementar vale para todo o território nacional e vincula estados e municípios; uma lei municipal vale só para o território do município.

[140] A constituição pode ser unitária, naqueles países não federados, supra-nacional, como no caso da União Européia, federal, estadual, ou ainda municipal, no caso das leis orgânicas municipais.

interferência do direito, mediante disposição legal ou constitucional, que dispõe que aquela chave ***deve ser***[141] considerada válida.

Assim, a validação de todos os pares de chave abaixo do par máximo é uma validação jusmatemática.

Mas, para que seja possível identificar a que pessoa natural ou moral corresponde um determinado par de chaves é necessário que haja uma atividade de tipo cartorial que consiste na recepção por um agente reconhecido por lei como sendo um agente confiável. Este agente estará vinculado a somente uma autoridade certificadora de uma determinada ICP e será chamado de autoridade de registro ou de autoridade registradora.

9.4 O SISTEMA PÚBLICO BRASILEIRO DE VALIDAÇÃO DAS ASSINATURAS DIGITAIS: A ICP-BRASIL

A ICP-Brasil é um sistema normativo, que visa, nos termos da medida provisória que a criou, “garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras” (REPÚBLICA..., 2001).

A autoridade certificadora raiz da ICP-Brasil é uma função ocupada pelo Instituto Nacional de Tecnologia da Informação, que é uma autarquia vinculada à casa civil da Presidência da República (REPÚBLICA..., 2001).

Além da função de validação dos pares de chaves das demais autoridades certificadoras que compõem a ICP-Brasil, compete à AC-Raiz a tarefa de fiscalizar o cumprimento das normas que compõem o sistema ICP-Brasil, i.e., a Constituição Federal, em particular, a emenda constitucional n° 32, a própria medida provisória 2.200-2, que estabeleceu a ICP-Brasil, os decretos, as resoluções, portarias, instruções normativas do Comitê Gestor da ICP-Brasil e da AC-Raiz.

---

[141] A expressão ‘dever ser’ é aqui usada no sentido que lhe empresta Kelsen (1998), conforme se demonstrou no Capítulo ___ (norma e forma).

10 **CONSIDERAÇÕES CONCLUSIVAS: o fecho é uma abertura radical**

Ao se demonstrar que há uma seqüência de tecnologias usadas para jusvalidar *in***forma**ções jurídicas o trabalho conseguiu traçar o caminho das marcas pessoais à assinatura digital e, com isso, traçou bases para o desenvolvimento de um discurso que já está a permitir a alguns profissionais do direito, da ciência da *in***forma**ção, da *in***formá**tica, da ciência da computação, da matemática, da administração e da educação[142] interagirem proveitosamente ao trabalharem sobre o uso da criptografia e da assinatura digital, no grupo G-CIJ, do Centro Universitário das Faculdades Integradas da Bahia – FIB.

No curso da pesquisa que, ao menos do ponto de vista formal, hora se encerra, formou-se no Centro Universitário da Bahia o G-CIJ, Grupo de Gestão da *In***forma**ção e do Conhecimento Jurídicos. Contando com os docentes Prof. Dr. Benjamin de Almeida, Prof. Gustavo Carias e Prof. Mauro Leonardo Cunha, pela bacharela em direito Renata Botto de Farias, além de discentes oriundos dos cursos de direito, de sistemas de informação e de relações internacionais do próprio centro universitário, muitos já previamente graduados nos mais diversos cursos, o G-CIJ já se debruça por sobre a importância da criptografia e da assinatura digital para a gestão dos processos jurídicos, uma vez que eles não mais corram em suporte papel, o que já começa a ser realidade nalguns casos isolados, ainda que, os recursos se façam sempre usando do tradicional suporte em papel.

Em toda a literatura consultada referente ao tema da criptografia na área jurídica, mesmo se lançando mão da literatura internacional, há sempre um enorme salto da criptografia convencional para a criptografia assimétrica. Tal salto deixa no ar um clima de insegurança entre os estudiosos e os práticos do direito quanto ao domínio dos engenhos de jusvalidação das *in***forma**ções jurídicas e, por conseguinte, do valor probante de tais *in***forma**ções. Durante a dissertação foi possível demonstrar passo a passo o itinerário da evolução da criptografia convencional em direção à criptografia assimétrica. Isto gerou alívio ao pesquisador e a todos os seus leitores-colaboradores que pertencem às profissões jurídicas.

Foi possível, ainda, demonstrar como o direito brasileiro iniciou sua adequação à assinatura digital, pela criação da ICP-Brasil. Para além de tudo isto

---

[142] Ainda falta ao grupo um professional da área da comunicação.

criou-se um conceito para *in***forma**ção jurídica, que não se havia encontrado nem na literatura de ciência jurídica, nem na da ciência da *in***forma**ção um conceito de *in***forma**ção jurídica.

Crê-se a esta altura que o conceito de *in***forma**ção jurídica que se começa a estabelecer poderá servir de base para a consolidação da informática jurídica como ramo da ciência da informação dedicado ao estudo da informação jurídica, bem como auxiliará na interpretação dos direitos à informação, sobre a informação, de informar, de se informar e de ser informado, dos quais são titulares tanto os seres humanos, quanto as organizações.

O fecho deste documento se constitui na consolidação de uma abertura radical para a cooperação para a implantação em larga escala de esquemas jus-*in***forma**cionais de assinatura digital. A abertura radical se deve às possibilidades abertas pela organização de bases para discorrer, falar e a analisar os sistemas criptográficos assimétricos na condição de ferramentas juridicamente reconhecidas de jusvalidação da *in***forma**ção. Já se pode iluminar as bordas do mundo críptico da jusvalidação formal da *in***forma**ção-norma jurídica-jurígena; já se pode caminhar pelas bordas do sumidouro da lógica formal da *in***forma**ção jurídica.

Esta dissertação se encerra, pois, não consolidada, mas sim flexibilizada, como relato duma pesquisa que só buscou o que lhe era plausível: um sucesso duplamente plenamente parcial: parcialmente cogitável e parcialmente incogitável.

REFERÊNCIAS

AFTALIÓN, Enrique R.; VILANOVA, José. **Introduccion al derecho:** conocimiento y conocimiento cientifico; historia de las ideas juridicas; teoria general del derecho; teoria general aplicada. Buenos Aires: Abeledo-Perrot,1988.

ALEXY, Robert. **Teoria da argumentação jurídica**: a teoria do discurso racional como teoria da justificação jurídica. Tradução de Zilda Hutchinson Schild Silva. São Paulo: Landy, 2001.

ALMEIDA, Marcus Elídius Michelli de. Aspectos da crise das empresas da nova economia. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Eds.). **Direito & internet**: aspectos jurídicos relevantes. Bauru: EDIPRO, 2000. Cap. 13, p. 315- 328.

ALVES, Lynn Rosalina Gama; SILVA, Jamile Borges da. **Educação e cibercultura**. Salvador: EDUFBA, 2001.

ANDERY, Maria Amália et al. **Para compreender a ciência**: uma perspectiva histórica. 10. ed. Rio de Janeiro: Espaço e Tempo, 2001.

ARDOINO, Jacques. **Les avatars de l'éducation**. Paris: Presses Universitaires de France, 2000.

ARENO, Márcia Aguiar; ZUFFO, Max. Delitos fiscais: validade da prova obtida em meio eletrônico. In: ROVER, Aires José (Org.). **Direito e informática**. Barueri, SP: Manole, 2004. Cap. 20, p. 413-441.

ASCENSÃO, José de Oliveira. **Direito da internet e da sociedade da informação**. Rio de Janeiro: Forense, 2002.

ASHBY, W. Ross. **Introdução à cibernética**. São Paulo: Perspectiva, 1970.

BABIN, Pierre. **A era da comunicação**. Tradução de Gilberto Vieira. São Paulo: Edições Paulinas, 1989.

BADESCU, Horia. **Stéphane Lupasco**. Tradução de Lúcia Pereira de Souza. São Paulo: Triom, 2001.

BADIOU, Alain. Arte e Filosofia. In: **Por uma nova teoria do sujeito**. Rio de Janeiro: Relume-Dumará, 1994.

BAQUER, Miguel Alonso. El nuevo rol de las Fuerzas Armadas en la resolución de conflictos. In: VIADEL, Antonio Colomer (coord). **El nuevo orden jurídico internacional y la solución de conflictos**. Madrid: Centro de Estudios Políticos y Constitucionales, 2000. Cap. IV, p. 87-96.

BARBAGALO, Erica. **Contratos eletrônicos**: contratos formados por meio de redes de computadores peculiaridades jurídicas da formação do vínculo. São Paulo: Saraiva, 2001.

BARRETTO, Ana Carolina Horta. Assinaturas eletrônicas e certificação. In: ROCHA FILHO, Valdir de Oliveira (Coord.). **Direito e a internet**. Rio de Janeiro: Forense Universitária, 2002. p. 1- 65.

BAUZA REILLY, Marcelo. La informática jurídica como una herramienta de trabajo para el Mercosur. El tratamiento juri-lingüístico de las fuentes de derecho. In: INSTITUTO DE DERECHO INFORMÁTICO. **Derecho Informático**. Montevideo – Uruguay: Fundación de Cultura Universitária, 2001. p. 17-31.

_____. Semblanza de la escuela de informática y derecho de Montpellier. In: INSTITUTO DE DERECHO INFORMÁTICO. **Derecho Informático**. Montevideo – Uruguay: Fundación de Cultura Universitária, 2001a. p. 9-16.

BENSOUSSAN, Alain; LE ROUX, Yves. **Cryptologie et signature électronique**: aspects juridiques. Paris: Hermés Science Publications, 1999.

BENYEKHLEF, Karim. **La protection de la vie dans les échanges internationaux d`informations**. Montreal: Thémis, 1992.

_____. Les transactions dématérialisées sur les voies électroniques: panorama des question juridiques. In: COLLOQUE LES AUTOROUTES ÉLECTRONIQUES, 1994, Montreal. **Actes du colloque les autoroutes électroniques: usages, droit et promesses**. Montreal: Yvon Blais, 1994. p. 115-146.

BERGÉ, Pierre; POMEAU, Yves; DUBOIS-GANCE, Monique. **Dos ritmos ao caos**. Tradução de Roberto Leal Ferreira. 1. reimp. São Paulo: Editora UNESP, 1996.

BIELSA, Rafael A. Método de análisis para una aplicación en informática jurídica documental. **Informática y Derecho**, Buenos Aires, v. 1, p. 41-87, set. 1987.

BITTAR, Eduardo C. B. **Linguagem jurídica**. São Paulo: Saraiva, 2001.

BOBBIO, Norberto. Do poder ao direito e vice-versa. In: CARDIM, Carlos Henrique(Org.). **Bobbio no Brasil**: um retrato intelectual. Brasília: Ed. UNB, 2001. p. 135-152.

_____. Governo dos homens e governo das leis. In: CARDIM, Carlos Henrique(Org.). **Bobbio no Brasil**: um retrato intelectual. Brasília: Ed. UNB, 2001a. p. 115-134.

BONAVIDES, Paulo. **Teoria constitucional da democracia participativa**: por um direito constitucional de luta e resistência; por uma nova hermenêutica; por uma repolitização da legitimidade. 2. ed. São Paulo: Malheiros, 2003.

_____. **Curso de direito constitucional**. 15. ed. atual. São Paulo: Malheiros, 2004.

BORGES, José Souto Maior. **Obrigação tributária**: uma introdução metodológica. São Paulo: Saraiva, 1984.

BOUCAULT, Carlos E. de Abreu; RODRIGUEZ, José Rodrigo (Orgs). **Hermenêutica plural**: possibilidades filosóficas em contextos imperfeitos. São Paulo: Martins Fontes, 2002.

BOURDIEU, Pierre. **Meditações pascalianas**. Tradução de Sergio Miceli. Rio de Janeiro: Bertrand Brasil, 2001.

BURKE, James; ORNSTEIN, Robert. **O presente do fazedor de machados**: os dois gumes da história da cultura humana. Tradução de Jorgensen Junior. Rio de Janeiro: Bertrand Brasil, 1998.

BURKE, Peter. **Uma história social do conhecimento**: de Gutenberg a Diderot. Tradução de Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2003.

BURNHAM, Teresinha Fróes. Sociedade da informação, sociedade do conhecimento, sociedade da aprendizagem: implicações ético-políticas no limiar do século. In: LUBISCO, Nídia M. L.; BRANDÃO, Lídia M.B.(Orgs.) **Informação e informática**. Salvador: EDUFBA, 2000. p. 283-305.

BURROUGHS, William. **A revolução electrónica**. Lisboa: Passagens, 1994.

CANARIS, Claus-Wilhelm. **Pensamento sistemático e conceito de sistema na ciência do direito**. Tradução de A. Menezes Cordeiro. 2. ed. Lisboa: Calouste Gulbekian, 1996.

CARVALHO, Ana Paula Gambogi. **Contratos via internet**. Belo Horizonte: Del Rey, 2001.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Tradução de Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar Ed., 2003.

_____. **A sociedade em rede**. Tradução de Roneide Venâncio Majer. São Paulo: Paz e Terra, 2001.

CASTORIADIS, Cornelius. **A instituição imaginária da sociedade**. Tradução de Guy Reynaud. 5. ed. Rio de Janeiro: Paz e Terra, 2000.

CELLA, Liliana. Derechos de la personalidad en las autopistas de la información. In: INSTITUTO DE DERECHO INFORMÁTICO. **Derecho Informático**. Montevideo – Uruguay: Fundación de Cultura Universitária, 2001. p. 39-46.

CHADUC, Jean-Marc. Environnements ouverts. In: LES AUTOROUTES DE L'INFORMATION: ENJEUX ET DÉFIS, 1995, Montréal. **Actes du colloque les autoroutes de l'information: enjeux et défis**. Montréal: Université de Montréal, 1995. p. 57-60.

CHERRY, Colin. **A comunicação humana**. Tradução de José Paulo Paes. 2. ed. São Paulo: Cultrix, 1974.

CHOMSKY, Noam. **Linguagem e pensamento**. Tradução de Francisco M. Guimarães. Petrópolis, RJ: Vozes, 1971.

CONCERINO, Arthur José. Internet e segurança são compatíveis? In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto. (Eds.). **Direito & internet**: aspectos jurídicos relevantes. Bauru: EDIPRO, 2000. Cap. 4, p. 131- 154.

CORRÊA, Gustavo Testa. A questão da tributação na internet. In: ROVER, Aires José (Org.). **Direito sociedade e informática**: limites e perspectivas da vida digital. Florianópolis: Boiteux, 2000. p. 75- 79.

COSTA, Marcos da. Movimentações financeiras eletrônicas no mercado bancário. In: GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva (Coords.). **Direito e internet**: relações jurídicas na sociedade informatizada. São Paulo: Revista dos Tribunais, 2001. cap. 9, p. 187- 209.

DEL NERO, Patrícia A. Bioinformática e o projeto genoma humano (PGH): os novos desafios para o direito. In: ROVER, Aires José (Org.). **Direito e informática**. Barueri, SP: Manole, 2004. cap. 7, p. 95-108.

CUNHA, Antônio Geraldo da. **Dicionário etimológico**. Rio de Janeiro: Nova Fronteira, 2005.

CUNHA, Mauro Leonardo; BURNHAM, Teresinha Fróes. Ágora e Liberdade: A norma como informação. In: CINFORM-Encontro nacional de ciência da informação, 5. , 2004, Salvador. **Anais [do] V CINFORM – Encontro nacional de ciência da informação.** Salvador: EDUFBA, 2004. Disponível em: <<http://www.cinform.ufba.br/v_anais/artigos/mauroLeonardo.html>>). Acesso em: 18 set. 2004.

DESCARTES, René. **Discurso sobre o método**. Tradução de Márcio Pugliesi e Norberto de Paula Lima. São Paulo: Hemus, [19-?].

DIAMANTAS, Hernant. Parangolé Brasil. SILVEIRA, Sérgio Amadeu da; CASSINO, João (Orgs.). **Software livre e inclusão digital**. São Paulo: Conrad, 2003. Cap. 18, p. 329-339.

DOMINGUES, Ivan. **O grau zero do conhecimento**. São Paulo: Loyola, 1999.

DUPAS, Gilberto. **Ética e poder na sociedade da informação**. 2. ed. rev. e ampl. São Paulo: Ed. UNESP, 2001.

EINSTEIN, Albert. **Relativity**: The special and the general theory. Tradução para inglês de Robert W. Lawson. Avenel, Nova Jersey, EUA: Wings Book, 1961.

ELECTRONIC FRONTEER FOUNDATION. **Is your printer spying on you?**. São Francisco, EE.UU: Electronic Fronteer Foundation, 2005. Disponível em: <<http://www.eff.org/Privacy/printers/>>. Acesso em: 06 dez. 2005.

FERRAZ JUNIOR, Tercio Sampaio. **A ciência do direito**. 2. ed. São Paulo: Atlas, 1980.

_____. A liberdade como autonomia recíproca de acesso à informação. GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva (Coords). **Direito e internet**: relações jurídicas na sociedade informatizada. São Paulo: Revista dos Tribunais, 2001. Cap. 11, p. 241- 247.

_____. **Introdução ao estudo do direito**: técnica, decisão, dominação. 4. ed. São Paulo: Atlas, 2003.

_____. **Teoria da norma jurídica**: ensaio de pragmática da comunicação. Rio de Janeiro: Forense, 2000.

FEYERABEND, Paul. *Contra o método*. Francisco Alves, 3a edição, Rio de Janeiro, 1989.

FOUCAULT, Michel. **A verdade e as formas jurídicas**. Tradução de Roberto Cabral de Melo Machado e Eduardo Jardim Morais. 3. ed. Rio de Janeiro: NAU Editora, 2002.

FREE SOFTWARE FOUNDATION. **GNU general public license**,1991**.** Disponível em: http://www.gnu.org. Acesso em: 18 mar. 2004.

GARCIA, Dinio de Santis. **Introdução à informática jurídica**. São Paulo: Ed. USP, 1976.

GERMAN, Christiano. **O caminho do Brasil rumo à era da informação**. Tradução de Naumann e Marcelo Gross Villanova. São Paulo: Konrad-Adenauer-Stiftung, 2000.

GIDDENS, Anthony. **Mundo em descontrole**. Tradução de Maria Luiza X. de A. Borges. 2. ed. Rio de Janeiro: Record, 2002.

GREENFIELD, Susan A. **O cérebro humano**: uma visita guiada. Tradução de Alexandre Tort. Rio de Janeiro: Rocco, 2000.

GROSSI, Paolo. **Mitologias jurídicas da modernidade**. Tradução de Arno Dal Ri Júnior. Florianópolis: Boiteux, 2004.

GUATTARI, Félix. **Caosmose**: um novo paradigma estético. Tradução de Ana Lúcia de Oliveira e Lúcia Cláudia Leão. São Paulo: Editora 34, 1992.

GUIBOURG, Ricardo A.; ALENDE, Jorge O.; CAMPANELLA, Elena M. **Manual de informática jurídica**. Buenos Aires: Astrea, 1996.

GUIMARÃES, Edgar. **Controle das licitações públicas**. São Paulo: Dialética, 2002.

HABERMAS, Jürgen. **La inclusión del otro**: estudios de teoría política. Barcelona: Paidós, 1999.

HAWKING, Stephen. **A brief history of time**: from the big bang to black holes. Nova York, NY, EUA: Bantam Books, 1990.

_____. **Os gênios da ciência**: **s**obre os ombros de gigantes: as mais importantes idéias e descobertas da física e da astronomia organizadas e comentadas pelo mais famoso físico da atualidade. Tradução de Heloisa B. S. Rocha, Lis Horta Mariconi, Sergio M. Dutra e Marco Mariconi. Rio de Janeiro: Elsevier, 2005.

HOBBES, Thomas. **Leviatã**: ou matéria, forma e poder de um estado eclesiástico e civil. Tradução de Pietro Nassetti. São Paulo: Martin Claret, 2001.

HOBSBAWM, Eric J. **A revolução francesa**. Tradução de Maria Tereza Lopes Teixeira e Marcos Penchel. Rio de Janeiro: Paz e Terra,1996.

IMPRENSA NACIONAL (BRASIL). **Evolução Histórica**. Brasília: Imprensa Nacional, 2005. Disponível em: http://www.in.gov.br/imprensa/jsp/hist.jsp. Acesso em: 05 nov. 2005.

JORGE, Maria Manuel Araújo. **Biologia, informação e conhecimneto**. [Lisboa]: Calouste Gulbenkian, 1995.

KELSEN, Hans. **Teoria pura do direito**. Tradução de João Baptista Machado. 6. ed. São Paulo: Martins Fontes, 1998.

_____. **A democracia**. Tradução de Ivone Catilho Benedetti, Jefferson Luiz Camargo, Marcelo Brandão Cipolla e Vera Barkow. 2. ed. São Paulo: Martins Fontes, 2000.

_____. **A ilusão da justiça.** Tradução de Sérgio Tellaroli. 3. ed. São Paulo: Martins Fontes, 2000a.

_____. **Teoria geral do direito e do estado**. Tradução Luís Carlos Borges. 3. ed. 2. tir. São Paulo: Martins Fontes, 2000b.

KELSEN, Hans. **O estado como integração**: um confronto de princípios. Tradução de Plínio Fernandes Toledo. São Paulo: Martins Fontes, 2003.

KELSEN, Hans; KLUG, Ulrich. **Normas jurídicas e análise lógica**. Tradução de Paulo Bonavides. Rio de Janeiro: Forense, 1984.

KUHN, Thomas. **A estrutura das revoluções científicas**. 5. ed. São Paulo: Perspectiva, 1997.

LANGACKER, Ronald W. **A linguagem e sua estrutura**: alguns conceitos lingüísticos fundamentais. Tradução de Gilda Maria Corrêa de Azevedo. 4. ed. Petrópolis: Vozes, 1980.

LAVIÉ, Humberto Quiroga. **Cibernética y política**. Mendoza: Ediciones Ciudad Argentina, 1986.

LEITE, Flamarion Tavares. **Os nervos do poder**: uma visão cibernética do direito. São Paulo: Max Limonad, 2001.

LESSIG, Lawrence. **Code** and other laws of cyberspace. New York: Basic Books, 1999.

LÉVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. 2. ed. São Paulo: Ed. 34, 2000.

_____. **O que é o virtual?** Tradução de Paulo Neves. 6. reimpr. São Paulo: Ed. 34, 2003.

LORENZ, Edward N. **A essência do caos**. Tradução de Cláudia Bentes David. Brasília: Editora UnB, 1996.

LOSANO, Mario G. La informática jurídica hacia el tercer milenio. In: INSTITUTO DE DERECHO INFORMÁTICO. **Derecho Informático**. Montevideo – Uruguay: Fundación de Cultura Universitária, 2001. p. 81-101.

LUHMANN, Niklas. **Sociologia do direito I**. Tradução de Gustavo Bayer. Rio de Janeiro: Edições Tempo Brasileiro, 1983.

_____. **Poder**. Tradução de Martine Creusot de Rezende Martins. Brasília: Editora Universidade de Brasília, 1985.

_____. **Sociologia do direito II**. Tradução de Gustavo Bayer. Rio de Janeiro: Edições Tempo Brasileiro, 1985a.

LUSSATO, Bruno. **Informação, comunicação e sistemas**. Lisboa: DinaLivro, 1995.
MARCACINI, Augusto Tavares Rosa. **Direito e informática**: uma abordagem jurídica sobre criptografia. Rio de Janeiro: Forense, 2002.

MATTELART, Armand. A era da informação: gênese de uma denominação descontrolada. In: MARTINS, Francisco Menezes; SILVA, Juremi Machado da (Org.). **A genealogia do virtual**: comunicação, cultura e tecnologias do imaginário. Porto Alegre: Salina, 2004. p. 81-107.

MATURANA, Humberto; VARELA, Francisco. **De máquinas y seres vivos**. 3. ed. Santiago: Universitária, 1994.

MATURANA, Humberto. **A ontologia da realidade**. 2. reimpr. Belo Horizonte: Ed. UFMG, 2001.

_____. **Cognição, ciência e vida cotidiana**. 1. reimpr. Belo Horizonte: Ed. UFMG, 2001a.

MAXIMILIANO, Carlos. **Hermenêutica e aplicação do direito**. 9. ed. 3. tir. Rio de Janeiro: Forense, 1984.

MEL, H. X.; BAKER, Doris. **Cryptography decrypted**. 2. reimpr. Boston: Addison-Wesley, 2001.

MENKE, Fabiano. **Assinatura eletrônica:** aspectos jurídicos no direito brasileiro. São Paulo: Revista dos Tribunais, 2005.

MORENO, Edward David; PEREIRA, Fábio Dacênio; CHIARAMONTE, Rodolfo Barros. **Criptografia em software e hardware.** São Paulo: Novatec, 2005.

MORIN, Edgar. **O método 1**: a natureza da natureza. Tradução de Ilana Heineberg. Porto Alegre: Sulina, 2002.

_____. **O método 3**: o conhecimento do conhecimento. Tradução de Juremir Machado da Silva. 2. ed. Porto Alegre: Sulina, 1999.

OST, François. **O tempo e o direito**. Tradução de Maria Fernanda Oliveira. Lisboa: Instituto Piaget, [199-?].

PERELMAN, Chaïm; OLBRECHTS-TYTECA, Lucie. **Tratado da argumentação**: A nova retórica. Tradução de Maria Ermantina Galvão. 5. tir. São Paulo: Martins Fontes, 2002.

PESSIS-PASTERNAK, Guitta. **Do caos à inteligência artificial**: quando os cientistas se interrogam. Tradução de Luiz Paulo Rouanet. 3. reimp. São Paulo: Editora UNESP, 1993.

PIAGET, Jean. Comentarios sobre las observaciones críticas de Vygotsky. In: VYGOTSKY, Lev S. **Pensamiento y lenguaje**: teoria del desarrollo cultural de las funciones psíquicas. Tradução para o espanhol de Maria Margarida Rotger. Buenos Aires: Fausto,1998. (Inclui comentários críticos de Jean Piaget.), p. 199-215.

PIMENTEL, Alexandre Freire. **O direito cibernético**: um enfoque teórico e lógico-aplicativo. Rio de Janeiro: Renovar, 2000.

POPPER, Karl. **A lógica da pesquisa cientifica.** Tradução de Leonidas Hegenberg e Octanny Silveira da Mota. 17. ed. São Paulo: Cultrix, [200-?].

PRIGOGINE, Ilya. **O fim das certezas**: tempo, caos e as leis da natureza. Tradução de Roberto Leal Ferreira. 3. reimpr. São Paulo: Editora da Universidade Estadual Paulista, 1996.

REPÚBLICA FEDERATIVA DO BRASIL. **Constituição** da República Federativa do Brasil, de 05 de outubro de 1988. Atualizada até a emenda constitucional n°48. Brasília: SENADO FEDERAL, 2005. Disponível em:

http://www6.senado.gov.br/con1988_10.08.2005/index.htm. Acesso em: 07 dez 2005.

_____. **Medida Provisória 2.200-2**, de 24 de agosto de 2001. Disponível em: http://legislacao.planalto.gov.br/legislacao.nsf/Viw_Identificacao/mpv2.200-2-2001?OpenDocument. Acesso em: 07 dez. 2005.

RIO GRANDE DO SUL. **Lei nº 11.871**, de 19 de dezembro de 2002. Dispõe sobre a utilização de programas de computador no Estado do Rio Grande do Sul. Disponível em: http://www.al.rs.gov.br/legis<http://www.al.rs.gov.br/legis/M010/M0100099.ASP?Hid_Tipo=TEXTO&Hid_TodasNormas=264&hTexto=&Hid_IDNorma=264. Acesso em: 20 mar. 2004.

ROSENSTOCK-HUESSY, Eugen. **A origem da linguagem**. Tradução de Pedro Sette Câmara, Marcelo de Polli Bezerra, Márcia Xavier de Brito e Maria Inês Panzoldo de Carvalho. Rio de Janeiro: Record, 2002.

ROUSSEAU, Jean Jacques. **O contrato social**. Tradução de Antonio de Pádua Danesi. 3. ed. São Paulo: Martins Fontes, 1996.

RUELLE, David. **Acaso e caos**. Tradução de Roberto Leal Ferreira. 2. ed. São Paulo: Editora da Universidade Estadual Paulista, 1993.

SANTOLIM, César Viterbo Matos. **Formação e eficácia probatória dos contratos por computador**. São Paulo: Saraiva, 1995.

SANTOS, Boaventura de Sousa. Introdução: As Tensões da Modernidade Ocidental. In: _____. **Reconhecer para libertar**: os caminhos do cosmopolitismo cultural. Rio de Janeiro: Civilização Brasileira, 2003.

SAUSSURE, Ferdinand de. **Curso de Lingüística geral**. Tradução de Antônio Chelini, José Paulo Paes e Izidoro Blikstein. 3. ed. São Paulo: Cultrix, 1971.

SCHLEIERMACHER, Friedrich. **Hermenêutica**: Arte e Técnica da interpretação. Tradução de Celso Reni Braida. 3. ed. Petrópolis: Vozes, 2001.

SHIRLEY, Robert Weaver. **Antropologia Jurídica**. Tradução de ?. São Paulo: Saraiva, 1987.

SILVA NETO, Amaro Moraes e. **Privacidade na internet**: um enfoque jurídico. Bauru, SP: EDIPRO, 2001.

SILVEIRA, Sérgio Amadeu da. Inclusão digital, software livre e globalização contra-hegemônica. SILVEIRA, Sérgio Amadeu da; CASSINO, João (Orgs.). **Software livre e inclusão digital**. São Paulo: Conrad, 2003. Cap. 1, p. 17-46.

STRECK, Lenio Luiz. **Hermenêutica jurídica e(m) crise**: uma exploração hermenêutica da construção do Direito. 4. ed. rev. atual. Porto Alegre: Livraria do Advogado, 2003.

TEIXEIRA, João de Fernandes. **Mentes e Máquinas**: uma introdução à ciência cognitiva. Porto Alegre: Artes Médicas, 1998.

TERADA, Routo; SETZER, Valdemar W. **Introdução à computação e à construção de algoritmos**. São Paulo: Makron Books, 1992.

TEUBNER, Gunther. **Droit et réflexivité**: l'auto-référence en droit et dans l'organisation. Paris: LGDJ–Bruyland, 1996.

TRUDEL, Pierre et. al. **Droit du cyberespace**. Montreal: Thémis, 1997.

TUCCI, José Rogério Cruz e. Eficácia probatória dos contratos celebrados pela internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Eds.). **Direito & internet**: aspectos jurídicos relevantes. Bauru: EDIPRO, 2000. cap. 10, p. 273- 281.

VARELA, Francisco J.; THOMPSON, Evan; ROSCH, Eleanor. **A mente incorporada**: ciências cognitivas e experiências humanas. Tradução de Maria Rita Secco Hofmeister. Porto Alegre: Artmed, 2003.

VYGOTSKY, Lev S. **Pensamiento y lenguaje**: teoria del desarrollo cultural de las funciones psíquicas. Tradução para o espanhol de Maria Margarida Rotger. Buenos Aires: Fausto,1998. (Inclui comentários críticos de Jean Piaget.)

WARAT, Luis Alberto. **O direito e sua linguagem**. 2. ed. Porto Alegre: Sergio Antonio Fabris, 1995.

WIENER, Norbert. **Cibernética**.: ou contrôle e comunicação no animal e na máquina. São Paulo: Polígono e Universidade de São Paulo, 1970.

_____. **Cibernética e Sociedade**. São Paulo: Cultrix, 1984.

YURCIK, William; TAN, Zixiang. The Great (Fire)wall of China. In: TPRC'96, 24, 1996, Vienna, VA, Estados Unidos da América. **TPRC Programs and Papers Archive.** Disponível em: <<http://www.tprc.org/abstracts/tan.txt>> Acesso em: 20 mar. 2004.

APÊNDICE – Usando a matemática para demonstrar didaticamente a *forma*ção das ferramentas de validação jurídica da in*forma*ção

A ligação entre matemática e informação foi extensamente demonstrada por Claude Elwood Shannon (1949). Neste tópico visa-se a explicar que uma evolução [matemática] da criptologia alterou a forma da [in]*forma*ção digitalmente [tele]comunicada. Mais a diante, demonstrar-se-á que esta mudança na forma é [do ponto de vista jurídico] uma mudança qualitativa, e que esta mudança jus-qualitativa da forma da [in]*forma*ção tem o potencial de ampliar a propensão a fluir da [in]*forma*ção.

Vale lembrar que criptografia assimétrica é toda aquela em que a chave usada para decifrar o código seja diferente daquela utilizada para cifrar a mensagem.

Mantendo-se em mente que cada chave criptográfica é um número, torna-se difícil [para aqueles que não tenham uma formação – ou, ao menos, uma inclinação – matemática] imaginar como uma operação pode ser realizada com um número e revertida com outro [aparentemente] independente. Um tal conceito desafia o senso comum. Mas, é bom lembrar: ele só é útil porque está baseado num uso da matemática que vai além do senso comum.

Ao senso comum dizer que uma operação de divisão tem dois resultados parece ser irrazoável. Mas, de fato, a operação de divisão tem dois resultados: o quociente e o resto. Esta asserção está na base do tipo específico de matemática usado para implementar a criptografia assimétrica: a matemática modular. É justamente a matemática modular que torna possível a criptografia assimétrica e, por conseguinte, a assinatura e a certificação digital.

1 – Inversos: um exemplo simples de chaves aparentemente assimétricas

Um exemplo bastante simples de como duas chaves aparentemente assimétricas é o seguinte:

Chave privada: 0,125
Chave pública: 8

Pode parecer que as chaves são completamente independentes. Porém:

0,125= 1/8

Ou seja, a assimetria é apenas aparente. 0,125 é o inverso de 8.

As chaves que compõem o par de chaves do exemplo acima podem ser facilmente ligadas. É por isto mesmo que a única utilidade do par de chaves do exemplo é a de ferramenta didática. O problema matemático que liga uma chave do par à outra é demasiado simples. Este par de chaves então é inútil do ponto de vista da segurança da informação.

2 – Nem tão longe assim do senso comum: níveis diversos de complexidade matemática

Há, para alívio dos usuários da criptografia assimétrica, problemas matemáticos com dois caminhos diferentes de solução: um relativamente simples, e outro extremamente mais complexo que o primeiro. É este tipo de problema que torna possível a existência de uma criptografia cujo funcionamento dependa de duas chaves diversas. É muito mais fácil [sem usar calculadora] multiplicar 9832x9832 que calcular a raiz quadrada do resultado[143]. |

A segurança de um sistema criptográfico assimétrico depende de o problema para determinar a chave pública a partir da chave privada ser muito mais difícil de se resolver que o problema inverso.

[143] O resultado da multiplicação acima é 96668224

3– Matemática modular

À complexidade matemática do problema há que se agregar a lógica da matemática modular, mais especificamente, a propriedade de números que sejam um o inverso modular do outro.

A escolha dos inversos modulares se baseia no fato de que eles são muito mais difíceis de se encontrar [calcular], que os inversos comuns [os multiplicativos].

A noção de inverso modular é a pedra fundamental da criptografia assimétrica. Mas, para que se possa entendê-la, é importante entender alguns conceitos básicos de matemática modular: o de divisão modular e o de multiplicação modular.

4 – Divisão modular

Há dois resultados de uma divisão. Na matemática do dia-a-dia, seleciona-se comumente o quociente. Em matemática modular, o resultado de uma operação de divisão que interessa é o resto, e não o quociente. Mas não é um valor qualquer de resto: os números negativos não são aceitos. Assim, em matemática modular, o resultado de 14 ÷ 5 é 4, ou seja, o resto. E, ainda, o resultado de (-14) ÷ 5 também é 4, ou melhor:

14 mod 5 = 4
e
(-14) mod 5 = 4

5 – Multiplicação modular

Na multiplicação modular o resultado é limitado pelo valor do módulo, assim:

(4x4) mod 10 = 6
Já que
16 mod 10 =6
e
(3x7) mod 10 = 1
Já que
21 mod 10 = 1

6 – Inversos modulares

Um par de números cujo resultado da multiplicação modular do primeiro pelo segundo tenha resultado igual a 1 é composto por números que são denominados inversos modulares. Uma vez que no exemplo acima usou-se a multiplicação (3x7) mod 10, pode-se dizer que, no módulo 10, 3 e 7 são inversos. Num sistema criptográfico assimétrico hipotético cujo módulo fosse 10, poder-se-ia usar 3 como valor da chave privada. Sendo assim, 7 seria a chave pública.

Note-se que é muito mais fácil resolver o problema a seguir:

(3x7) mod 10 = ?

Do que resolver o problema abaixo:
(7x?) mod 10 =1

Mas, ainda é demasiado fácil determinar o valor da incógnita, pois ela será um valor entre 0 e 9. Já que o módulo 10 limita os números a este intervalo. (MEL; BAKER, 2001, p. 108)

É claro que o módulo 10 é um exemplo cuja utilidade é tão somente didática. O algoritmo RSA, comumente empregado em logicais de criptografia, usa módulos cujo comprimento excede 200 dígitos. (MEL; BAKER, 2001, p. 108)

Num sistema criptográfico assimétrico é necessário usar um módulo de valor mais elevado. Pelo menos para fins didáticos, não é necessário um módulo cujo valor seja um googol[144].

Didaticamente é bastante usar o módulo 101, [145] que já possibilita a demonstração não assistida por computador da diferença da complexidade entre os dois caminhos de resolução de problemas e a aparente desconexão lógico-matemática entre o valor da chave privada e seu inverso no módulo 101, ou seja, o valor da chave pública.

[144] 10^{100}, ou seja um doxigentilhão. (ROWLETT, 2005)
[145] O uso por MEL; BAKER (2001, p. 108) do módulo 101 é, além de matematicamente interessante, sugestivo do ponto de vista pedagógico. É comum usar o número 101 para significar ‘one on one’, o que quer dizer algo parecido com olho no olho.

7 – Cálculos didáticos: aprendendo com o módulo 101:

Se, de um lado, é verdade que, do ponto de vista da aplicação prática da criptografia para gerar sigilo ou assinaturas digitais, o módulo 101 é inútil, pois com o poder computacional de que se dispõe hoje, é relativamente fácil resolver este problema, por outro lado, a sua utilidade didática é inegável: com o módulo 101 é possível demonstrar de uma maneira compreensível para um largo número de pessoas como é possível se trabalhar com criptografia assimétrica para garantir sigilo da informação.

No exemplo a seguir demonstra-se, mediante o uso do módulo 101, que há uma enorme diferença de grau de dificuldade dos procedimentos matemáticos necessários para se quebrar o sigilo da comunicação, com emprego da criptografia assimétrica, dos nomes de cidades selecionadas numa lista comparativamente com o que aconteceria se se tivesse optado por usar criptografia convencional.

Segue-se ao exemplo didático propriamente dito:

Um par de números muito interessante do ponto de vista didático é constituído por 22 e 23. Estes números são inversos no módulo 101. Ou seja:

$22x23 \bmod 101 = 1$

Daí decorre que, para um número ‘y’ qualquer:

$(22x23)y \bmod 101 = y$

“O importante é notar que $22x23 \bmod 101$ funciona como uma identidade multiplicativa” (MEL; BAKER, 2001, p. 109), como $23x23=506$, pode-se dizer que sempre que multiplicar qualquer número por 506 e dividir o resultado por 101, o resto da divisão, i.e., o resultado da divisão modular, será sempre o número original.

Assim:

Quadro 2

Núm	x	Mod
3	1.51	3
5	2.53	5
10	5.06	10
20	10.1 20	20

Atenção:

O resultado relevante da divisão modular é o resto da divisão, não o quociente. São os valores dos restos que aparecem na coluna da direita.

8 – Seqüência de números super-incremental

Há um tipo de seqüência de números que possui uma propriedade extremamente conveniente para a transmissão de dados econômica e dotada de um [pequeno] grau de sigilo. Mas que, somada à aplicação dos inversos modulares, será de grande utilidade para a geração de chaves em criptografia assimétrica.

Trata-se das seqüências numéricas super-incrementais. Uma seqüência super-incremental de números inteiros pode ser preparada da seguinte maneira[146]:

Eleja-se um número inteiro qualquer maior que zero;

O próximo número terá de ser o primeiro inteiro maior do que o dobro deste primeiro número;

O número seguinte será o primeiro inteiro maior que a soma de todos os números anteriores;

O número subseqüente, de forma idêntica, será o próximo primeiro inteiro maior que a soma de todos os números que o antecedam na seqüência, e assim, sucessivamente.

[146] Estas informações implícitas na fonte se depreendem de uma leitura atenta do texto de Mel; Baker (2001, p. 99)

Um exemplo de seqüência numérica super-incremental está disponível a baixo:

1
3 = 2+1
5 = (3+1) +1
10 = (5+3+1) +1
20 = (10+5+3+1) +1
40 = (20+10+5+3+1) +1

A propriedade matemática das seqüências numéricas super-incrementais que importa à criptografia assimétrica se demonstra no exemplo a seguir:

Se, conforme o quadro a seguir, um único município for associado a cada número de uma seqüência numérica super-incremental, o resultado de qualquer soma de quaisquer valores dos números da seqüência identificará com precisão um grupo de municípios selecionados. Pode-se ainda expressar a mesma idéia de outra forma: a seleção de um conjunto qualquer de municípios nesta tabela pode ser comunicada transmitindo-se somente ao receptor o valor da soma dos índices, i.e., dos números que estão vinculados aos municípios.

Quadro 3

1	Recife
3	Parry Sound
5	Montreal
10	Salvador
20	Itamaracá
40	Olinda
80	Jaboatão
160	Lauro de Freitas

Demonstração[147]:

a) Se o autor comunicar ao leitor tão somente o número 29, ainda assim, o leitor será capaz de identificar quais foram os municípios selecionados;

b) Se o autor comunicar ao leitor tão somente o número 33, ainda assim, o leitor será capaz de identificar quais foram os municípios selecionados;

c) Se o autor comunicar ao leitor tão somente o número 73, ainda assim, o leitor será capaz de identificar quais foram os municípios selecionados;

d) Se o autor comunicar ao leitor tão somente o número 10, ainda assim, o leitor será capaz de identificar quais foram os municípios selecionados;

e) Se o autor comunicar ao leitor tão somente o número 185, ainda assim, o leitor será capaz de identificar quais foram os municípios selecionados;

Para resolver problemas como este, deve-se proceder da seguinte forma: usar o número indicado no exercício e percorrer a tabela de números super-incrementais do valor mais alto para o mais baixo efetuando subtrações entre o número indicado em cada alínea do exercício e o número da tabela que lhe seja imediatamente inferior. Caso o valor da diferença não esteja contido na tabela, a solução será o número da tabela usado como subtraendo; caso o valor da diferença se encontre na tabela, a solução será a diferença.

Para o número 73:
73 - 40 = 33
33 - 20 = 13
13 - 10 = 3

Assim, conclui-se que as cidades selecionadas foram aquelas cujos índices são 40, 20, 10 e 3, i.e., Olinda, Itamaracá, Salvador e Parry Sound.

Mas, dado que, para este sistema de comunicação sucinta de informação funcionar, é necessário que haja compartilhamento da tabela, se este se der pela colaboração de um portador indigno de confiança, então, não há garantias do sigilo quanto a que municípios teriam sido selecionados para serem visitados pelo autor no

[147] Resultados da demonstração: a) Itamaracá, Montreal, Parry Sound e Recife; b)Itamaracá, Salvador e Parry Sound; c) Olinda, Itamaracá, Salvador e Parry Sound; d) Salvador; e) Lauro de Freitas, Itamaracá e Montreal.

próximo ano. O encontro entre autor e leitor poderá, portanto, ser objeto de escuta por parte de um portador bisbilhoteiro.

9 – Geração de chaves públicas a partir de chaves privadas usando inversos modulares

Voltando para o exemplar modulo 101, pode-se demonstrar como é possível gerar chaves públicas procedendo-se da seguinte maneira:

- Existindo uma chave privada, cujo valor seja igual a um número que faça parte de uma seqüência super-incremental;
- Multiplicando-se o valor numérico da chave privada pelo valor do número mais alto dentre um par de números que sejam, no módulo 101, inversos entre si.

Um dos procedimentos de deciframento desenvolvidos em Bletchley Park era o *rodding*[148] – primeiro método utilizado para quebrar códigos e decifrar mensagens compostas pela máquina Enigma. Uma vez determinado o valor da chave por meio do *rodding*, configuravam-se os rotores de uma máquina chamada Typex[149], e, posteriormente, com o avanço da tecnologia da máquina Enigma, tais chaves eram utilizadas na máquina Colossus.[150]

Daí, no módulo 101, usando-se o par de inversos 22 e 23, pode-se gerar a chave privada da seguinte maneira:

---

[148] O Rodding foi desenvolvido com base no Tratado sobre a Enigma de Alan Turing (SALE, 2005) e o vocábulo inglês significa castigo físico com uma vareta na língua portuguesa, muito usado para disciplinar as crianças na Inglaterra daquela época. A metáfora foi empregada para evidenciar o trabalho de "castigar o texto" com repetidas tentativas matemáticas de decodificação.

[149] Typex era uma máquina mecânica baseada na versão comercial da máquina enigma alemã dos anos de 1920, utilizada em conjunto com outras máquinas para simular o funcionamento da enigma militar dos anos de 1940.

[150] A máquina Colossus não tinha rotores, já que era uma máquina completamente eletrônica, mas que, para o pleno funcionamento da comutação eletrônica, precisava da informação sobre qual chave utilizar.

Quadro 4

Chave Privada	x 23 x 22	Mod 101
1	506	1
3	1518	3
5	2530	5
10	5060	10
20	10120	20
40	20240	40
80	40480	80
160	80960	59

E assim, sucessivamente.

10 – Exemplo de ciframento 'assimétrico':

Quadro 5

Chave Privada (Números mantidos em sigilo) * Coluna cujos valores devem ser desconhecidos pelo portador e pelo receptor da chave pública	Mensagem	X 23	Chave Pública (Números amplamente divulgados)* Selecione daqui os números que identificam os municípios e some-os para indicar a seleção
1	Recife	23	23
3	Parry Sound	69	69
5	Montreal	115	14
10	Salvador	230	28
20	Itamaracá	460	56
40	Olinda	920	11
80	Jaboatão	1840	22
160	Lauro de Freitas	3680	44

Demonstração: Enviando seguinte quadro de *in***forma**ções para um confidente.

Quadro 6

Recife	23
Parry Sound	69
Montreal	14
Salvador	28
Itamaracá	56
Olinda	11
Jaboatão	22
Lauro de Freitas	44

Basta pedir que um confidente some o valor dos municípios selecionados. Pede-se então a um terceiro que ele indique quais foram os municípios selecionados por seu confidente. Note que se tornou muito mais difícil identificar os municípios selecionados.

Para quem sabe que o par de números inversos no modulo 101 que foi utilizado foi 22 e 23, há um procedimento matemático simples e determinístico que garante a solução do problema. Eis como funciona. Suponha-se que o valor da soma seja 65:

65 x 22 = 1430 Lembrete: 22 é o inverso de 23 no módulo 101

1430 mod 101 = 16

16 é, então, o valor a ser encontrado diante da tabela de chaves privadas

16 - 10 = 6

6 - 5 = 1

Quadro 7

Chave Privada (Números mantidos em sigilo) * Coluna cujos valores devem ser desconhecidos pelo portador e pelo receptor da chave pública	Mensagem
1	Recife
3	Parry Sound
5	Montreal
10	Salvador
20	Itamaracá
40	Olinda
80	Jaboatão
160	Lauro de Freitas

As cidades selecionadas foram, conforme tabela original, as seguintes: Salvador, Montreal e Recife.

Note-se que para quem desconheça:

a) o módulo utilizado, i.e., mod 101;

b) o par de inversos no módulo escolhido, i.e., 22 e 23; e

c) as chaves privadas, i.e., 1, 3, 5, 10, 20, 40, 80, 160.

Mas conheça apenas a relação chaves públicas / mensagens, a seguir:

Quadro 8

Mensagem	Chave Pública (Números amplamente divulgados)* Selecione daqui os números que identificam os municípios e some-os para indicar a seleção
Recife	23
Parry Sound	69
Montreal	14
Salvador	28
Itamaracá	56
Olinda	11
Jaboatão	22
Lauro de Freitas	44

Será bastante mais difícil descobrir as cidades selecionadas que para quem conheça a chave privada, o inverso 22 e o módulo 101.

.

ANEXO – Medida Provisória n°. 2.200-2, de 24 de Agosto de 2001

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO 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.

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

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

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

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.

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.

Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 7º Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

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

Art. 9º É vedado a qualquer AC certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

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

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

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

Art. 11. A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.

Art. 12. Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal.

Art. 13. O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.

Art. 14. No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei.

Art. 15. Integrarão a estrutura básica do ITI uma Presidência, uma Diretoria de Tecnologia da Informação, uma Diretoria de Infra-Estrutura de Chaves Públicas e uma Procuradoria-Geral.

Parágrafo único. A Diretoria de Tecnologia da Informação poderá ser estabelecida na cidade de Campinas, no Estado de São Paulo.

Art. 16. Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.

§ 1º O Diretor-Presidente do ITI poderá requisitar, para ter exercício exclusivo na Diretoria de Infra-Estrutura de Chaves Públicas, por período não superior a um ano, servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a serem exercidas.

§ 2º Aos requisitados nos termos deste artigo serão assegurados todos os direitos e vantagens a que façam jus no órgão ou na entidade de origem, considerando-se o período de requisição para todos os efeitos da vida funcional, como efetivo exercício no cargo, posto, graduação ou emprego que ocupe no órgão ou na entidade de origem.

Art. 17. Fica o Poder Executivo autorizado a transferir para o ITI:

I - os acervos técnico e patrimonial, as obrigações e os direitos do Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia;

II - remanejar, transpor, transferir, ou utilizar, as dotações orçamentárias aprovadas na Lei Orçamentária de 2001, consignadas ao Ministério da Ciência e Tecnologia, referentes às atribuições do órgão ora transformado, mantida a mesma classificação orçamentária, expressa por categoria de programação em seu menor nível, observado o disposto no § 2º do art. 3º da Lei nº 9.995, de 25 de julho de 2000, assim como o respectivo detalhamento por esfera orçamentária, grupos de despesa, fontes de recursos, modalidades de aplicação e identificadores de uso.

Art. 18. Enquanto não for implantada a sua Procuradoria Geral, o ITI será representado em juízo pela Advocacia Geral da União.

Art. 19. Ficam convalidados os atos praticados com base na Medida Provisória nº 2.200-1, de 27 de julho de 2001.

Art. 20. Esta Medida Provisória entra em vigor na data de sua publicação.

Brasília, 24 de agosto de 2001; 180º da Independência e 113º da República.

FERNANDO HENRIQUE CARDOSO
José Gregori
Martus Tavares
Ronaldo Mota Sardenberg
Pedro Parente

CUNHA, Mauro Leonardo de Brito Albuquerque. **Da marca pessoal à assinatura digital:** formas crípticas de validação da *in***forma**ção jurídica. 2006. 147f. il. Dissertação (Mestrado em Ciência da Informação) – Instituto de Ciência da Informação, Universidade Federal da Bahia. Salvador. Orientadora: Teresinha Fróes Burnham.

Salvador, 21 de fevereiro de 2006.

Mauro Leonardo de Brito Albuquerque Cunha