CENTRO UNIVERSITÁRIO DE BRASÍLIA

FACULDADE DE CIÊNCIAS JURÍDICAS E CIÊNCIAS SOCIAIS

CURSO DE RELAÇÕES INTERNACIONAIS

NAIANA RODRIGUES PEREIRA

ICP-Brasil:FUNCIONALIDADE PARA O REGIME DE COMÉRCIO INTERNACIONAL

Brasília – DF

2009

NAIANA RODRIGUES PEREIRA

ICP-Brasil: FUNCIONALIDADE PARA O REGIME DE COMERCIO INTERNACIONAL

Monografia apresentada como requisito parcial para a conclusão do curso de bacharelado em Relações Internacionais do Centro Universitário de Brasília – UniCEUB.

Orientador: Prof.º Marcelo Gonçalves Valle

Brasília – DF

2009

ICP-Brasil:FUNCIONALIDADE PARA O REGIME DE COMÉRCIO INTERNACIONAL

Banca examinadora:

_____

Marcelo Gonçalves Valle
(Orientador)

_____

Frederico Seixas Dias
(Membro)

_____

Carlito Roberto Zanetti
(Membro)

Brasília – DF

2009

“Aprender é a única coisa de que a mente nunca se cansa, nunca tem medo e nunca se arrepende”.

Leonardo da Vinci

RESUMO

O presente trabalho procura analisar a funcionalidade da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) para o regime de comércio internacional desenvolvido pela Organização Mundial do Comércio (OMC). Para isso será observado as características técnicas da ICP-Brasil e outros modelos internacionais disponíveis. Segue-se por mostrar o crescimento do comércio internacional relacionado à tecnologia da informação e por fim os princípios da OMC que regula o comércio internacional. Ao final conclui-se que as características técnicas da ICP-Brasil estão em consonância com os princípios da OMC, entretanto todo o seu formato institucional é devidamente oposto aos princípios centrais da OMC.

Palavras-chave: ICP-Brasil, OMC, regime internacional.

ABSTRACT

The purpose of this paper is to analyze the functionality of the Brazilian Public Key Infrastructure (ICP-Brasil) for the international trade developed by the World Trade Organization (WTO). Then, it is observed the technical characteristics of ICP-Brasil and other international disposables models. It follows to show the growth of information technology trade and it ends showing the principles of WTO that regulates the international trade. It concludes that the technical characteristics of ICP-Brasil is in consonance with the principles of OMCs, but the institutional format of ICP-Brasil is opposed to the WTO central principles

Key-words: ICP-Brasil, WTO, international regime.

LISTA DE SIGLAS

ABC – Agência Brasileira de Cooperação
AC – Autoridade Certificadora
AC Raiz – Autoridade Certificadora Raiz
ACT – Autoridade de Carimbo de Tempo
AES – *Advanced Encryption Standard*
AR – Autoridade Resgistradora
ARPA – Agência de Projetos e Pesquisa Avançadas
BXA – *Bureau of Export Administration*
CECA – Comunidade do Carvão e do Aço
CEE – Comunidade Econômica Européia
CG – Comitê Gestor
COTEC – Comissão Técnica Executiva
CSS – *Central Security Service*
DES – *Data Encryption Standard*
e-CAC – Centro de Atendimento Virtual ao Contribuinte
EUA – Estados Unidos da América
HD – *Hard Drive* ou Disco Rígido
ICP-Brasil – Infraestrutura de Chaves Públicas Brasileira
ITI – Instituto Nacional de Tecnologia da Informação
LCR – Lista de Certificados Revogados
MERCOSUL – Mercado Comum do Sul
MIT – *Massachusetts Institute of Tecnology*
MRE – Ministério das Relações Exteriores
NIST – *National Institute of Standards and Tecnology*
NSA – *National Security Agency*
OI – Organização Internacional
OMC – Organização Mundial do Comércio
ONG – Organizaççao não-governamental
ONU – Organização das Nações Unidas
RAM – *Randomic Memory*
RSA - *Rivest-Shamir-Adleman*
UE – União Européia
URSS – União das Repúblicas Socialistas Soviéticas

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

INTRODUÇÃO

Esta pesquisa destina-se a relacionar a Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil), seus princípios e capacidades técnicas, ao regime de comércio criado pela Organização Mundial do Comércio (OMC) com a intenção de verificar se o modelo brasileiro é funcional ao comércio internacional.

O desenvolvimento da Internet como um meio de troca de informações e dados auxiliou no desenvolvimento do comércio internacional. Entretanto, este meio não é seguro, não impede que outrem visualize ou modifique dados confidenciais armazenados e/ou trocados. Uma forma de garantir essa segurança é criptografia, no caso brasileiro, disponível pela ICP-Brasil.

A ICP-Brasil é a autarquia federal responsável pelo processo de criptografia e de certificação digital. Por meio desses processos é possível afirmar quem criptografou determinado dado. A este processo dá-se o nome de Assinatura Digital, que é o foco do modelo brasileiro. Este modelo permite visualizar se houve alterações no documento e determinar a data da troca das informações. Dessa forma, apresenta uma grande utilidade para o comércio on-line e trocas de informações via Internet.

A comercialização de bens e serviços está sujeita a regras internas de seus Estados e também a outras originadas de tratados internacionais. E internacionalmente, se tratando de comércio, a Organização Mundial do Comércio (OMC) é a organização internacional que atua diretamente no tema.

Portanto, esta pesquisa tentará responder à seguinte indagação: em que medida a ICP-Brasil preenche critérios de funcionalidade para o regime de comércio internacional desenvolvido no âmbito da OMC? Para a resposta desta indagação, duas outras questões deverão ser previamente respondidas. A primeira referente à estrutura interna da na ICP-Brasil: em que medida a ICP-Brasil garante segurança aos arquivos e dados por ela protegidos? E a segunda relacionada à OMC: em que medida a ICP-Brasil, como uma forma de prestação de serviço, está em consonância com os princípios da OMC?

Este intuito decorre da percepção que há um vácuo nos estudos sobre a ICP-Brasil, de forma ampla, e, mais especificamente, dentro do campo das Relações Internacionais. A falta de dados e pesquisas anteriores contribui ao desafio, pela dificuldade de achar textos acadêmicos; ao passo que permite uma abordagem mais ampla sobre o tema. Desta forma, a monografia foi realizada num nível mais abrangente ao tratar da comparação apenas dos princípios e características técnicas da ICP-Brasil com os princípios da OMC.

Para tanto, o devido trabalho está divido em três capítulos. O primeiro apresenta o corpo teórico de Relações Internacionais, com foco na Interdependência Complexa. Esta teoria servirá como aporte de análise e comparação entre a ICP-Brasil e a OMC. O segundo foca na questão técnica da ICP-Brasil, situando-a dentro de algumas opções internacionais e mostrando sua relevância técnica.

O terceiro capítulo apresenta o Comércio Internacional no setor de computação e vendas on-line e, se dedica a apresentar os princípios da OMC, comparando-os com as diversas características da ICP-Brasil e buscando mostrar se esta insituição, em seu formato atual, atende o perfil do regime internacional formado no Comércio Internacional. Para finalizar este trabalho é feita a conclusão arrematando os capítulos e delineando uma possíbilidade futura para a ICP-Brasil no contexto internacional.

CONCEITOS, TEORIAS E COOPERAÇÃO INTERNACIONAL

Este capítulo delineará duas teorias de Relações Internacionais, o Realismo e a Interdependência Complexa, justificando o uso desta última na análise sobre a Certificação Digital. Para tanto está dividido em duas partes, a primeira que apresentará as teorias, valorizando o papel das empresas como atores internacionais, a amplitude do conceito de segurança e o de funcionalidade em cada uma. A segunda parte foca a cooperação internacional e a importância da agenda dos Estados para que ela possa ocorrer. Dessa forma, haverá um suporte teórico capaz de explicar a consolidação do modelo brasileiro de Infra-estrutura de Chaves Públicas (ICP-Brasil), que será tratada no capítulo seguinte.

1.1 – Teorias, atores e limites

> A expressão Relações Internacionais indica, nos termos mais genéricos, o complexo das relações que intermedeiam entre os Estados (...); implica a distinção da esfera específica das Relações Internacionais da esfera das relações interna dos Estados[1].

O campo de estudo das Relações Internacionais foca nas interações que envolvem a transposição de fronteiras, conseqüentemente, os Estados. Estes atores são centrais aos estudos e, Bull os define como:

> Ccomunidades políticas independentes, cada uma das quais possui um governo e afirma a sua soberania com relação a uma parte da superfície terrestre e a um segmento da população humana. De um lado, os estados têm, com relação a este território e a essa população, o que poderíamos chamar de 'soberania interna', ou seja, a supremacia sobre todas as demais autoridades dentro daquele território e com respeito a essa população; de outro, detêm o que se poderia chamar de 'soberania externa', que consiste não na supremacia mas na independência com respeito às autoridades externas[2].

Para um fato, um acontecimento, um contrato ser considerado internacional ele necessitaria cruzar as fronteiras de no mínimo dois Estados; entretanto, a ultrapassagem das fronteiras não é mais, necessariamente, física. Os contratos

[1] PISTONE, Sergio. Relações Internacionais. In: BOBBIO, Norberto. Dicionário de Política. p, 1089.
[2] BULL, Hedley. A sociedade anárquica, pg.13.

de serviços, como mostra Friedman em *O mundo é plano*, são firmados e executados sem que os envolvidos precisem sair da sua residência, ou seja, sem transpor de fato qualquer fronteira, mas mantendo o aspecto internacional do contrato, como é possível observar no trecho:

> Vivek Kulkarni chefiava a secretaria governamental de Bangalore responsável por atrair investimentos globais de alta tecnologia. Ao deixar o cargo, em 2003, fundou uma empresa chamada B2K, com uma divisão denominada Brickwork, que fornece secretários indianos para executivos globais muito atarefados. Digamos que você dirija uma empresa e lhe pediram que proferisse uma palestra e fizesse uma apresentação em Power Point dentro de dois dias. Seu 'secretário executivo remoto' na Índia, contratado via Brickwork, vai fazer toda a pesquisa para você, criar a apresentação e enviar tudo por e-mail, de modo que esteja na sua mesa no dia previsto.[3]

A perda da transposição física decorre do processo de globalização que é, segundo Saraiva, "a internacionalização crescente dos circuitos produtivos e dos sistemas financeiros"[4]. Portanto, cabe também às Relações Internacionais estudar o processo de globalização, tanto por seu aspecto econômico, quanto suas conseqüências políticas e, neste trabalho, sob seu aspecto tecnológico que permite a continuidade deste processo[5].

As Relações Internacionais são um campo de estudo multidisciplinar, que analisa, interpreta e explica as relações entre os diversos atores internacionais, apesar de o Realismo citar apenas os Estados como atores. Ela surgiu como campo de estudo em 1919, após o fim da Primeira Guerra, por meio da Cadeira Woodrow Wilson no País de Gales.

O momento histórico de sua criação era peculiar, foi primeira vez que o mundo observava tamanha destruição e, nascia o ímpeto de impedir que as guerras ocorressem. Por isso durante vários anos o estudo das Relações Internacionais focou a segurança como elemento primordial das relações internacionais. A teoria Realista foi responsável por criar as raízes desses

[3] FRIEDMAN, Thomas. O mundo é plano, pg.45
[4] SARAIVA, José Carlos. Relações Internacionais: dois séculos de história, pg. 160.
[5] OLSSON. Globalização e atores internacionais. In: OLIVEIRA, Odete Maria. Relações Internacionais: interdependência e sociedade global, pg. 543.

estudos, que durante a Guerra Fria conseguiu explicar a atuação dos atores internacionais.

O Realismo foi a principal teoria utilizada ao longo do século XX, analisando os acontecimentos da bipolarização em seus momentos de maior tensão, como a Crise dos Mísseis, os conflitos de interesse entre os Estados Unidos e a União Soviética, a Guerra do Vietnã, entre outros. Entretanto, por se centrar na segurança como preocupação primária, constante e mais importante dos Estados, acabava por não conseguir analisar as relações nos momentos de distensão. Portanto, mesmo explicando os elementos centrais da atuação dos Estados, não conseguia analisar todo o cenário internacional.

Na década de 1980, Robert Keohane e Joseph Nye desenvolveram uma nova teoria, a Interdependência Complexa. Ela mostra que os atores internacionais se relacionam com interesses, objetivos distintos e, também que novos atores deveriam ser incluídos, como as empresas, organismos internacionais e a sociedade civil. Dessa forma, enquanto alguns atores estão preocupados com a segurança da sociedade internacional, outros atuam na busca de resolver problemas sociais, ambientais, etc. Desta forma, criaram um novo paradigma que proporciona uma maior amplitude de análise dos diversos atores.

1.1.1 – O Realismo

Consolidado após a Segunda Guerra Mundial, o Realismo implementou no estudo das relações internacionais a racionalidade dos Estados e a segurança nacional como objetivo primário. Os Estados são os únicos atores da sociedade internacional, segundo esta vertente teórica.

Essa sociedade difere das outras formas de sociedade devido a qualidade de seus membros. Eles são formados por outras sociedades; estando numericamente em menor quantidade que os indivíduos que formam as sociedades nacionais. Além do reduzido número, são heterogêneos, não existindo

um Estado padrão e, em conjunto são imortais[6]. Eles estão ligados por regras e instituições comuns, entretanto, a anarquia domina o cenário internacional. O Realismo para explicá-la busca um paralelo com a obra de Hobbes, *O Leviatã*.

O autor inglês explica a criação do Estado pela necessidade de garantir a segurança à vida dos seus cidadãos. O Estado é formado por um pacto entre todos os indivíduos que transferem seus direitos de uso da força a ele. Portanto, é constituída, retratado pela figura de um monstro, uma instituição que possui como objetivo central a proteção da vida de seus cidadãos; para este fim o Estado se torna, por direito, o único a deter o poder coercitivo, impedindo a beligerância entre seus cidadãos.

Este pacto social é firmado pra acabar com o "estado de natureza". Este é o momento anterior à formação do Estado, no qual todos possuem o direito de usar a força uns contra os outros. Ele era caracterizado pela insegurança, pela guerra de todos contra todos, onde os mais fortes iriam, por sua capacidade coerciva, dominar os mais fracos. Dessa forma, o cenário internacional é descrito como este estado de natureza, pois nele convivem Estados com os mesmos direitos e interesses, onde o ganho de poder de um equivale à redução de poder dos outros; ou seja, sempre que um ganhar poder outro o perderá na mesma proporção, havendo uma soma zero de poder dentro desta sociedade internacional.

Existe um aparente paradoxo entre uma ordem anárquica e uma sociedade de estados com instituições comuns. Porém anarquia representa a falta de um governo central, o que permite que possa haver conflitos e cooperação segundo o interesse e o objetivo de cada ator[7]. O que realmente reflete a sociedade internacional, na qual não existe por princípio um Estado soberano aos outros, central. Portanto, a ordem internacional que é "padrão de atividades que sustenta os objetivos elementares ou primários da sociedade dos estados"[8] só é possível num cenário que garanta a própria soberania dos atores.

[6] WIGHT, Martin. A política do poder, p. 98 e 99.
[7] WIGHT, Martin. A política do poder, p.97.
[8] BULL, Hedley. A sociedade anárquica, p.13.

O Realismo procura explicar a atuação dos atores, os Estados, nesta ordem sem um governo central, mas que é constituída por algumas regras, valores e instituições comuns. Em seu suporte teórico desponta os três princípios implícitos na obra de Maquiavel, em primeiro lugar a história é uma seqüência de causa e efeito, cujo curso se pode analisar e entender através do esforço intelectual; em segundo lugar, a teoria não cria a prática, mas a prática cria a teoria e por último, a política não é não é uma função da ética, mas sim a ética o é da política[9].

Para o Realismo a política e a sociedade são governadas por leis objetivas e que, portanto, para poder melhorar a sociedade é necessário conhecê-las[10]. Para comprovar a existência dessas leis a teoria vê-se obrigada a remeter-se à realidade, no sentido que apenas a comparação com os fatos reais pode garantir a sustentabilidade da teoria. Ou seja, ela é desenvolvida a partir do que de fato ocorre no ambiente internacional, não buscando encaixá-la em padrões pré-estabelecidos. Esta preocupação, em verificar empiricamente a teoria, é posta a prova pela singularidade dos acontecimentos, os fatos nunca são idênticos entre si, nem inteiramente diferentes. E é pela comparação entre eles e as construções mentais da teoria que pode entender os princípios, leis da política internacional

"A humanidade reage a situações sociais por meio de padrões repetitivos. A mesma situação, uma vez reconhecida em sua identidade com situações anteriores, suscita a mesma resposta"[11], isso é o que permite haver acontecimentos únicos com características similares a outros.

A teoria realista possui o foco nos acontecimentos como são e não como deveriam ser, portanto, não há a preocupação com os motivos, as ideologias por traz das decisões, mas apenas com o interesse definido pelo poder.

A política será caracterizada pela preocupação constante com o poder e, independente do fim desejado, o poder é um objetivo imediato. Carr o divide em poder político, militar, econômico e de opinião. O poder político significa a

[9] CARR, Edward. Vinte anos de crise, p.86.
[10] MORGENTHAU, Hans. A política entre as nações, p. 4 e 5.
[11] MORGENTHAU, Hans. A política entre as nações, p. 11.

capacidade de controle de determinadas ações de um Estado por outro, por meio da influência[12]. O poder militar é, em última instância, o determinante dos acontecimentos, assim, os Estados não podem se esquecer da estratégia e de melhorar suas forças armadas, e nem do conhecimento sobre os exércitos alheios, também em tempos de paz. Por ser o determinante dos acontecimentos, em última hipótese, durante a Guerra Fria, momento auge da teoria realista, os temas que envolviam aspectos militares foram tratados como interesse máximo do Estado, portanto, como *hight politics;* enquanto os econômicos e sociais tinham menor interesse estatal se tornaram *low politics.*

Até a Primeira Guerra Mundial a guerra foi uma instituição reafirmada constantemente, como direito primário dos Estados, nas palavras de Maquiavel "justa, na verdade é a guerra, quando necessária, e piedosa as armas quando só nas armas reside a esperança"[13]. Após as duas guerras a Organizações das Nações Unidas (ONU) regulamentou o uso da força; limitando em apenas três casos: quando decidido pelo Conselho de Segurança, para legítima defesa pessoal e coletiva e nos casos de libertação nacional. Assim, hoje por mais determinante que forças armadas sejam, o seu uso foi limitado, incentivando a utilização de outras formas, econômicas, culturais, para influenciar os Estados.

O poder econômico fica em segundo plano quando comparado ao militar. Entretanto, o desenvolvimento da civilização está pautado, especialmente após a Revolução Industrial, nos ganhos econômicos, nas melhorias derivadas das novas tecnologias e na influência que o comércio possui. Hoje a capacidade de interação e influência econômica é importantíssima, tanto pelo aumento da quantidade de empresas com filiais em outros países, quanto pelo modo como o sistema monetário adquire uma influência, especialmente com a capacidade tecnológica atual que permite transações rápidas, constantes, sem a eficiente fiscalização e controle pelos governos.

Entretanto, no cenário de Guerra Fria, por mais que ocorressem relações econômicas importantes, o comércio não tinha a amplitude que possui na

[12] MORGENTHAU, Hans. A política entre as nações, p. 57.
[13] MAQUIAVEL, Nicolau. O príncipe, p. 150.

atualidade. As duas potências estavam preocupadas com zonas de influência, no desenvolvimento do poder bélico, por isso este modo de influência foi deixado de lado. Mesmo os planos econômicos, como o plano Marshall implementado pelos Estados Unidos de 1947 a 1951 ocorreu com conotações políticas de impedir que a doutrina socialista se firmasse nos estados europeus. Portanto, o interesse imediato era impedir o aumento de poder dos soviéticos, sua área de influência, que significaria a perda de poder pelos norte-americanos.

Os aspectos militares deste período são de extrema importância para entender o atual papel da economia nas decisões políticas e poder dos Estados. Neste período que ocorreu, em função das questões militares, o desenvolvimento de satélites; por convênios entre militares e universidades, a Internet. Castells escreve sobre a criação da Internet:

> A Internet se desenvolve a partir da interação entre a ciência, pesquisa universitária fundamental, os programas de pesquisa militar dos Estados Unidos – uma combinação curiosa – e a contracultura radical libertária. [...]. Simplesmente observo que a Internet nasce como programa de pesquisa militar mas que, na verdade, nunca teve aplicação militar. Este é um dos grandes mitos existentes.[14]

A opinião pública passou, após a Primeira Guerra, a ganhar destaque no cenário internacional, mas ela não possuía capacidade de influenciar significativamente as relações internacionais. Entretanto, é fundamental ao Estado possuir apoio interno para as decisões externas, principalmente quando envolva conflitos armados. Portanto no período da Guerra Fria foi gasto elevadas somas com propaganda, ou como ficou conhecida a guerra psicológica[15].

Esta época, além do apoio interno, era interessante e necessário, tanto para os Estados Unidos quanto para a União Soviética, criar zonas de influência. Ambos investiram em programas de rádios em vários idiomas, a indústria cinematográfica aderiu ao processo associando o inimigo aos vilões, tudo para manter essas zonas e desmerecer a ideologia oposta.

---

[14] CASTELLS, Manuel. Internet e sociedade em rede. In: MORAES. Por uma outra comunicação, p. 257.
[15] MATTERLART, Armand. Comunicação-mundo, p.95.

Hoje a participação da sociedade civil é muito maior que outrora, com a criação de Organizações Não-Governamentais, e há possibilidade dela se inserir e participar mais ativamente nas relações internacionais. Em muitos temas, como meio ambiente, pobreza, direitos humanos a sociedade civil consegue ações mais efetivas que os Estados na resolução dessas questões.

Maquiavel em *O Príncipe* separa a política da moral. O autor distingue a forma de atuar do Estado que será julgado pelo seu êxito e se este for bom, não importará os meios empregados[16]. Assim tendo os indivíduos uma série de preceitos morais e éticos a seguir, como não matar, respeitar a propriedade privada, dentre vários outros, mas o Estado não pode segui-los. Sua função é manter a segurança nacional interna e externa, deve manter, como único, o direito de utilizar elementos de força e coerção. Entretanto, isso não significa que não haja moralidade alguma, há sim valores, entre eles dois de grande significado, o primeiro da sobrevivência da instituição estatal e o da prudência na tomada de decisões os quais são extremamente significantes para a atuação estatal.

Portanto, a teoria realista, no que tange à participação internacional de empresas, não as vê como atores das relações internacionais. E trata as questões econômicas não ligadas diretamente a elementos bélicos como *low politics*, tema de baixo interesse para o Estado. A valorização da segurança nacional ocorre em termos militares, despreocupando-se com a segurança de informações de outros setores. A funcionalidade voltada à economia não é o foco desta teoria.

Assim, quando a ameaça de uma guerra total, nuclear, se afastou, que a União Soviética não conseguiu mais seguir os avanços dos Estados Unidos e, principalmente, quando os outros temas, de *low politics*, entraram na agenda de atuação e preocupação dos Estados o Realismo não tinha como explicá-los, demandando um novo corpo teórico, a Interdependência Complexa.

1.1.2 – A Interdependência Complexa

[16] MAQUIAVEL, Nicolau. O príncipe, p.101.

Tanto a Interdependência Complexa quanto o Realismo são tipos ideais para analisar a realidade das relações internacionais. Ambos são incapazes de explicar a atuação de todos os atores em todos os contextos e a todo tempo. Mas, com o objetivo de suprir a necessidade teórica de analisar as relações internacionais por um prisma distinto da segurança nacional voltada ao aspecto militar que foi criada a Interdependência Complexa.

> Ela, acima de tudo, substitui a dicotomia entre 'guerra e paz' pela de 'cooperação e competição', revelando que o mundo não vive apenas de enfrentamentos e, mesmo nestes casos, não são apenas militares, mas também políticos e econômicos[17].

A primeira diferença significativa é que engloba mais atores internacionais, empresas multinacionais, organismos internacionais, sociedade civil que atua, principalmente, por meio das ONGs. Ou seja, por ator internacional não é demandado o status jurídico, mas a possibilidade de realizar ações internacionais. Os papéis exercidos também se mesclam, sendo resultado da função que exercem.

Com o ingresso de novos atores são desenvolvidos novos canais de comunicação que ultrapassam o do Realismo. Enquanto este observa apenas a canal inter-estatal, caracterizado pelas relações tradicionais entre os Estados, a Interdependência Complexa mostra os canais transgovernamentais, nos quais as burocracias estatais agem em vários assuntos de distintas naturezas, temas de forma a se tornar inviável dizer que os Estados são uma unidade coerente; e o transnacional que se caracteriza pela ação de outros atores não estatais.

Por esses canais é possível notar a existência de regras, normas e procedimentos que regulam a atuação dos atores. A isto Keohane e Nye chamam de regimes internacionais[18]. Krasner desenvolve um trabalho mais extenso sobre os regimes internacionais ao defini-lo como princípios, normas, regras e procedimento decisórios explícitos ou implícitos sob os quais convergem expectativas dos atores em uma determinada área das relações internacionais[19].

---

[17] OLSSON. Globalização e atores internacionais. In: OLIVEIRA. Relações Internacionais: interdependência e sociedade global, p. 549.
[18] KEOHANE, Robert; NYE, Joseph. Power and interdependence, p.17.
[19] MUELLER, Milton. The internet and the global governance, p. 242.

Desta forma ele hierarquiza os passos para criar um regime internacional eficiente. Os princípios são tratados por Mueller como conceitos, padrões de comportamento definidos em termos de direitos e obrigações aceitos pelos atores numa determinada área. As normas, que prosseguem da existência dos princípios, são valores morais e de conduta. As regras e procedimentos exprimem a criação de estruturas e instituições que definem regras e leis para o funcionamento da sociedade[20], ou seja, traduzem em termos práticos os princípios e normas acordados entre os membros da sociedade.

Apesar das regras não vigorarem em todos os setores e para todos os atores, elas não podem ser ignoradas. Há regras valem para um considerável número de Estados, como a União Européia que possui sólidas normas jurídicas para seus estados-membros. Porém não são todos os temas que possuem regras internacionais, alguns, como, por exemplo, o contra-terrorismo, que não possui nada que o regulamente.

Portanto essas interações desenvolvem papéis relevantes a todos os atores. Por exemplo, as ONGs atuam de maneira significativa em temas sociais, como direitos humanos, problemas ambientais. As empresas transnacionais estão interessadas com o aumento dos lucros e perdendo sua nacionalização decorrente da flexibilização conseguem se expandir a vários países; e os Estados mantendo seu poder em órgãos significativo como a ONU, mais precisamente o Conselho de Segurança. Todo este aglomerado de papéis e funções constitui um cenário que não apresenta uma soma zero de poder. O interesse é o ganho absoluto, o que irá ganhar, não como o sistema repassará esses ganhos, ou seja, se ele em relação aos outros estará mais forte ou fraco[21]. Esta análise, ganhos relativos, é voltada exclusivamente à composição internacional de poder, visível em casos onde a segurança bélica figura como aspecto fundamental[22].

[20] MUELLER, Milton. The internet and the global governance, p. 242.
[21] JÚNIOR. Poder e interdependência: perspectivas de análise das Relações Internacionais na óptica de Robert O. Keohane e Joseph S. Nye. In: OLIVEIRA, Odete Maria. Relações Internacionais: interdependência e sociedade global, p. 189.
[22] ROCHA. Poder, interdependência e interdependência complexa. In: OLIVEIRA, Odete Maria. Relações Internacionais: interdependência e sociedade global, p. 468.

Outro aspecto relevante da teoria é o significado de interdependência. Ela significa dependência mútua, com efeitos recíprocos, possuindo constrangimentos e custos associados[23]; que não pode ser entendida apenas em sua vertente de ganhos, nem que ela acabará com os conflitos. Os custos não são meramente econômicos, mas de natureza mais ampla – políticos, econômicos, sociais, entre outros. Ou seja, um ator só é interdependente quando ele precisa pesar as ações de outros por lhe causar efeitos relevantes, custos altos que influenciem significativamente em suas políticas. Portanto, nem toda relação, por mais importante que seja, é necessariamente interdependente. Se os custos são baixos de forma a não causar constrangimentos aos envolvidos, eles têm apenas interconexões; entretanto, se ao contrário, as ações de um causam conseqüências significativas, são interdependentes.

Os conflitos, continuam existindo na Interdependência Complexa, apresentam novas característica e podem até serem intensificados. Estes são verificáveis nas controvérsias econômicas, nas atuações de Estados com interesses contrários. Seu aumento ocorrerá devido à quantidade de temas que agora formam a agenda internacional. Entretanto, devido ao custo econômico, à aceitação pela sociedade internacional, aos tratados internacionais, o uso do poder bélico é pouco utilizado. Essa redução da possibilidade de utilização de pressões militares é mais evidente dentro de grupos de países que possuem maiores interesses comuns e/ou estejam sob um mesmo regime internacional.

Além da possibilidade bélica, cada vez mais limitada, há outras formas de agir de um ator que influem em conseqüências mais custosas a outros. Essas podem ser extremamente negativas, sem utilizar a pressão militar. Um exemplo é o mercado especulativo, a saída ou entrada de divisas podem desestruturar a economia dos Estados, influindo em decisões governamentais que não conseguem regulamentar e nem controlar o fluxo de capital. Dessa forma novas formas de atuação, pressão, influência são demandadas, sem envolver o uso da força.

[23] KEOHANE, Robert; NYE, Joseph. Power and interdependence, p.7 e 8.

Uma das formas de influenciar as decisões, de exercer poder sobre um ator é justamente não ser interdependente de algo. Assim o fato de não ser altamente influenciado, de não ter altos custos decorrentes da decisão do outro, faz com que em relação a este haja um maior poder de barganha. Essas ações só são possíveis de serem tomadas quando há o conhecimento da sensibilidade e vulnerabilidade envolvidas.

Como dito a interdependência remete a altos custos entre os atores, mas estes ocorrem em dois tempos distintos, o primeiro que é imediato, ou seja, os custos sem a mudança das políticas, a sensibilidade. O segundo, a vulnerabilidade, são os custos após a revisão das políticas. Estes são mais importantes, pois tendo o ator a possibilidade de mudar sua atuação sem constrangimentos elevados, ele assim fará. Ou seja, as decisões principais deverão ser tomadas num cenário que ultrapasse o imediatismo e para serem uteis, funcionais devem trazer ganhos ou reduzir a possibilidade de dependência em relação aos fatores externos.

Os Estados não fazem uma agenda baseada na racionalidade realista. As agendas são formadas tendo em consideração o interesse de vários grupos nacionais que exercem pressões políticas, especialmente por meio de *lobbies*, entidades de classe, sindicatos. Agindo em conjunto aos diversos interesses que são apresentados nas agendas, existe também a grande diversidade de órgãos que exercem papéis internacionais por um Estado. Essa burocracia, por mais que existam políticas públicas delineadas, atuam de forma a impedir a centralização e conseqüente racionalidade. Portanto, hoje a agenda de cada país tenta alcançar internacionalmente o máximo para suprir os interesses internos divergentes.

Essa possibilidade de criar uma agenda ampla é vantajosa para os Estados com menor poder bélico, mas de importância econômica. Além de não observar o aspecto militar para designar a importância do Estado nas questões a serem tratadas (exceto nos casos onde o tema realmente envolva questões bélicas),a ampliação das agendas conecta temas aparentemente dispersos entre si. Ou seja, para conseguir uma abertura comercial necessita-se de trocas de interesse, cada interessado cede em um aspecto para alcançar seus interesses. Isso é

visível nos encontros da Rodada de Doha, onde os países industrializados e os em desenvolvimento procuram ceder em algum aspecto para poderem se beneficiar em outros. Esse modelo de acordo e de atuação é possível quando não se está num cenário envolto em intenções belicistas.

A Interdependência Complexa, portanto, desenvolve um corpo teórico que muda a análise das relações internacionais. Enquanto o Realismo apresentava uma constante dicotomia entre a possibilidade de guerras e a tentativa de consolidar a paz, a Interdependência Complexa altera esta análise. Tratando-se de um cenário onde os custos são os aspectos mais importantes a serem avaliados e que se busca o ganho absoluto ao relativo, fica a questão da possibilidade de cooperar ou de competir para alcançá-los.

Esta teoria para a análise do desenvolvimento da Criptografia Brasileira é extremamente mais viável e completa do que a Realista. Por mais que o modelo adotado tenha sido, em suas intenções, identificado como tema de segurança nacional, ele não é tratado em termos bélicos. E a implementação para uso das empresas e sociedade civil ocorreu pela pressão e interesse do setor empresarial. Portanto, essa tecnologia, que foi estruturada por meio da análise de vários modelos disponíveis internacionalmente, deverá ser analisada por uma teoria que compreenda a incidência de uma série de fatores alheios à esfera burocrática brasileira e que, apesar de cotada como segurança nacional, não pode ser entendida pelos aspectos realistas.

1.2 – Cooperação Internacional

Uma ação de cooperação técnica internacional é “uma intervenção temporária destinada a promover melhorias qualitativas e/ou estruturais num determinado contexto sócio-econômico’’[24] tanto para a resolução de problemas quanto para melhor aproveitamento das oportunidades existentes. A cooperação permite acessar tecnologia, experiências, conhecimento e capacitação de indivíduos, de empresas públicas e privadas (associações, institutos, federações); portanto não existem *a priori* papéis pré-estabelecidos para quem presta a

[24] ABC. Diretrizes para o desenvolvimento da cooperação técnica Internacional multilateral e bilateral, p. 7.

cooperação e para quem a recebe, cada caso deve ser analisado e projetado de forma única, a alcançar da melhor forma o objetivo proposto.

A justificativa para a implementação de uma cooperação não está nos recursos alocados e não, necessariamente, no que é produzido diretamente (laboratórios, estradas, centro de saúde, etc.), mas sim nos benefícios ensejados por aqueles recursos em termos de contribuição para o desenvolvimento socioeconômicos do país (renda, transporte mais barato, melhoria de saúde pública). Três vantagens são observáveis ao Estado que recebe a cooperação. Primeiro há a melhoria da capacidade de seus funcionários que são treinados; segundo, as instituições aprendem novas formas de gestão e de exercer suas atividades; e terceiro, em conseqüência dos dois primeiros, melhoram as estratégias internas delineadas pelos Estados. Portanto, as políticas públicas, principalmente as que dependem de parceria com o setor privado e ONGs são mais bem formuladas e executadas. Além da possibilidade de conscientizar a população que se torna mais participativa, mais cidadã.

A ONU foi a responsável pela difusão e pelo incentivo para ocorrência das cooperações internacionais. Até 1959 era utilizado o termo “assistência técnica”, que foi substituído por “cooperação técnica”[25]. Este termo pressupõe a existência de partes desiguais (uma que detém o conhecimento e outra que deseja recebê-lo) que possuem o interesse mútuo na troca que será efetuada.

> Segundo Soares: não se trata de mera questão vocabular, mas de uma mudança de enfoque no que respeita aos movimentos internacionais de recursos [...] trata-se, antes, da afirmação de um direito ao desenvolvimento por parte desses Estados [em vias de desenvolvimento], conjugados com um dever de cooperação por partes dos países industrializados, dentro dos princípios já enunciados da Carta da Organização das Nações Unidas.[26]

Para que essas ações continuem a ocorrer é preciso haver estruturas internas, administrativas, governamentais que permitam a continuidade. Assim, a prioridade das cooperações era e, continua sendo, capacitar o corpo

[25] Assembléia Geral da ONU. Resolução 1383 (XIV)B.
[26] SOARES, Guido. A cooperação técnica internacional. In: MARCOVITCH, Jacques. Cooperação Internacional. Estratégia e gestão, p. 170.

administrativo responsável pela promoção de políticas públicas, envolvendo, principalmente, a administração, tecnologia e gestão, garantindo a autonomia dos países.

> A cooperação internacional tem como um dos seus primeiros pressupostos a idéia da 'alteridade', isto é: respeito de um Estado pela existência de outros Estados, cujos objetivos podem e devem ser por eles traçados[27].

As relações de cooperação além de promover o desenvolvimento, respeita a autonomia do Estado beneficiário, pois objetiva que este possa continuar melhorando por conta própria, não havendo qualquer intervenção na soberania e políticas adotadas por seu governo. Ela também estreita os laços, as relações entre os atores envolvidos, pois há uma troca de experiências, reciprocidade; além da melhoria do processo administrativo e legal.

Ela pode ser realizada por Organismos Internacionais, Estados, Organizações não-governamentais e entre parcerias entre esses membros. Como a cooperação não visa lucros, não há participação de empresas como proponentes dessas relações[28]. Estas, se envolvidas são, normalmente, prestadoras de serviços terceirizados. O aspecto financeiro é importante, pois o dinheiro investido em cooperação não é re-embolsável. Portanto, para que haja a validade do projeto este deverá trazer as fontes do orçamento e os respectivos responsáveis.

Entretanto, não são caracterizados como cooperação os auxílios enviados para superação de crises, como por exemplo, a fome na África ou as catástrofes naturais, essas emissões de recursos que visam a resolução de crises são assistências humanitárias e não cooperação. A cooperação não visa remediar conjunturalmente uma situação, mas promover mudanças estruturais.

Portanto, para caracterizar uma ação entre Estados como cooperação internacional é necessário observar todas essas particularidades. Se tratando da

---

[27] AMORIM, Celso. Perspectivas da cooperação internacional. In: MARCOVITCH, Jacques. Cooperação Internacional. Estratégia e gestão, p. 151.

[28] ABC.

ICP-Brasil é fundamental delinear estas características pois ao primeiro momento pode parecer que o modelo brasileiro deriva de acordos de cooperação, entretanto após observar os critérios descritos fica possível perceber que não pode ser assim descrito.

Após observar os vários atores atuantes dentro do tema tratado (empresas, Estados, burocracias estatais e Organizações Internacionais) fica perceptível que a escolha pela Interdependência Complexa como arcabouço teórico é mais pertinente que o Realismo. Ela é capaz de prover dois conceitos importantes. O primeiro da existência de mais de um ator, ou seja, de que as empresas também são atores internacionais relevantes; e o segundo de custos que ultrapassam aspectos econômicos para observar a utilidade de determinada medida.

Com o aporte dos conceitos abordados neste capítulo é possível notar a importância das características técnicas da ICP-Brasil e dos conceitos por trás de sua formação e que guiam seu funcionamento.

MODELOS DE CRIPTOGRAFIA

A Certificação Digital é uma forma de manter a confidencialidade, a integridade e a disponibilidade de dados e documentos eletrônicos. Ela utiliza processos algébricos (criptografia, decriptografia, função de *hash*[29]) difíceis de serem quebrados. É, portanto, uma forma de garantir a segurança da informação, no processo de armazenamento e troca de dados. Para entender as vantagens de seu uso é necessário verificar sua capacidade de segurança, que perpassa a álgebra, o modelo adotado pelo Brasil e o próprio conceito de segurança de informações.

Este capítulo se desenvolve em três partes. A primeira visa explicar o conceito de segurança da informação, assim como os conceitos e processos técnicos da criptografia, decriptografia e função de *hash*. Após, na segunda parte, será visualizado os modelos americano e europeu de Infra-estrutura de Chaves Públicas, assim como a escolha brasileira. Na ultima seção explicita-se a segurança do modelo brasileiro perpassando seus princípios, suas vantagens e críticas.

2.1 Criptografia, segurança de dados eletrônicos

O desenvolvimento da Internet[30], da possibilidade de armazenar dados e arquivos em redes de computadores e de trocá-los, foi gerado por meio de uma série de fenômenos diversos ocorridos em vários locais e por várias pessoas ao redor do globo[31]. O início de seu desenvolvimento foi marcado pelo trabalho de três centros de pesquisas desvinculados um dos outros: *Massachusetts Institute*

[29] É um algoritmo que permite a comprovação da integridade da mensagem. KUROSE, James e ROSS, Keith. Redes de computadores e a Internet: uma nova abordagem, p. 460

[30] "A Internet é na verdade uma rede de redes. Em outras palavras, ela é um conjunto interconectado de redes públicas e privadas, cada uma com gerenciamento próprio". Ela está fundamentada em quatro princípios desenvolvidos por Cerf e Kahn: autonomia entendida como a capacidade da rede de operar por si só sem depender de mudanças internas para funcionar com outras redes; serviço de melhor esforço que significa a capacidade de transmitir dados de fim a fim sem perder a mensagem; roteadores sem estado que demonstra que os roteadores podem transmitir a informação sem necessidade de um estado apropriado e por último o controle descentralizado, que a Internet não deveria ter um controle centralizado. KUROSE, James e ROSS, Keith. Redes de computadores e a Internet: uma nova abordagem, p. 3 e 46.

[31] CASTELLS, Manuel. Internet e sociedade em rede. In: de MORAES, Dênis. Por uma outra comunicação, p. 258.

of Technology (MIT), *Rand Institute* e *National Physical Laboratory*; os dois primeiros estado-unidenses e o último inglês. Na década de 1960 eles iniciaram valiosas descobertas de como interligar e trocar informações por meio de redes de computadores, a pioneira foi a ARPAnet desenvolvida pela agência norte-americana ARPA (Agência de Projetos e Pesquisa Avançada)[32]. À medida que suas redes foram se desenvolvendo, pela implementação de cabos de fibras ópticas a partir de 1977 e da padronização de sua linguagem, permitiu que mais usuários tivessem acesso à Internet, podendo receber, ler, criar e disponibilizar esses dados na rede mundial de computadores.

> A difusão de computadores pessoais, aparelhos de fax, Windows e modems conectados a uma rede de telefone global se juntou no fim dos anos 1980 e início dos anos 1990 para criar a plataforma básica que deu início à revolução global da informação. A chave era a combinação de tudo isso num único sistema intreroperável. Isto aconteceu [...] quando tivemos em forma bruta uma plataforma computacional padronizada – o PC (computador pessoal) da IBM[33] – juntamente com uma interface de usuário gráfica padronizada [...] – Windows[34] – e com um instrumento de comunicação padronizado – modems *dial-up*[35] e a rede mundial de telefones. Uma vez que tínhamos a plataforma interoperacional básica, os aplicativos [...] conduziram sua difusão para qualquer lugar [36].

A difusão e possibilidade de modificar os arquivos recebidos tornaram uma das maiores razões para os investimentos em segurança da informação.

2.1.1 – A segurança da informação

A segurança se desenvolve para barrar qualquer processo de alteração de dados, isso, pois é impossível descomprovar a originalidade de um dado, já que não existem cópias no sistema eletrônico. Ou seja, todo dado inserido numa linguagem eletrônica é por excelência original.

---

[32] KUROSE, James e ROSS, Keith. Redes de computadores e a Internet: uma nova abordagem, p. 44.
[33] A IBM é uma empresa norte-americana criada na década de 1880 atuando na eletrônica e alcançando o espaço computacional rapidamente. Ela foi a responsável pela disseminação dos computadores pessoais a partir do início da década de 1980.
[34] Sistema operacional desenvolvido pela Microsoft que desenvolveu a interface de usuário gráfica.
[35] Forma de conectar o computador a rede telefônica para ter acesso a Internet.
[36] FRIEDMAN, Thomas. O mundo é plano, p. 73.

> Sem o certificado é muito fácil você simular mentiras, manejos. Sabe por quê? No mundo digital não há cópias, tudo no mundo digital é original. Pega um documento, bota na rede, se você digitalizou o documento, acabou. Quantas cópias você fizer, você está fazendo originais porque não tem cópias no mundo digital. Então você simula isso se você quiser. O certificado que impede essa simulação. Seu certificado torna você único no mundo.[37]

> Segurança da informação é definida como a área do conhecimento que se dedica à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade ou como a prática de gestão de riscos de incidentes que comprometam: confidencialidade, integridade e disponibilidade da informação[38].

Portanto, busca-se dificultar o acesso aos arquivos e dados armazenados, para manter a integridade e confidencialidade desses arquivos, pois qualquer coisa que seja feita na rede pode ser detectada eletronicamente. Assim, tudo que circula na Internet é passível de ser interceptado e, não sendo possível barrar este processo o fundamental é proteger o conteúdo da informação.

> Godoy define os elementos os quais a segurança da informação se preocupa como: confidencialidade (...) é a capacidade de controlar quem pode ou não ter acesso às informações e sob quais circunstâncias; integridade é a garantia de que as informações armazenadas ou transmitidas não serão alteradas; e a disponibilidade é a garantia de que as informações estarão disponíveis sempre que necessário[39].

Os ataques à segurança podem ser passivos e/ou ativos, conforme o interesse e o grau de ingerência do intruso. Os ataques passivos ocorrem quando há apenas a leitura da mensagem interceptada, enquanto os ativos decorrem da alteração dos dados[40]. A criptografia desponta como uma forma de garantir as características de confidencialidade, integridade e disponibilidade dos documentos. Ela também, quando se utiliza a assinatura digital[41], consegue atestar a autenticidade de quem envia a mensagem.

2.1.2 - O processo de criptografar e decriptografar

[37] BARRA, Marcelo. Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e a formação do Estado eletrônico, p. 54.
[38] GODOY, Max Bianchi. A segurança da informação e o sucesso das organizações,
[39] GODOY, Max Bianchi. A segurança da informação e o sucesso das organizações,
[40] STALLINGS, William. Cryptography and network security, p. 7.
[41] A Assinatura Digital é a criptografia da função de *hash*; será tratada na parte 2.1.3.1.

A criptografia acompanha a história humana. No Egito antigo os hieróglifos poderiam ser caracterizados como criptografia, pois apenas uma parcela restrita da população tinha conhecimento de seus significados. Júlio César, imperador romano, desenvolveu seu próprio sistema de cifração pela substituição de letras. Segundo Vaudenay, a comunicação por códigos era normalmente requerida pelas diplomacias, nos períodos de guerras e por pessoas e empresas privadas quando necessitavam de proteção contra terceiros.[42]

> Segundo Kurose: As técnicas criptográficas permitem a um remetente disfarçar os dados de modo que um intruso não consiga obter nenhuma informação com base nos dados interceptados. O destinatário, é claro, deve estar habilitado a recuperar os dados originais a partir dos dados criptografados [43].

A criptografia é "o estudo de métodos que permitam ocultar o conteúdo de mensagens ou dados armazenados" [44]. Ela decorre da necessidade de enviar uma mensagem por um canal inseguro, canal o qual a mensagem pode ser interceptada por terceiros (ataques ativos e passivos), por exemplo a Internet, prevenindo que o conteúdo da mensagem seja visto e/ou alterado.

A mensagem original ou texto claro[45] é criptografada por um algoritmo criptográfico por meio da inserção de uma chave[46], produzindo ao final um texto cifrado[47] incompreensível - processo de cifração. Quando esta mensagem cifrada chegar ao destinatário ele deverá possui a chave que permita transformar o texto cifrado novamente no texto claro, original - decifração.

---

[42] VAUDENAY, Serge. A classical introduction to cryptography, p. 1 e 2.
[43] KUROSE, James e ROSS, Keith. Redes de computadores e a Internet: uma nova abordagem, p.444.
[44] GODOY, Max Bianchi. A segurança da informação e seu sucesso para as organizações, p. 71.
[45] É a informação que se deseja cifrar. Normalmente são arquivos de texto, figuras, planilhas, tabelas, etc.
[46] "Uma cadeia de números ou de caracteres como entrada para o algoritmo de criptografia". KUROSE, James e ROSS, Keith. Redes de computadores e a Internet: uma nova abordagem, p.445.
[47] É a informação após o processo de cifração. É um conjunto de dados ininteligíveis em si, que é o resultado da criptografia em si.

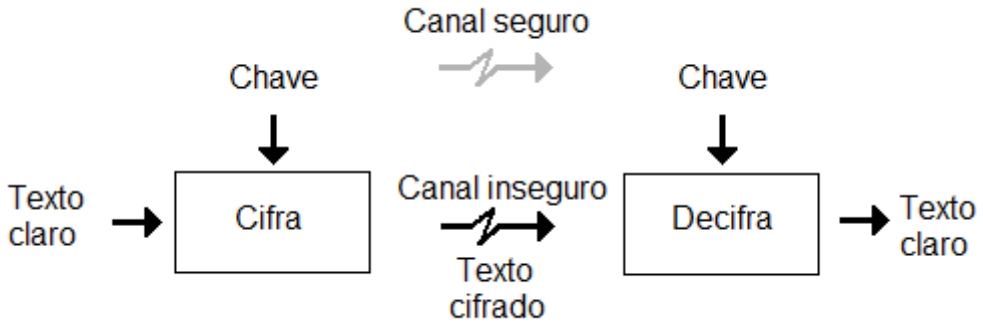

Figura 2.1

Fonte: STALLINGS, William. Cryptography and network security

Essas duas chaves podem ser iguais, criando-se um sistema de chaves simétricas ou podem ser distintas entre si, permitindo que uma das chaves seja conhecida por todos e a outra, pessoal e secreta. Neste caso é criado um sistema de chaves públicas ou assimétricas que é a base da ICP-Brasil. Se a chave for incorreta o texto claro não é cifrado e nem a decifração ocorre.

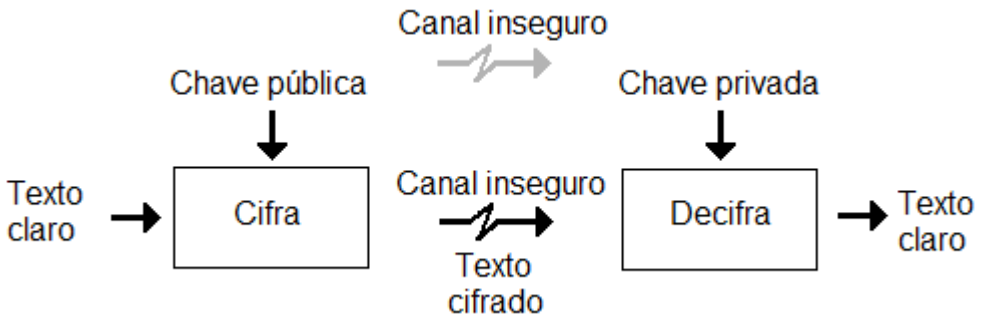

Figura 2.2[48]

Fonte: ITI. O que é certificação digital?

O processo de cifração e decifração pode utilizar uma função algorítmica que permite a transposição ou permutação e substituição dos dados fornecidos, no caso do *Data Encryption Standard* (DES) e/ou *Advanced Encryption Standard* (AES) ou uma função matemática como o RSA, (*Rivest-Shamir-Adleman*) iniciais de seus criadores que o desenvolveram no MIT. Normalmente os sistemas que

[48] A chave pública é o cógido de caracteres disponibilizado a toda a comunidade eletrônica, juntamente com os Certificados Digitais. As chaves privadas são de conhecimento restrito ao usuário. O tema será abordado no item 2.1.3.

trabalham com permutações e substituições utilizam os dois elementos, para aumentar a segurança envolvida.

A transposição é o rearranjo dos elementos contidos no texto claro, enquanto a substituição é a transformação de um elemento (bits, letras) em outro. O processo pode ser feito por elementos ou por blocos. Os processos por caracteres é a transposição e/ou substituição de cada elemento individualmente; enquanto os blocos são as transposições e substituições de unidades sempre de mesmo tamanho – bits – rearranjadas ou substituídas entre si. Portanto, a tendência é utilizar vários estágios de substituições e permutações (normalmente em blocos de 64 ou 128 bits) para gerar um texto cifrado mais difícil de ser criptoanalisado[49].

Estes sistemas precisam resistir aos ataques brutos, ou seja, a tentativa de determinar a(s) chave(s) (uma para as simétricas e duas para os sistemas assimétricos) ou o processo de criptografia[50]. Segundo Bauchmann, existem ataques por força bruta, cujo sucesso depende da exaustão de tentativas, utilizando programas de computadores. Os tipos existentes são: ataque somente ao texto cifrado – o atacante, ou intruso, conhece apenas os textos cifrados e tenta descobrir a chave ou recuperar os textos claros; ataque ao texto comum conhecido, onde conhece o par de textos, ou seja, o cifrado e o texto claro; ataque ao texto comum selecionado – o intruso consegue cifra textos claros, mas desconhece a chave e tenta descobri-la; ataque ao texto cifrado selecionado, onde consegue decifrar os textos, mas desconhece a chave[51]. Portanto, busca-se o sigilo perfeito da criptografia, que é a impossibilidade do intruso mesmo conseguindo o texto criptografado, decifrá-lo[52].

Com a atual capacidade e velocidade dos computadores a tecnologia dos sistemas criptográficos ou criptossistemas precisam aumentar sempre para manter seu sigilo perfeito. Por isso que em 2000 os Estados Unidos alteraram o padrão que utilizam, o anterior foi adotado em 1977, o DES, e trocado pelo AES.

[49] STALLINGS, William. Cryptography and network security, p. 57 e 64.
[50] Os ataques por força bruta são conhecidos como criptoanálise, que é o ataque a criptossistemas.
[51] BUCHMANN, Johannes. Introdução à criptografia, p. 88 e 89.
[52] BUCHMANN, Johannes. Introdução à criptografia, p. 128.

O DES foi um padrão de chaves simétricas (apenas uma chave de 56 bits), seu algoritmo foi comprovado, durante vários anos, ser forte a ataques, entretanto o tamanho de sua chave foi questionado desde o princípio. O DES é decorrente do algoritmo Lucifer desenvolvido pela IBM em 1971 que utilizava inicialmente chaves de 128 bits, porém como à época era inviável colocá-la apenas em um único chip foi substituída pela de 56 bits[53]. Apesar de questionado o tamanho da chave e também o fato de sua estrutura interna de funcionamento ser amplamente conhecida, foi um algoritmo que rapidamente se espalhou.

Em 1994 o NIST (*National Institute of Standards and Tecnology*), divisão do Departamento de Comércio dos Estados Unidos, órgão do governo responsável pelas escolhas de padrões técnicos, re-afirmou a utilização do DES por outros cinco anos. Em 1999 o NIST considerou a utilização do 3DES, o mesmo algoritmo que faria o processo de criptografia três vezes, apesar de sua segurança interna a chave continuava igual, suas transposições continuavam no mesmo padrão (64 bits) que não mantinha segurança suficiente, por isso o motivo de substituí-lo.

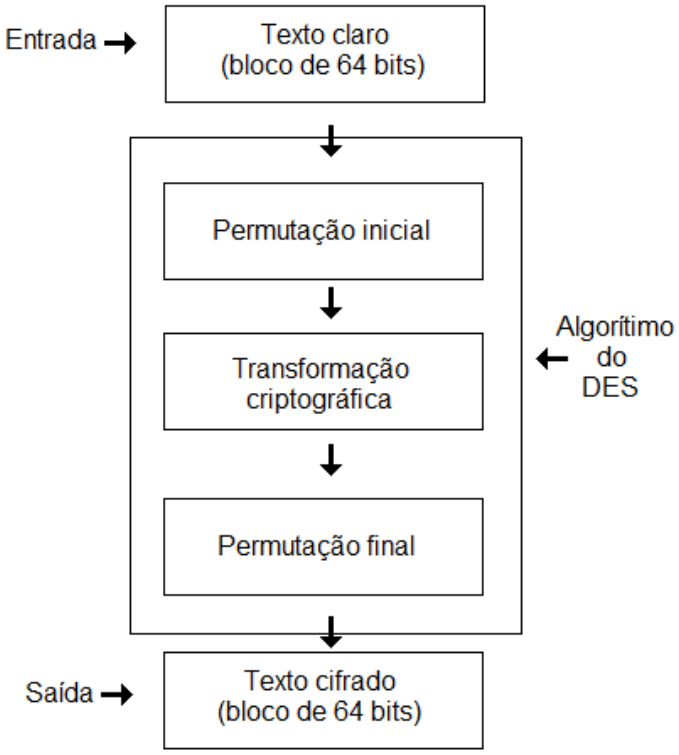

Figura 2.3

[53] STALLINGS, William. Cryptography and network security, p. 35.

Fonte: STALLINGS, William. Cryptography and network security

O AES foi colocado em uso prático em novembro de 2001. Ele é desenvolvido pela fórmula de *Rijndael*, e também é utilizado para os sistemas de chaves simétricas. Os padrões para a escolha do algoritmo baseou-se em sua segurança interna, ou seja, capacidade de criptoanalisar sua chave, que é no AES de no mínimo 128 bits; o tempo necessário para criptografar arquivos para ser utilizado em operações que demandasse rapidez, como *broadband*[54] *links*. E facilidade de implementação dos *hardwares*[55] e *softwares*[56] nas diversas máquinas, assim como o espaço demandado tanto no HD[57] quanto de memória RAM[58] .

Dessa forma, toda a sociedade conhece o padrão utilizado e sabe como ele cria suas chaves e seu processo de permutações e substituições. O que o torna atualmente impossível de ser quebrado é a dificuldade de descobrir as chaves utilizadas, tanto pela criptoanálise do algoritmo e, no caso das chaves assimétricas de determinar a chave privada a partir da pública.

> O desenvolvimento da criptografia por chaves públicas é o maior e talvez a única real revolução em toda a história da criptografia. [...] A criptografia por chaves públicas proporciona uma partida radical das que foram dadas anteriormente. Pois, o algoritmo é baseado em funções matemáticas e não em substituições e permutações. Mais importante, a criptografia por chaves públicas é assimétrica, envolvendo o uso de duas chaves separadas, em contraste ao sistema simétrico de cifração, que utiliza apenas uma chave[59].

O algoritmo responsável pela cifração no sistema de chaves públicas é o RSA. Seu processo de criptografia é distinto do DES e AES, pois não utiliza substituições e/ou permutações, mas fórmula matemática[60]. Para criar a estrutura de criptografia é necessário desenvolver várias variáveis (as chaves pública e

[54] Broadband é o mesmo que Banda Larga, uma forma de fornecimento de transmissão de dados para acesso à Internet.
[55] São os componentes físicos, placas que integram o computador.
[56] São os programas do computador,
[57] O disco rígido ou HD é o local onde os dados são salvos.
[58] Memória utilizada apenas enquanto a máquina está em funcionamento, quando desligada é totalmente apagada.
[59] STALLINGS, William. Cryptography and network security, p. 258.
[60] STALLINGS, William. Cryptography and network security, p. 262.

privada e, o algoritmo de criptografia) que sejam primas entre si e que no final a divisão entre elas seja um número inteiro igual a 1, ou seja, são números inteiros difíceis de quebrar. Quanto maior o número mais lento será a criptografia dos documentos, porém mais seguro será o processo[61].

Portanto, para criar as chaves e o algoritmo o processo é:

> 1. Escolher dois números primos grandes, *p* e *q*. [...]
>
> 2. Computar *n* = *pq* e *z* = (*p*-1)(*q*-1);
>
> 3. Escolher um número *e* menor do que *n* que não tenha fatores comuns (exceto o 1) com *z*. *e* e *z* são primos entre si.[...]
>
> 4. Achar um número *d*, tal que *ed*-1 seja exatamente divisível (isto é, que não haja resto na divisão) por *z*. Em outras palavras, dado *e*, escolhemos *d* tal que o resto da divisão *ed* por *z* seja o número inteiro 1.
>
> Portanto, a chave pública que estará disponível a todos é o par de números (*n,e*) e a chave privada o par (*n,d*)[62]

Ou seja, para conseguir descobrir uma taxa em função da outra é necessário o valor de “p” e “q”, pois apenas com a chave pública (“n”, “e”) torna-se inviável descobrir “d”.

O tamanho das chaves, juntamente com “p” e “q”, são as variáveis fundamentais para o sucesso do algoritmo. Por isso, para empresas aconselha-se utilizar chaves de 1024 bits e para pessoas físicas de 768 bits. Segundo a *RSA Data Security* responsável pelo modelo de funcionamento das chaves, uma chave de 512 bits criptografa numa velocidade de 21,6 Kbytes por segundo, enquanto a de 1024 bits a 7,4 Kbytes por segundo. “O DES é, no mínimo cem vezes mais veloz em *software* e entre mil e dez mil vezes mais veloz em *hardware*”[63], o que faz com que muitas vezes diferentes tipos de chaves sejam utilizadas em conjunto. Isso ocorre quando se utiliza o sistema de chaves públicas apenas para

[61] BAUCHMANN, Johannes. Introdução à criptografia, p. 132.
[62] KUROSE, James e ROSS, Keith. Redes de computadores e a Internet: uma nova abordagem, p. 451.
[63] KUROSE, James e ROSS, Keith. Redes de computadores e a Internet: uma nova abordagem, p. 452.

passar de forma segura uma chave simétrica que será utilizada doravante para a troca de informações, dessa forma utiliza-se um meio seguro apenas para a troca da nova chave, pois esta consegue cifrar com mais rapidez.

Portanto, a escolha das chaves decorre da necessidade que cada usuário verifica, pois diferentes funções demandam diferentes níveis de segurança. Dessa forma, o conhecimento das vantagens e limites de cada tipo de chave é relevante para entender a escolha brasileira pelas chaves públicas.

2.1.3 – Chaves públicas e privadas

As chaves são os códigos que iniciam o processo de cifração ou decifração. A qualidade, ou seja, o modo como ocorrerão os processos depende do tamanho da chave. Quanto maior a chave (em bits) melhor será a cifração do texto claro, mais difícil de quebrá-lo. A dificuldade para quebrá-lo, no sistema de chaves simétricas – DES e o AES –, depende da obtenção de dados suficientes que permitam descobrir a seqüência de permutações e substituições ou para o sistema tentar por força bruta determinar a chave utilizada. Já no sistema de chaves públicas é necessário a impossibilidade de determinar a chave privada a partir da respectiva chave pública e também a proteção das demais variáveis.

O sistema simétrico necessita de total proteção da chave, pois a mesma chave é capaz de cifrar e decifrar as mensagens. Dessa forma, a garantia de que os arquivos ou mensagens trocados não foram visualizados como texto claro – a integridade dos mesmos – decorre da plena segurança das chaves. Para este tipo de sistema é importante que a troca de chaves ocorra de forma segura, por um canal que seja extremamente difícil de ela ser interceptada, ou seja, seria totalmente desaconselhável que fossem trocadas pela Internet. Portanto, trata-se de um sistema que a chave não pode ser compartilhada, por exemplo, dentro de um setor de uma empresa. Ela deverá ser restrita apenas quem irá utilizá-la. Mas este tipo de sistema é extremamente mais veloz que o de chaves públicas, pois o algoritmo demanda menos recursos técnicos dos computadores, o que beneficia seu uso.

O sistema de chaves públicas, entretanto, mantém qualidades e características extremamente vantajosas. Apesar das duas chaves cifrarem e decifrarem as mensagens, apenas é possível decifrar a mensagem com o par da chave, ou seja, a mensagem cifrada com a chave pública só poderá ser decifrada pela chave privada e vice-versa. Desta forma, a segurança é aumentada desde que seja impossível determinar uma chave em função de outra. Esse sistema também permite conhecer se o texto recebido é o mesmo que fora enviado, ou seja, se sua integridade foi mantida.

2.1.3.1 – Função de *Hash*, Integridade e Assinatura Digital

A capacidade de garantir a veracidade dos documentos trocados, que o arquivo ou mensagens intercambiadas não foram alterados decore da função de *hash*. Ela é um algoritmo que transforma um texto em tamanho variável em uma seqüência final de tamanho determinado. Ou seja, se o texto claro for de 1024 bytes ou de 512 bytes ambos no final sairão cada um com uma seqüência de 16 ou 20 bytes[64].

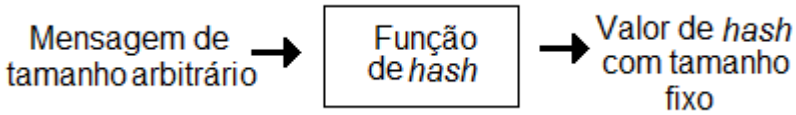

Figura 2.4

Fonte: STALLINGS, William. Cryptography and network security

> É importante perceber que as chances de duas mensagens quaisquer resultarem em um mesmo valor de *hash* pode ser considerada desprezível. Pode parecer paradoxal, mas é mais fácil encontrar duas mensagens que resultem em um *hash* de mesmo valor do que achar uma mensagem que resulte um *hash* de valor determinado. [...] Assim quantos valores randômicos de *hash* de 64 bit você tem de gerar para encontrar um que resulte um *hash* para um valor particular? 2^{64} ou aproximadamente 10^{19}. Quantos valores randômicos de *hash* de 64 bit você tem de gerar para achar dois que resultem um *hash* de mesmo valor? 2^{32}.[65]

[64] PUTTINI, Ricardo e SOUSA JUNIOR, Rafael. P. 50
[65] PUTTINI, Ricardo e SOUSA JUNIOR, Rafael. P. 50

Ela é utilizada, pois, ademais de sempre ter como saída (resultado do algoritmo) uma seqüência pequena de dados, essa seqüência modifica-se drasticamente em função de pequenas alterações como a inserção de um espaço dentro de um texto, ou da troca de uma letra[66], além de ser desprezível a possibilidade de duas mensagens possuírem propositadamente o mesmo resultado de *hash*. Dessa forma o resumo da mensagem enviado deverá ser comparado ao resumo da mensagem que o destinatário mandará produzir ao receber o arquivo, verificando se não foi alterado. Por meio da função de *hash* torna-se legalmente impossível alegar que determinado arquivo, com tal conteúdo não foi enviado.

Essa função é considerada uma função lixo, pois o arquivo de origem não pode ser recuperado do resultado da saída. Ela é apenas um comparativo para atestar que o arquivo enviado não foi modificado, entretanto, caso o texto cifrado – o que tiver sido enviado – for deletado é impossível recuperá-lo pelo resumo da mensagem (resultado da saída).

A integridade é, portanto, atestada pela comparação entre a função de *hash* enviada junto ao texto cifrado e a função de *hash* que será calculada pelo receptor da mensagem. Caso o resultado seja igual, a mensagem não foi alterada. Ele deverá ser utilizado para o envio de qualquer arquivo. Porém para os extremamente longos cujo conteúdo, caso seja interceptado, possa ser visualizado como texto claro, torna-se a garantia ideal. Ou seja, ao invés de criptografar tanto o texto claro quanto a função de hash, cifra-se apenas esta. Dessa forma o processo de criptografia é mais rápido e a segurança do conteúdo, em termo de integridade, é mantida. É justamente a cifração da função de *hash* que caracteriza a assinatura digital, pois permite assegurar que o texto que será visualizado é integro.

[66] ITI. O que é certificação digital?, p. 6. Disponível em: http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf Acesso em: 10 de abril de 2009.

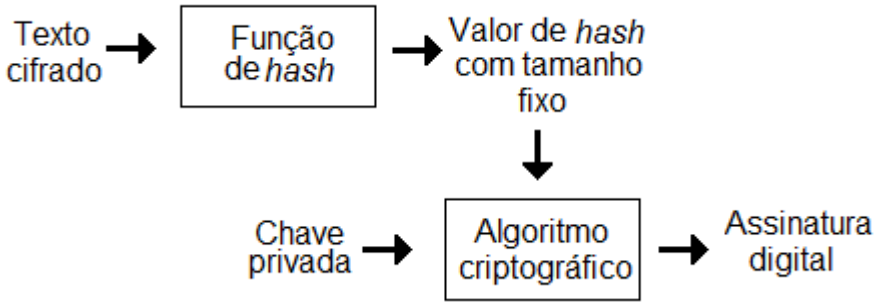

Figura 2.5

Fonte: ITI. O que é certificação digital?

Dessa forma a comparação entre os resultados de *hash* ocorrerá:

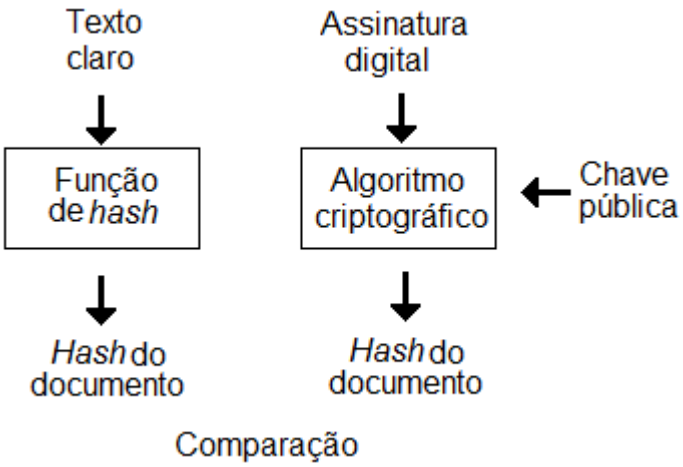

Figura 2.6

Fonte: ITI. O que é certificação digital?

Outra característica do sistema de chaves públicas é a autenticação. Quando o texto é cifrado a partir da chave privada de alguém, fica legalmente comprovada a autenticação da pessoa, pois apenas ela tem acesso a sua chave, assumindo por tanto todos os aspectos legais do documento enviado. A segurança e a validação do processo de assinatura digital são garantidas pelos certificados digitais.

2.1.3.2 – Certificados Digitais e Autenticidade

Da mesma forma que para documentos impressos quanto se deseja colher a assinatura de alguém precisa do reconhecimento de firma em cartório, para os

documentos eletrônicos o Instituto Nacional de Tecnologia (ITI), autarquia federal responsável pela gestão da ICP-Brasil, garante o mesmo processo. Quando a pessoa física ou pessoa jurídica deseja fazer seu cadastro e conseguir sua assinatura digital a AC[67] requisitante faz um certificado digital, que é o documento on-line para ser visualizado e conferido por terceiros. Ele contém informações sobre o responsável pela chave o qual o documento foi criptografado, dessa forma garante-se que quem a assinatura do documento.

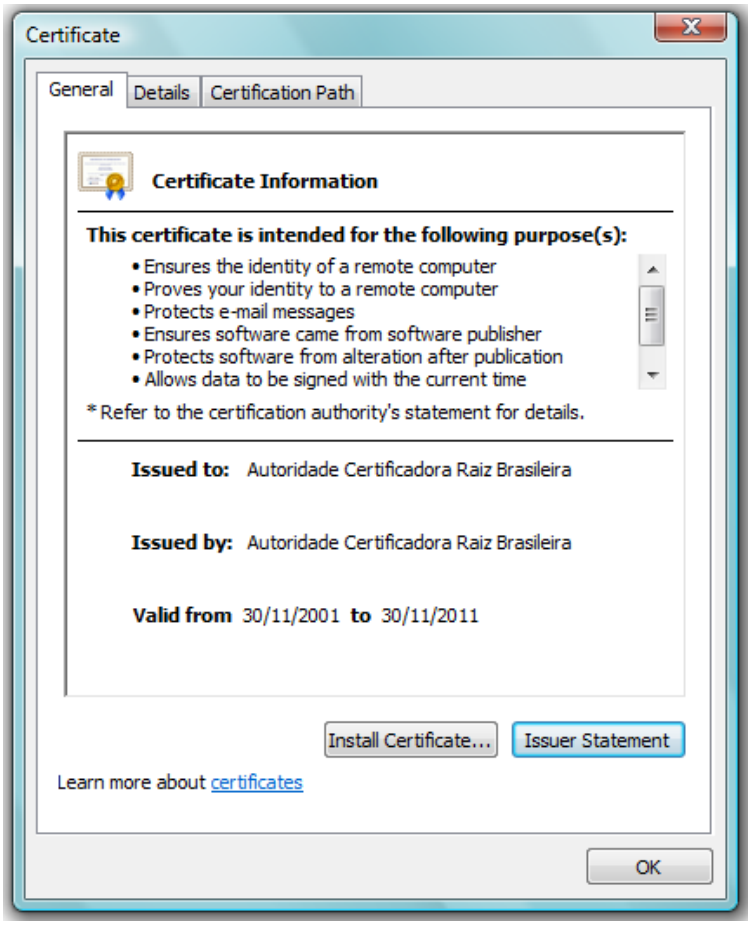

Figura 2.7

Fonte: ITI.

Entretanto o processo de autenticidade só é possível de ser comprovado para as cifrações feitas pela chave privadas e não pela pública. Portanto, normalmente fazem-se duas cifrações de documentos. Os arquivos cifrados pela chave privada assumem as responsabilidades legais de quem o assina,

[67] Autoridade Certificadora

entretanto ele poderá ser decifrado por quem possuir a respectiva chave pública. Enquanto os arquivos cifrados por chaves públicas só poderão ser decifrados pelas respectivas privadas[68]. Dessa forma ocorrem duas cifrações, a primeira com a chave privada do remetente e a segunda com a chave pública do destinatário. Assim, apenas o destinatário possuidor da chave privada referente à pública poderá ter acesso à informação trocada, mantendo a certeza de que ela veio do remetente, pois estará cifrada com a chave privada do mesmo.

Para algumas empresas, como por exemplos de vendas on-line, não é relevante saber quem é o comprador, apenas proteger as informações dele. Elas utilizam esse sistema, quando ocorre a compra, as informações – especialmente numero do cartão de crédito – são repassadas, sem mesmo o comprador saber, cifradas à empresa[69]. Por meio da chave pública, que demandará a chave privada da empresa, impedindo que os dados sejam interceptados e visualizados por terceiros e não demanda nenhum esforço de quem está fazendo compras on-line. É, portanto uma utilização que cada dia aumenta, sem que os usuários desses sites saibam como e o quanto suas informações são mantidas confidenciais.

Os certificados digitais, ao contrário de documentos como CPF ou documento de identidade, possuem uma data de vigência que poderá ser renovada quando necessário. Este processo é uma medida de segurança, pois as renovações demandam a troca da chave privada; além de permitir a atualização dos dados do usuário. A renovação pode ocorrer antes que ele venha a expirar, permitindo a continuação ininterrupta de funcionamento. O ITI disponibiliza de forma pública a Lista de Certificados Revogados (LCR), expedida por cada Autoridade Certificadora (AC), dessa forma há como conferir se o certificado continua válido.

---

[68] ITI. O que é certificação digital, p. 5. Disponível em: http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf Acesso em: 10 de abril de 2009.

[69] É utilizado normalmente a SSL (Secure Sockets Layer) desenvolvida pela Netscape que cifra dados e autentica a relação entre um cliente e um servidor Web ou o SET (Secure Eletronic Transactions) desenvolvido pela Visa Internacional e a MasterCard Internacional que criptografa apenas tipos específicos de dados relacionados a cartões de pagamentos. KUROSE, James e ROSS, Keith. Redes de computadores e a Internet, p.475 e 478.

Após a expiração do certificado é impossível assinar documentos, mas pode conferir as assinaturas realizadas mesmo quando ele não está mais em uso. Isso decorre da possibilidade de agregar elementos de data e hora a todos os documentos assinados, que é conhecido como carimbo de tempo que é emitido pela Autoridade de Carimbo de Tempo (ACT). A regulamentação final ocorreu na reunião do Comitê Gestor (CG) da ICP-Brasil em novembro de 2008.

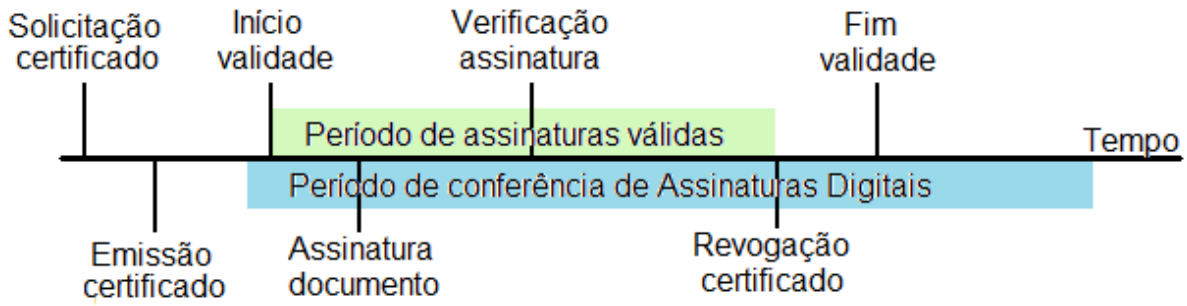

Figura 2.8

Fonte: ITI. O que é certificação digital?

O ITI é o responsável pela segurança da ICP-Brasil e conseqüentemente de todos os elementos necessários ao funcionamento das Certificações Digitais, da fórmula criptográfica, da garantia temporal dos dados trocados. Entretanto o modelo brasileiro não é o único existente na sociedade internacional, cada Estado possui liberdade para escolher seus padrões e modelos a serem seguidos por seus cidadãos.

2.2 – Os modelos disponíveis

O modelo adotado pelo Brasil é apenas uma forma de estruturar o processo de criptografia pelo mundo.

> Uma infra-estrutura de chaves públicas não é apenas um feixe de leis, mas todo um conjunto de regimes normativos, procedimentos, padrões e formatos técnicos que viabilizam o uso em escala da criptografia de chaves públicas em rede digital aberta. Estrutura o suporte para a tecnologia de chaves públicas, de forma a permitir o gerenciamento e controle do uso de chaves (assinaturas) e certificados digitais. A função

primeira de uma ICP, portanto, é permitir, por meio das autoridades certificadoras (AC), a distribuição e o uso de chaves públicas e certificados com garantia de segurança.[70]

O governo brasileiro comparou cerca de 70 modelos antes da decisão de criar o ITI e a ICP-Brasil[71], sendo os mais significativos o norte-americano e o europeu. A diferença marcante entre os dois é a presença do governo no processo. A decisão do governo brasileiro pelo atual modelo, assim como os motivos e processo de funcionamento da ITI serão vistos mais a frente.

2.2.1 – Estados Unidos, sistema privado

Os Estados Unidos mantém desde sua formação histórica a tendência de não intervenção pública em assuntos privados, com o sistema de criptografia a decisão percorreu o mesmo critério.

Em 1901 o governo norte-americano fundou o NIST que se responsabilizou pela padronização de sistemas que deveriam ser utilizados pelas agências governamentais, juntamente com a NSA (*National Security Agency*)[72]. A iniciativa privada começou a utilizar os mesmo padrões, não por exigência federal, mas pela segurança assumida, ou seja, por acreditar que o governo escolheria um padrão com excelência para a administração pública utilizar. Dessa forma que em 1977 o NIST decidiu pelo uso do DES[73] e em 2001 pelo AES em seu lugar[74]. Na década de 1990 houve a tentativa de criar um programa o *Capstone* que reuniria todas as informações de criptografia com chave simétrica de 80 bits, função de *hash*, assinatura digital com o algoritmo equivalente conhecido como *Clipper*, mas o projeto não saiu do papel.

A NSA funciona desde 1952 e atua em vários setores destas tecnologias, como na divulgação para o restante do país, na escolha dos padrões, bem como limitando ou incentivando as empresas. Ela possui a função de proteção do

[70] FILHO, Demócrito Reinaldo. A ICP-Brasil e os poderes regulatórios do ITI e do CG. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=7576. Acesso em: 05 de julho de 2009.
[71] BARRA, Marcelo. Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e a formação do Estado eletrônico, p. 49.
[72] Site NIST: http://www.nist.gov/public_affairs/general2.htm Acesso em: 06 de maio de 2009.
[73] STALLINGS, William. Cryptography and internet security, p. 73.
[74] Federal information. Processing Standards Publication 197. Disponível em: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf Acesso em: 06 de maio de 2009.

território americano contra forças externas e, tem mandato específico para lidar com as comunicações. O interesse da NSA é decodificar as comunicações estrangeiras que sejam importantes para a manutenção da segurança norte-americana e impedir a utilização de métodos criptográficos fortes pelos considerados inimigos nacionais.[75] Dentro da agência está o CSS (*Central Security Service*) serviço especializado na utilização da criptografia para fins militares, um dos responsáveis pela proteção do território norte-americano[76].

Depois do fim da guerra fria e da queda da União Soviética[77] foi colocada em cheque, pelas empresas que trabalham com criptografia e desejavam fazer uso comercial de suas habilidades, a política adotada pela agência. Até o ano 2000 os Estados Unidos possuíam uma legislação extremamente restritiva às exportações de computadores, estes não poderiam ser criptograficamente superiores a 56 bits para DES e 512 bits para RSA, ambas as configurações capazes de serem criptoanalisadas pela NSA. A redução do controle sobre a capacidade criptográfica dos computadores exportados ocorreu apenas para exportações voltadas a empresas e sociedade civil. As relações comerciais com outros governos ou para Estados que os norte-americanos possuem embargos – como Cuba, Irã, Síria, Iraque, Coréia do Norte – não poderão ocorrer. A função da NSA neste caso é de avisar ao BXA (*Bureau of Export Administration*) quaisquer suspeitas relacionadas ao tema.

A real preocupação da agência de segurança norte-americana é o desenvolvimento privado dessas tecnologias, que possa cair em mãos erradas e seja impossível o controle e a proteção dos Estados Unidos, o que é feito pela quebra dos códigos de comunicações dos demais países. Ou seja, não há o interesse em criar uma autoridade pública para autenticar documentos ou em criar um controle centralizado; e sim de, por meio das leis, limitar as ferramentas e sistemas possíveis de serem utilizados por empresas, de forma que as agências federais estejam sempre um passo a frente na tecnologia disponível. Além do

[75] SCHNEIER, Bruce. Applied cryptography, p. 597 e 598.
[76] Site do CSS. Disponível em: http://www.nsa.gov/about/central_security_service/index.shtml Acesso em: 06 de maio de 2009.
[77] Durante a Guerra Fria, especialmente no episódio da Crise dos Mísseis em Cuba, a NSA/CSS teve grande participação na busca de informações por meio da criptografia. Disponível em: http://www.nsa.gov/about/cryptologic_heritage/index.shtml Acesso em: 06 de maio de 2009.

aparato legal a NSA possui um poder de influência, pois é um dos maiores clientes dessas companhias.

Apesar de não haver a segurança pública dos documentos assinados, existe uma vantagem em trabalhar-se com a iniciativa privada. A possibilidade de desenvolvimento cresce, pois as empresas precisam, devido à concorrência, desenvolver seus *softwares, hardwares* e sistemas criptográficos para melhor atender a demanda. O fato de o órgão responsável ser um dos clientes mais ativos das principais empresas possui o aspecto positivo de demandar, quando necessário e para um número alto de máquinas (todo o governo federal americano), a qualidade de seus sistemas; porém causa uma pressão para que seus padrões sejam seguidos, ou seja, um constrangimento de desenvolver-se segundo as exigências e desejos do NSA.

Portanto, o modelo americano é regido pelas empresas privadas que seguem as normas ditadas pela NSA e também por sua influência econômica. A legislação nacional não se responsabiliza pelos documentos criptografados, mas estes também são considerados como legalmente imputáveis pelos tribunais norte-americanos

Dessa forma o sistema adotado pelo Brasil diferencia-se do modelo norte-americano, ficando muito mais próximo ao sistema europeu.

2.2.2 – União Européia, sistematização européia

Enquanto os Estados Unidos desenvolveram um sistema totalmente privado de criptografia, tanto para o governo quanto para a iniciativa privada, a União Européia lançou as bases para um sistema regido por normas públicas com o trabalho conjunto de várias empresas privadas. Assim seu objetivo não era criar um sistema público, semelhante ao brasileiro, mas legislar sobre como deveria funcionar em nível macro (europeu) os diversos sistemas adotados por cada membro.

A União Européia é o resultado de uma série de tratados bilaterais e multilaterais assinados pelos vários Estados europeus. Ele se iniciou em 1951

com o tratado da Comunidade do Carvão e do Aço (CECA) entre Alemanha, Bélgica, França, Itália, Luxemburgo e Países Baixos. Após, em 1957 foi assinado o Tratado de Roma que criou a Comunidade Econômica Européia (CEE). E em 1993, já contando com 12 membros efetiva-se a União Européia (UE) por meio do tratado de Maastricht, que atualmente conta com 27 membros: Alemanha, Áustria, Bélgica, Bulgária, Dinamarca, Eslovênia, Espanha, Estônia, Finlândia, França, Grécia, Holanda, Hungria, Irlanda, Itália, Letônia, Lituânia, Luxemburgo, Malta, Portugal, Polônia, Eslováquia, Chipre, Reino Unido, República Tcheca, Romênia, Suécia[78].

Essa estrutura governamental envolveu a criação de uma série de instituições[79] políticas e jurídicas que permitam uma gestão eficiente do bloco, baseando-se na estrutura de três pilares da União. Seus pilares são: o Comunitário que se refere aos Tratados que formam a União Européia, o da Política Externa e Segurança Comunitária e o da Justiça e Assuntos de Interior. Dentre eles o da segurança comunitária é o que melhor explica as resoluções do Parlamento sobre a criptografia. No documento emitido por esta instituição fica evidente a associação entre a criptografia como uma forma de proteção de atividades econômicas. Além disso, relaciona a segurança de dados proporcionada pela assinatura digital e o sistema de chaves públicas com questões de espionagem internacional e mesmo de trabalho conjunto entre as diversas polícias secretas. Dessa forma faz uma análise semelhante as do NIST e NSA norte-americanos[80].

> Entretanto, a Europa, no segmento econômico sofre com a diversidade legislativa: a existência de regras divergentes quanto ao reconhecimento legal das assinaturas

[78] Livro azul 2008 da cooperação da união Européia no Brasil, p. 6. Disponível em: http://www.delbra.ec.europa.eu/pt/downloads/book%20livro%20azul%202008%20completo.pdf Acesso em: 03 de maio de 2009.

[79] Comissão Européia que elabora propostas legislativas, é a guardiã dos tratados e executa as políticas comunitárias. O Parlamento europeu composto por deputados eleitos em todos os Estados-membros com capacidade legislativa juntamente com o Conselho. Conselho Europeu é formado pelos chefes de Estado que define as linhas políticas gerais da União. Conselho de Ministros é formado por ministros das respectivas áreas de atuação se encaixa no pilar de Política Externa e Segurança Comum. Tribunal de Justiça Europeu detém o monopólio de interpretação das normas de Direito Comunitário. E o Tribunal de Contas que se responsabiliza pela averiguação do orçamento e contas da União Européia. Disponível no site da Comissão Européia no Brasil: http://www.delbra.ec.europa.eu/pt/about_us/4.htm Acesso em: 24 e agosto de 2009.

[80] Eurpean Parliament. Temporary Committe on the ECHELON Interception System. P, 8.

> electrónicas e à acreditação dos prestadores de serviços de certificação nos Estados-Membros pode criar um obstáculo importante à utilização das comunicações electrónicas e do comércio electrónico,dificultando assim o desenvolvimento do mercado interno; por outro lado, a existência de um quadro comunitário claro para as assinaturas electrónicas reforça a confiança e a aceitação geral das novas tecnologias[81].

O tema desperta maiores dificuldades e importância para a região devido a diversidade jurídica e quantidade de países. Cada Estado, em sua legislação, prevê limitações, usos e instituições públicas e privadas (segundo o caso) para atuar nesta relação. O relatório, de 1999, da *Global Internet Liberty Campaing* mostra essa diversidade, por exemplo, a Alemanha não concordava com a adoção de restrições a exportações de equipamentos que contenham capacidade criptográfica; enquanto a França estava alterando suas normas que a isolavam na questão criptográfica, pois permitia apenas a utilização de chaves com até 56 bits. Neste mesmo período a Espanha começou a lançar bases para um controle governamental sobre as empresas que criam produtos que demandavam essa tecnologia[82]. Portanto, era importante que o Parlamento europeu chegasse a um ponto em comum, criando regras sobre o tema. Sua função não era criar uma instituição como a ICP-Brasil, mas um corpo normativo que delineasse o caminho e os limites que cada membro teria para legislar sobre o tema.

> A presente directiva não procura harmonizar a prestação de serviços no que diz respeito à confidencialidade da informação quando estes são abrangidos por disposições nacionais em matéria de ordem pública ou de segurança pública[83].

Dessa forma são três leis que tratam sobre o tema na União Européia a Diretiva 1999/93CE, a Decisão da Comissão de 6 de novembro de 2000[84] e a

---

[81] Diretiva 1999/93CE. Disponível em: http://www.scee.gov.pt/NR/rdonlyres/B1436BD4-3892-40D6-8C16-7993D14990C3/0/directiva199993EC_PT.pdf Acesso: 22 de agosto de 2009.

[82] Eletronic Privacy Information Center. Cryptography and liberty 1999: an international survey of encryption policy. Disponível em: http://gilc.org/crypto/crypto-survey-99.html Acesso em: 03 de maio de 2009.

[83] Diretiva 1999/93CE. Disponível em: http://www.scee.gov.pt/NR/rdonlyres/B1436BD4-3892-40D6-8C16-7993D14990C3/0/directiva199993EC_PT.pdf Acesso: 22 de agosto de 2009.

[84] Especifica as características da entidade (pública ou privada) responsável pela avaliação das empresas atuantes no setor. Disponível em: http://www.scee.gov.pt/NR/rdonlyres/B7C0AD7E-927D-4A79-BF8C-957359B4E6CB/0/DecisaoDaComissao_6Novembro2000.pdf Acesso em: 22 de agosto de 2009.

Decisão da Comissão de 14 de julho de 2003[85]. A primeira norma, do Parlamento, refere-se à liberdade de cada Estado-membro de legislar e controlar o tema. Entretanto, é resguardado o direito a concorrência e bem como a empresas privadas prestarem o serviço.

> Deve existir a possibilidade de os serviços de certificação serem prestados tanto por uma entidade pública, como por uma pessoa singular ou colectiva, quando estabelecida nos termos da legislação nacional[86] .

> E mantém a imputabilidade de assinaturas digitais: a liberdade de as partes acordarem entre si os termos e condições em que aceitam dados assinado electronicamente deve ser respeitada, dentro dos limites permitidos pela lei nacional; as assinaturas electrónicas utilizadas no âmbito de tais sistemas deverão produzir efeitos legais e ser admitidas como meios de prova em processos judiciais[87].

Portanto, a União Européia por meio desta diretiva cria a base de seu sistema de chaves públicas caracterizado pela responsabilidade de cada Estado-nacional que deverá observar a necessidade de correspondência entre os vários sistemas privados disponíveis.

Essa consolidação jurídica que caracteriza a proximidade com o Brasil, já que mesmo se tratando que modelos distintos quanto a participação pública (aqui reside um monopólio estatal), ambos são consolidados em aspectos legais que garantem a imputabilidade da assinatura digital. Outra semelhança é a utilização deste sistema pela burocracia de cada Estado:

> As assinaturas electrónicas serão utilizadas no sector público no âmbito das administrações nacionais e comunitárias e nas comunicações entre essas administrações, assim como com os cidadãos e os operadores económicos, por exemplo em contratos

[85] Apresenta as normas técnicas que deverão nortear as empresas de criptografia. Disponível em: http://www.scee.gov.pt/NR/rdonlyres/DCA14039-00D6-4AB4-8F56-72F8258FF83A/0/DecisaoComissao_20030714.pdf Acesso em: 22 de agosto de 2009.
[86] Diretiva 1999/93CE. Disponível em: http://www.scee.gov.pt/NR/rdonlyres/B1436BD4-3892-40D6-8C16-7993D14990C3/0/directiva199993EC_PT.pdf Acesso: 22 de agosto de 2009.
[87] Diretiva 1999/93CE. Disponível em: http://www.scee.gov.pt/NR/rdonlyres/B1436BD4-3892-40D6-8C16-7993D14990C3/0/directiva199993EC_PT.pdf Acesso: 22 de agosto de 2009.

> públicos, em matéria de sistemas de fiscalidade, de segurança social, de saúde e judiciário[88].

Essa Diretiva também prevê que haja cooperação internacional no sentido de haver interoperabilidade dos diversos tipos de criptografia existentes. Este intuito decorre da percepção que o comércio eletrônico cresce ao longo dos anos. O modelo brasileiro aproxima-se do europeu, pois dentre os vários pesquisados possui uma amplitude geográfica significativa e previamente propõe uma "conversação" com outros modelos existentes além de focar numa legislação prévia. Essas características são as responsáveis pela escolha brasileira.

2.2.3 – A escolha brasileira

A estrutura nacional de criptografia é o resultado da conversão de diversos fatores distintos entre si como (necessidade de melhorar a segurança do próprio governo, pressão de setores econômicos, segurança nacional mantida pela possibilidade de controlar o que é criptografado). Portanto, foi uma decisão pautada na satisfação de diversos interesses que demandam particularidades. Na busca do modelo a ser adotado pelo Brasil houve uma pesquisa das legislações de diversos países, em especial Estados Unidos e Europa, de forma a buscar, dentre os padrões adotados na sociedade internacional, um que pudesse vir ao encontro das necessidades locais. Essa coleta de informações contou com a colaboração de servidores dos governos, consultores, mas não se aproxima de um caso de cooperação internacional.

> O trabalho que a gente teve de fato, e onde sustentou meu trabalho, foi a legislação comparada, a legislação dos outros países. E depois de quando conhecida a legislação, eu fazia o contato com as pessoas nesses outros países.[89]

O conhecimento das legislações dos demais países é extremamente relevante para o desenvolvimento e melhoria das estruturas internas como escreve Godoy:

---

[88] Diretiva 1999/93CE. Disponível em: http://www.scee.gov.pt/NR/rdonlyres/B1436BD4-3892-40D6-8C16-7993D14990C3/0/directiva199993EC_PT.pdf Acesso: 22 de agosto de 2009.

[89] BARRA, Marcelo. Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e a formação do Estado eletrônico, p. 27.

> O estudo dos direitos estrangeiros aventa leitura do mundo, de costumes, de práticas. É fonte inegável de enriquecimento cultural. O exame de sistemas normativos de outros povos oxigena a musculatura intelectual, tempera a curiosidade, aguça a inteligência, eleva o espírito.[90]

A escolha pelo modelo europeu perpassa a própria estrutura do Direito adotado no Brasil. O Estado brasileiro pertence à família romano-germânica[91] que é caracterizada pela pré-existência de leis, normas para o devido funcionamento da sociedade. Dessa forma, toda ação será julgada pelas leis existentes no ordenamento jurídico nacional, o que demandou do Estado uma busca pela verificação do que existia previamente sobre o tema de criptografia nos demais países.

> O padrão britânico não bate com a Europa. O nosso comportamento sociológico-jurídico é mais próximo do europeu. Então vamos fazer o seguinte: 'Como isso é uma coisa nova, eu acho que se botarmos o padrão europeu não vai assustar ninguém e as pessoas terão facilidade de assimilação, porque nós estaremos fazendo uma coisa da maneira que sempre fizemos. E da maneira que estamos acostumados a fazer'.[92]

A proximidade jurídica é, portanto, a explicação e a razão pela escolha brasileira ter como foco o modelo europeu que se preocupa em legislar as ações dos Estados neste contexto. Isso traz à ICP-Brasil uma estabilidade e aceitação por parte dos usuários. Além do mais o modelo europeu permite uma interoperabilidade com os demais modelos existentes:

> Se nós entrarmos no modelo europeu, não estará fechada a comunicação nossa com os americanos e com os asiáticos. Quando eu faço um modelo tupiniquim aqui, eu

---

[90] GODOY, Arnaldo. Notas introdutórias ao Direito Comparado. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=10824 Acesso em: 04 de julho de 2009.

[91] "Divide-se o Direito mundial, basicamente, em três grandes 'famílias': a) romano-germânica (Direito Romano, que evoluiu principalmente pela influência da França, Alemanha e Itália); b) 'common law' (Direito Inglês, que ganhou maior impulso nos Estados Unidos, com contornos diferenciados); c) Direito dos países socialistas (que se iniciou na extinta União Soviética).

O Brasil, colonizado pelos portugueses, pertence à 'família' romano-germânica. Aqui, como em todos os países dessa 'família', a 'lei' (norma, regra geral, editada pelo Legislativo) é a principal fonte do Direito.

Os Estados Unidos da América, antiga colônia inglesa, pertentem à 'família' da 'common law', como já dito acima. Aí a 'jurisprudência' é a principal fonte do Direito". MARQUES, Luiz Guilherme. Direito Comparado e jurisprudência. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=1643 Acesso em: 04 de julho de 2009.

[92] BARRA, Marcelo. Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e a formação do Estado eletrônico, p. 27.

> talvez tivesse dificuldade de comunicação com o resto do mundo. O modelo europeu necessariamente terá que se comunicar com os americanos e, vice-versa. De saída nós vamos estar iguais aos europeus, o que não é nenhuma má companhia. (...) Se estivermos errando, estamos errando com a Comunidade Européia inteira.[93]

Nesse contexto que foi criada a ICP-Brasil, por meio da Medida Provisória 2200/01, seguida por suas edições a MP 2200-1/01 e pela MP 2200-2/01.

2.3 – A ICP-Brasil

A ICP-Brasil surgiu na idéia do governo eletrônico (ICP-Gov)[94] e, em sua concepção original, iria servir apenas a relações intra-governamentais. Ou seja, apenas a burocracia, a administração pública utilizaria esta ferramenta[95]. A modificação do alcance e a conseqüente formatação que pudesse atingir a sociedade civil, especialmente empresarial, ocorreu do trabalho da Febraban (Federação Brasileira de Bancos).

O setor bancário brasileiro movimenta bilhões de reais por seus serviços on-line, contando com um desenvolvimento em informática reconhecido internacionalmente e com uma pauta de cliente (numericamente) ampla[96]; e necessitava de uma ferramenta que garantisse o montante enviado, para quem, quando e por quem. E a forma mais segura seria utilizar uma ferramenta governamental que garantisse a veracidade dos dados trocados com a utilização da assinatura digital, bem como a responsabilização do titular da chave privada por seu acesso e segurança.

---

[93] BARRA, Marcelo. Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e a formação do Estado eletrônico, p. 49.

[94] A ICP-Gov foi normatizada pelo Decreto 3587/00 e depois revogada pelo Decreto 3996/01.

[95] IPEA. Na ultima pesquisa das razões para a melhoria da produtividade no serviço público decorre dos aprimoramentos tecnológicos; dentre eles de certificação digital. Notícia disponível em: http://www.iti.gov.br/twiki/bin/view/Noticias/PressRelease2009Aug21_202422 Acesso em: 24 de agosto de 2009.

[96] Segundo a Febraban, em 2001 existia 8,8 milhões de brasileiros com Internet Banking e em 2007 este número já alcançava 29,8 milhões. As despesas em tecnologia dos bancos foram de 14,869 milhões em 2007. E a quantidade de movimentação bancária com origem no Internet Banking passou de 729 milhões em 2001 para 6,163 bilhões em 2007. Fonte: Febraban. Disponível em: http://www.febraban.org.br/p5a_52gt34++5cv8_4466+ff145afbb52ffrtg33fe36455li5411pp+e/sitefebraban/informacoes_do_setor.pdf Acesso em: 05 de julho de 2009.

> 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.[97]

O Art. 6, parágrafo único rege o controle de chaves: “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”.[98]

Com a pressão da Febraban foi possível criar uma instituição que além de servir aos propósitos governamentais pudesse também auxiliar a sociedade além da esfera política:

> A ICP-Brasil, quando saiu por Medida Provisória, tinha por objetivo o nosso lado, o lado da iniciativa privada: era permitir que o contrato eletrônico tivesse validade jurídica e o maior ator era o setor bancário. Então o que a gente queria era encontrar um instrumento legal que na Justiça não nos trouxesse problemas. Documentos assinados a distância, não precisam estar frente a frente, só perante uma tecnologia.[99]

A instituição justifica o benefício para o cliente:

> A melhoria para o cliente foi muito maior com a tecnologia que os bancos deram, do que os lucros que os bancos tiveram. É lógico: eles não conseguiriam ter o lucro que tiveram se não tivessem feito o uso de tecnologia – mas o cliente passou a ganhar muito mais com aquilo. As facilidades que eles têm de poder acessar, conduzir os negócios dele, com muito menos ônus, muito menos burocracia, à distância, é um negócio inominável – não se paga isso aí.[100]

Dessa forma a ICP-Brasil pôde ser criada, conforme é atualmente conhecida, ganhando características de funcionalidade à esfera privada e mantendo o interesse do Estado em segurança. Esta se refere a duas instâncias distintas, a primeira da segurança da informação interna (era a idéia inicial da ICP-Gov) e, atribuída pelo atual formato da estrutura adotada no Brasil da segurança em relação a atividades criminosas.

---

[97] Art. 10, §1º da MP 2200-2.
[98] Art. 6, parágrafo único da MP 2200-2.
[99] BARRA, Marcelo. Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e a formação do Estado eletrônico, p. 36.
[100] BARRA, Marcelo. Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e a formação do Estado eletrônico, p. 39.

Os Estados são formados em duas diferentes instâncias uma interna e outra internacional. Ele é formado por um território, uma população e um poder centralizado aceito internamente e internacionalmente. Dessa forma o Estado possui em sua característica interna o direito de legislar sobre os diversos temas cabíveis a sua sociedade e de punir os que agirem em desrespeito a essas normas jurídicas. Neste sentido de instituição máxima, por meio das esferas de poder (Legislativo, Executivo e Judiciário), ele detém o direito de legislar sobre as tecnologias que serão utilizadas para a proteção de suas informações. Entretanto, o modelo adotado não possui somente defensores, desde sua criação a OAB do Brasil e a seção de São Paulo questionou a democracia que envolvia a decisão brasileira, como desenvolve Costa e Marcacini:

> Não bastasse atropelar com uma medida provisória, sem nenhuma urgência ou relevância, as discussões que a sociedade civil e o Poder Legislativo vêm travando há pelo menos dois anos sobre um tema novo, tormentoso, que guarda relação com variados ramos do Direito e que atinge diretamente ampla gama de interesses políticos e econômicos, o próprio conteúdo da Medida Provisória 2.200 cria um inaceitável centralismo de poderes e informações em um órgão cuja composição é monopolizada pelo Executivo Federal.[101]

A OAB também considera os resultados jurídicos do modelo brasileiro, pois ao "certificar chaves que assinam um documento eletrônico, é falar da prova documental", o que implica na capacidade de legislar toda a esfera jurídica – direito comercial, civil, administrativo, tributário, etc. – que possa vir a utilizar esta ferramenta[102].

Para corrigir a falta de democracia argumentada pela OAB, em julho foi emitida a uma nova MP, a 2200-1/01 que altera os artigos criticados[103], preservando as Instituições Democráticas brasileiras, e mantendo a centralização num só órgão. A decisão do governo de criar uma estrutura centralizada pode ser

[101] Da COSTA, Marcos e MARCACINI, Augusto. A urgência e relevância em violentar a Internet brasileira. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=2291 Acesso em: 05 de julho de 2009.
[102] Da COSTA, Marcos e MARCACINI, Augusto. A urgência e relevância em violentar a Internet brasileira. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=2291 Acesso em: 05 de julho de 2009.
[103] A MP 2200-1/2001 editou o conteúdo dos artigos 3.º; 5.º Incisos II IV; 6.º caput; 8.º, § único; 9.º e 12 §§ 1.º e 2.º.

explicada como uma forma última de o Estado manter um controle sobre os fluxos de informações e impedir a criminalidade nela envolvida.

Internamente o Estado possui como parâmetro a proteção dos membros da sociedade, ao tentar assegurar que o conteúdo trocado com a utilização da criptografia não seja criminoso ele está exercendo sua função. E internacionalmente o Estado visa e, neste aspecto torna-se a base da ICP-Gov, a proteção da informação armazenada dentro de sua estrutura política. Enquanto no âmbito doméstico ele é a instituição central, no internacional ele divide o cenário com outros atores, sendo os mais significativos os demais Estados. Dessa forma, a criptografia tenta impedir que as informações e documentos considerados como de segurança elevada[104] não sejam acessados por pessoas não autorizadas.

Portanto, a ICP-Brasil provém da idéia de assegurar as informações governamentais, aliada a noção de legalidade das informações trocadas. Este cenário da razão de estado encontrou um paralelo ao interesse privado o que permitiu que a ICP-Brasil pudesse atingir ao mesmo tempo as esferas públicas e privadas e para manter uma qualidade na promoção de suas funções foram definidos os princípios da ICP-Brasil.

2.3.1 – Princípios da ICP-Brasil

A ICP-Brasil, como será visto mais a frente, possui como autoridade gestora o Comitê Gestor da ICP-Brasil, um órgão vinculado à Casa Civil e que possui como membros tanto representantes do governo como da sociedade civil.[105] Este comitê criou um Termo de Referência que “surgiu da necessidade de

[104] O decreto 4553/02 define as qualidades das mensagens sigilosas, bem como seus níveis. E trata da utilização dos métodos de criptografia como forma de envio e recebimento desses documentos. Já o decreto 5301/04 define os níveis de segurança que os documentos oficiais se subdividem em: ultra-secreto, secreto, confidencial e reservado.

[105] BRUNO, Gilberto. Considerações sobre a criação da infra-estrutura de chaves públicas brasileira e seu comitê gestor. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=2310 Acesso em: 04 de julho de 2009.

definição de um arcabouço de normatização institucional que detalhasse as suas funções, atribuições, competências e organização funcional".[106]

Dessa forma, foram construídos nove princípios os quais devem ser observados na atuação da ICP-Brasil. O primeiro é o da Responsabilização, onde "a responsabilidade e a responsabilização dos proprietários, prestadores de serviço e usuários de sistemas de informação e outras partes envolvidas com a segurança dos sistemas de informação devem ser explicitas e documentadas".[107]

É seguido pelo Conhecimento que visa manter a informação ao alcance de todos os envolvidos no processo da ICP-Brasil – prestadores de serviços, usuários, proprietários – de forma que eles estejam sempre atualizados em relação aos sistemas normativos utilizados pela instituição, impondo a ICP-Brasil a divulgação de todas as decisões e atos que afetem os envolvidos. A Ética é o terceiro princípio que atua no sentido de manter estruturas de informação e de segurança dentro da ICP-Brasil que respeitem os direitos e interesses legítimos de todos.

As normas, regras e procedimentos da ICP-Brasil devem observar de forma adequada os vários pontos de vista como técnicos, administrativos, operacionais, comerciais, jurídicos, educacionais; esse é o quarto princípio da Multidisciplinaridade. Segue-se a Proporcionalidade sob o qual "a ICP-Brasil deverá contemplar níveis de segurança, normas, práticas e procedimentos compatíveis com a criticidade, a importância e o valor dos sistemas de informação que a utilizem, considerando-se os ambientes específicos envolvidos".[108]

---

[106] Presidência da República, Casa Civil. Termo de referência Comitê Gestor da ICP-Brasil: CG ICP-Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/consulta_publica/PDF/termodereferencia.pdf Acesso em: 04 de julho de 2009.

[107] Presidência da República, Casa Civil. Termo de referência Comitê Gestor da ICP-Brasil: CG ICP-Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/consulta_publica/PDF/termodereferencia.pdf Acesso em: 04 de julho de 2009.

[108] Presidência da República, Casa Civil. Termo de referência Comitê Gestor da ICP-Brasil: CG ICP-Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/consulta_publica/PDF/termodereferencia.pdf Acesso em: 04 de julho de 2009.

A harmonia e a coerência da segurança da informação disponível ao governo e à sociedade civil são possíveis pela integração e coordenação das normas, práticas e procedimentos da ICP-Brasil, que é o princípio da Integração. O princípio da Atualização, o sétimo, decorre das mudanças tecnológicas, exigindo da ICP-Brasil reavaliações periódicas de sua estrutura. O penúltimo princípio, a Escalabilidade refere-se ao crescimento da quantidade de usuários e alcance da ICP-Brasil e o último, a Interoperabilidade visa reduzir as incertezas em relação à integração com os demais sistemas de infra-estrutura existentes.[109]

Por meio desses princípios é possível desenvolver as normas, regras e procedimentos que verifiquem a efetiva utilização e funcionalidade da ICP-Brasil. Essa funcionalidade só poderá ser alcançada por meio da estrutura da ICP-Brasil.

2.3.2 – A estrutura da ICP-Brasil

A ICP-Brasil resulta da MP 2200-2 que estrutura o corpo funcional da instituição.

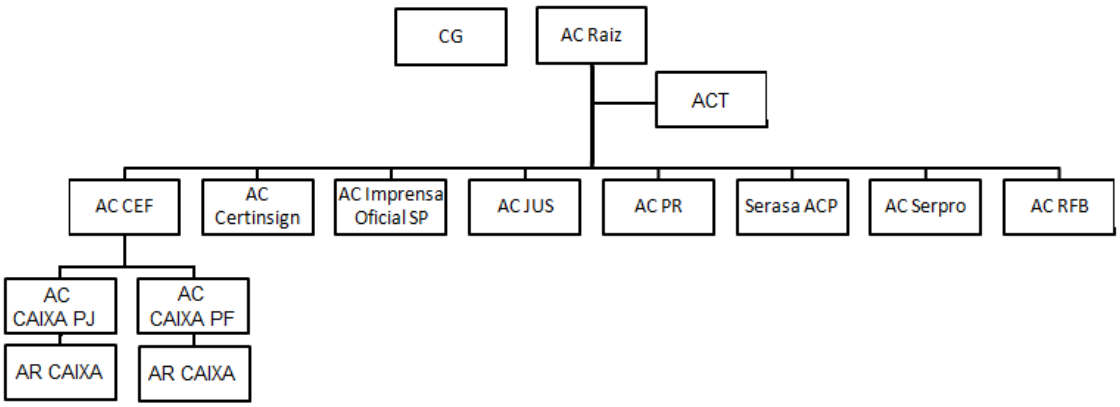

Figura 2.1[110][111]

[109] Presidência da República, Casa Civil. Termo de referência Comitê Gestor da ICP-Brasil: CG ICP-Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/consulta_publica/PDF/termodereferencia.pdf Acesso em: 04 de julho de 2009.

[110] O organograma foi produzido com base no apresentado pelo ITI no site: http://www.iti.gov.br/twiki/pub/Certificacao/EstruturaIcp/Estrutura_da_ICP-Brasil_-_site.pdf Acesso em: 05 de julho de 2009. Entretanto, a versão por eles produzida não trazem exemplo de AR, bem como a localização da ACT. Portanto, a Autoridade Certificadora de Tempo não se encontra definida no organograma da instituição, sendo este apenas uma amostra da possível localização que deverá assumir dentro da estrutura. As AR e AC foram colocadas apenas como exemplos didáticos, cada AC representada possui suas AC e AR.

Fonte: Autora

Apesar do organograma, por questões didáticas, não apresentar a totalidade de cada tipo de instituição, ele traz ao menos um exemplo da localização de cada uma das cinco. O Comitê Gestor (CG), a ACRaiz (Autoridade Certificadora Raiz), as AC (Autoridades Certificadoras), as AR (Autoridades Registradoras) – estas ficam abaixo das AC e devido seu elevado número não foram apresentadas na totalidade; e a Autoridade Certificadora de Tempo (ACT), é mais recente e não há ainda um organograma da instituição que informe sua exata localização.

Conforme o texto da MP, Artigo 3º, a ICP-Brasil possui como estrutura administrativa o Comitê Gestor da ICP-Brasil que é um órgão vinculado a Casa Civil da Presidência da República. Ele é composto por cinco representantes da sociedade civil designados pelo Presidente da República, além de um representante de um dos órgãos: Ministério da Justiça; Ministério da Fazenda; Ministério do Desenvolvimento, Indústria e Comércio Exterior; Ministério do Planejamento, Orçamento e Gestão; Ministério da Ciência e Tecnologia; Casa Civil e Gabinete de Segurança Institucional da Presidência da República.

A escolha pelo órgão a que se vincula foi estratégica e decorre da posição e função assumida pela Casa Civil. Ela é o órgão diretamente vinculado à Presidência e possui com função coordenar as diversas ações tomadas pelo governo, ela dispõe das ações horizontais, da interoperabilidade dos ministérios em torno das metas e objetivos delineados pelo governo.

> Você tem na Casa Civil uma instância de coordenação das ações do governo. Você tem Ministérios que têm políticas verticais, olhando cada um para o seu setor. Quem faz as integrações das políticas verticais é a Casa Civil. Essa é a lógica de você ter uma instância próxima ao poder principal do Presidente da República: de botar o governo para andar.[112]

[111] O organograma completo, mostrando as AR, se encontra no site do ITI, pelo endereço: http://www.iti.gov.br/twiki/pub/Certificacao/EstruturaIcp/Estrutura_completa.pdf Acesso em: 05 de julho de 2009.

[112] BARRA, Marcelo. Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e a formação do Estado eletrônico,

O Comitê Gestor (CG) possui a competência de coordenar a ICP-Brasil, estabelecendo as políticas, normas técnicas para o credenciamento das AC, AR e ACT. É responsável pelas atualizações da ICP-Brasil de modo a mantê-la em consonância com as demandas e desenvolvimentos tecnológicos, identificação de políticas de certificações externas, negociando acordos bilaterais e cooperando internacionalmente, observando os acordos internacionais adotados pelo Estado brasileiro. O CG também é o responsável pelas auditorias e fiscalizações da ACRaiz.[113]

Para seu devido funcionamento ele conta com uma Secretaria Executiva chefiada pelo presidente do ITI e pela Comissão Técnica Executiva (COTEC) sob a direção do Secretário-Executivo do Comitê Gestor. Além dos órgãos, está prevista reuniões em Plenário com todos os membros de forma da delinear a política e normatizar as regras da ICP-Brasil.

A ACRaiz, que é o ITI, é a primeira autoridade na cadeia de certificação, ela executa as decisões aprovadas pelo Comitê Gestor. Ela é a responsável por emitir os certificados das AC imediatamente subseqüentes a ela, além de auditá-las e fiscalizá-las. Segundo Pedro Rezende a ACRaiz por ser a primeira titular de emissão dos certificados, ela é a responsável por se auto-certificar. Em se tratado de outros modelos, onde não seja definido por lei o monopólio estatal, as empresas privadas atuantes no setor possuem acordos com as empresas criadoras de sistemas operacionais para que o auto-certificado esteja previamente disponível ao usuário. Essa associação permite que a chave pública da empresa certificadora, bem como seus certificados primários estejam ao alcance dos usuários[114]. Isso traz segurança ao certificado, pois há uma garantia que ultrapassa a própria instituição.

Quando é transmitido um dado criptografado, a única garantia de que a pessoa quem criptografou é realmente quem ela diz ser decorre do Certificado Digital emitido por terceiro. Ou seja, uma empresa se responsabiliza por garantir a

[113] Regimento Interno do Comitê Gestor da ICP-Brasil. Disponível em: http://www.iti.gov.br/twiki/pub/Main/ComiteGestor/Minuta_REG_INT_CG_ICP_BR_NOVA_VER_2_1.pdf Acesso em: 05 de julho de 2009.

[114] REZENDE, Pedro Antônio. Sobre a criação da ICP-Brasil. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=2705 Acesso: 05 de julho de 2009.

autoria das chaves por meio dos certificados, as AC (certificadas pela ACRaiz). Entretanto, esta mesma empresa necessita se auto-certificar, criar um certificado por ela e para ela e, neste momento, outrem poderia se passar por ela. Para evitar que isso ocorra que as empresas privadas se associaram aos produtores de sistemas operacionais, pois estes são essenciais para o funcionamento do equipamento; estes são os programas primários para que possa ser feita qualquer operação. Com a associação o computador já possui o certificado da empresa e quando demandado a conferência bastará o equipamento acessar seus dados, garantindo que o certificado auto-assinado da empresa seja válido.

> Segundo Rezende: os softwares que produzirão lavra e validação de assinaturas com valor legal, materializarão em sua lógica interna os protocolos que constituem o mecanismo autenticatório deste novo tipo de assinatura. Justamente o que mais precisa ser, de forma aberta e transparente, analisado, debatido, calibrado, revisado, justificado e integrado a outros mecanismos semelhantes hoje em operação no mundo virtual, ficará escondido, esacamoteado dentro da lógica de programas, hoje na sua grande maioria comercializados de forma totalmente opaca, com acesso público vedado à sua versão em "linguagem humana", em código fonte.[115]

A crítica conduzida à ICP-Brasil decorre do modelo brasileiro não possuir um sistema semelhante de associação, pois a ICP-Brasil possui licença para homologar os *softwares* que irá utilizar, ou seja, ela ao invés de colocar previamente seus certificados auto-assinados nos sistemas operacionais ela utiliza de *softwares* que precisam ser baixados pelos usuários, demandando uma confiança, sem garantia absoluta, de que o *software* bem como o certificado sejam verdadeiramente da ACRaiz.

As AC são entidades previamente certificadas pela ACRaiz que assumem a função de emitir aos titulares os certificados e o par de chaves – que deverá ser gerado pelo usuário, gerenciando os certificados e emitindo as listas de

[115] REZENDE, Pedro Antônio. Sobre a criação da ICP-Brasil. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=2705 Acesso em: 05 de julho de 2009.

certificados revogados[116]. Ela poderá, apenas quando previamente concedida pelo Comitê Gestor, emitir certificados a seus subseqüentes[117].

As AR possuem a função de identificar e cadastrar os usuários na presença dos mesmos, encaminhando suas solicitações a AC a qual está ligada. Elas, AC e AR, podem ser tanto entidades públicas quanto pessoas jurídicas de direito privado[118], por exemplo a AC OAB, AC Certisign e outras. Devido ao trato direto com o usuário e por sua responsabilidade em solicitar os certificados à AC, existe uma série de medidas de segurança em nível de pessoal (agentes de registro[119]) que busca impedir atos ilícitos. Essas medidas vão desde a impossibilidade de terceirização do serviço, dossiê de funcionários, treinamentos e acompanhamento constante no sentido de mantê-lo atualizado em níveis técnicos[120].

Portanto, no modelo adotado pelo Brasil, a sociedade possui seu principal contato com a estrutura da ICP-Brasil por meio das AR que fazem um cadastro, estes contam com uma data de validade, o que garante uma contínua atualização dos dados.

Os certificados digitais podem ser emitidos a pessoas físicas (nacionais e estrangeiros), bem como a pessoas jurídicas cujo CNPJ esteja válido.

Para as Pessoas Físicas a facilidade ocorre no envio de documentos e informações ao governo, por exemplo no envio da Declaração de Imposto de Renda Anual, na retirada de 2ª via de documentos enviados à Receita. Na modalidade de envio por Certificado Digital é aumentada a segurança e bem como a veracidade dos dados transmitidos. Enquanto às empresas a Assinatura Digital ganha relevância e mesmo destaque ao tratar principalmente da venda de mercadorias ao mercado externo.

---

[116] Artigo 6º da MP 2200-2/01.
[117] Artigo 9º da MP 2200-2/01.
[118] Artigos 7º e 8º da MP 2200-2/01.
[119] Pessoa responsável pela execução das atividades inerentes à AR. É a pessoa que realiza a validação e a verificação da solicitação de certificados.
[120] ICP-Brasil. Características mínimas de segurança para as AR da ICP-Brasil: DOC-ICP-03.01. Disponível em: http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-03.01_-_v_1.2.pdf Acesso em: 07 de julho de 2009.

O atual modelo brasileiro de pagamentos funciona com base nos certificados digitais e facilita pela conferência das informações. Outro destaque é o Siscomex, programa eletrônico utilizado para o preenchimento e emissão de documentos necessários à exportação e à importação de produtos. Atualmente ele funciona integrado à ICP-Brasil e facilita a vida das empresas que possuem o certificado. Dessa forma, a Receita Federal Brasileira criou o e-CAC (Centro de Atendimento Virtual ao Contribuinte) que dá acesso on-line a documentos sobre tarifas e pagamentos efetuados junto à Receita Federal do Brasil[121].

O processo de solicitação tende a ser relativamente simples, entretanto demanda a conferência das informações ao longo do tempo. Ou seja, de tempos em tempos é solicitado a apresentação física do detentor do certificado. Essa manutenção de contato físico é relevante, pois ainda não há um sistema desenvolvido de revogação de certificados, por exemplo em casos de falecimento. Este tema de revogações e mesmo da temporariedade envolvida nessa checagem de dados foi tema das últimas reuniões do CG[122].

A intenção do CG é emitir um Certificado Digital para cada brasileiro, algo semelhante ao Documento de Identidade, neste caso virtual. Esse projeto é do Instituto Nacional de Identificação, entretanto, há um longo caminho a ser percorrido para isso[123]. O CG necessita finalizar a criação de toda sua cadeia de funcionamento e garantir a manutenção da qualidade tecnológica da criptografia para poder galgar caminhos tão significativos.

A estrutura da ICP-Brasil é criticada pelo monopólio, pois este tende a reduzir a possibilidade de desenvolvimento de tecnologia, já que a concorrência é um fator importante na busca da qualidade. Esta é representada pela capacidade de impedir que dados sejam visualizados e alterados, a ICP-Brasil possui uma estrutura criptográfica eficiente. Ou seja, mesmo não tendo concorrência

[121] Receita Federal do Brasil. Disponível em: http://www.receita.fazenda.gov.br/publico/e-CAC/Manual_para_Acesso_ao_Portal_e_CAC.pdf Acesso em: 24 de agosto de 2009.
[122] Comitê Gestor. Ata da reunião de 10 de fevereiro de 2009. Disponível em: http://www.iti.gov.br/twiki/pub/Main/Atas/ATA_10_FEV_2009.pdf Acesso em: 15 de agosto de 2009.
[123] Comitê Gestor. Ata da reunião de 10 de fevereiro de 2009. Disponível em: http://www.iti.gov.br/twiki/pub/Main/Atas/ATA_10_FEV_2009.pdf Acesso em: 15 de agosto de 2009.

motivadora de desenvolvimento e também devendo observar seu padrão de Certificação para a ACRaiz ela utiliza softwares capazes de manter a segurança do dados. E por estar associada ao Estado, ou seja, ter a função de manter as informações governamentais é provável que não seja descuidado de sua qualidade, mas não é possível garantir a manutenção desses padrões.

Deve-se, todavia, fazer um paralelo com os dois modelos internacionais apresentados. Ambos os modelos admitem, sem perda de segurança, que empresas privadas participem do processo. Essa diferença para com o padrão adotado pelo Brasil é significativa quando for observado os princípios da OMC, expostos no próximo capítulo. Isso pois, não tendo em vista os custos políticos para a reformulação do atual modelo da ICP-Brasil, o fato de existir Estados importantes com modelos não monopolistas influe na percepção de que talvez o Brasil tenha criado uma instituição que ultrapassasse a real necessidade de segurança, ou seja, que o peso político dado à busca por segurança seja mais elevado do que ela de fato necessita.

Dessa forma após observar a sua estrutura interna tanto das funções que os *softwares* exercem, quanto da estrutura institucional que está devidamente preocupada em manter seus funcionários e ações dentro de um escopo de manutenção da eficiência é possível concluir em termos da primeira questão sobre a segurança que promove aos dados como estando no mesmo nível tecnológico dos demais países aqui estudados. Ou seja, de acordo com os padrões internacionais utilizados.

A par desse conjunto de informações sobre o funcionamento da segurança da informação, do modelo brasileiro com suas vantagens e críticas, principalmente estas, é possível comparar a estrutura nacional com o regime de comércio internacional desenvolvido pela OMC. E relacionar estes princípios e objetivos com as capacidades de segurança e objetivos da ICP-Brasil.

COMÉRCIO INTERNACIONAL E OMC

O comércio de bens e serviços internacionais aumenta a cada ano e representa parcelas mais significativas da obtenção de renda dos Estados. Este comércio pode ser analisado como um todo (Comércio Internacional) e sob a visão de uma legislação específica (Comércio Exterior). Essa diferença de perspectiva permite focar em diferentes instituições e regras que envolvem os processos de exportação e de importação.

Neste capítulo será observado como vem crescendo o comércio de bens relacionados à informática anterior a crise financeira de 2008, bem como a questão dos regimes internacionais. Neste caso, a OMC, pois ela é a instituição internacional responsável pelas questões de comércio internacional. Neste ensejo este capítulo está dividido no crescimento internacional do comércio focando tanto a questão das áreas mais significativas, o tamanho das empresas; seguido pela OMC, seus princípios, bem como o que ela remete à tecnologia da informação.

3.1 – O que é Comércio Internacional?

A diferença entre Comércio Internacional e Comércio Exterior decorre dos aspectos jurídicos, legais vinculados a cada um.

> Segundo Souza, o comércio internacional pode ser conceituado como o intercâmbio de mercadorias e serviços entre nações, sob a égide da legislação internacional, ou seja, ao amparo do Direito Internacional Público. [Enquanto o Comércio Exterior é] o intercâmbio de mercadorias e serviços entre agentes econômicos (empresas em diversos países), que operam sob a égide da legislação nacional[124].

Dessa forma a diferença está no objeto das normas internacionais que, no Direito Internacional Público trata-se dos direitos e obrigações dos Estados e Organismos Internacionais e das relações entre os mesmos. Enquanto as normas de Direito internacional Privado, as quais são as regentes do Comércio Exterior,

[124] SOUZA, Claudio Luiz. A teoria geral do comércio exterior: aspectos jurídicos e operacionais. p. 36 e 37.

tratam de direitos e obrigações dos indivíduos e organizações não vinculadas ao Estado[125].

Portanto, enquanto o Comércio Exterior observa a realidade internacional a partir de um foco interno, a legislação aplicada por cada Estado; o Internacional observa a realidade como um todo. E neste sentido de troca de bens e serviços observa a constância das trocas que continuam ocupando um lugar significativo na balança comercial[126] dos Estados, mesmo em tempo de crise.

A tabela abaixo mostra PIB mundial e a porcentagem dele que corresponde às trocas internacionais.

	2000	**2005**	**2006**	**2007**
PIB Mundial (U$ bilhões)	31.969,00	45.179,29	48.863,33	54.583,79
Exportação de bens e serviços (%PIB)	25	27	28	…
Importação de bens e serviços (%PIB)	25	27	29	…

Quadro 3.1[127]

Fonte: Banco Mundial[128]

Juntamente com este cenário o Banco Mundial divulgou a quantidade de usuários da Internet por cada cem habitantes que passou de 6.7 em 2000 para 16.2 em 2005 e 21.8 em 2007[129]. Estes dados refletem o início de uma cultura de acesso on-line. Portanto, pode esperar o aumento da quantidade de usuário que participam do Comércio Internacional sem saírem de sua residência.

Outra tabela significativa é a da OMC que mostra o aumento das exportações de computadores e serviços de informação. Ela não pode ser

[125] Global business. p. 264.
[126] A balança comercial é a diferença entre os produtos exportados e os importados. Ela é um componente da Balança de Pagamentos. Esta é composta pela Conta de transações Correntes na qual está inserida a Balança Comercial, Conta de movimentação de capitais e a Conta de resultado que a soma entre as duas contas.
[127] Os dados de 2007 não estavam disponíveis no site na data de visita do mesmo.
[128] Banco Mundial. Estatística mundiais de comércio. Disponível em: http://ddp-ext.worldbank.org/ext/ddpreports/ViewSharedReport?REPORT_ID=9147&REQUEST_TYPE=VIEWADVANCED Acesso em: 13 de agosto de 2009.
[129] Banco Mundial. Estatística mundiais de comércio. Disponível em: http://ddp-ext.worldbank.org/ext/ddpreports/ViewSharedReport?REPORT_ID=9147&REQUEST_TYPE=VIEWADVANCED Acesso em: 13 de agosto de 2009.

previamente relacionada ao aumento das compras on-line ou mesmo à possibilidade de utilizar este mecanismo para promover contratos via Internet. Porém possibilita o entendimento do aumento dos usuários expresso acima.

Exportações	**Valor (bilhões de U$)**	**Partes (%)**		**Porcentagem de mudança anual**			
	2005	**2000**	**2005**	**2000-05**	**2003**	**2004**	**2005**
América do Norte	12	19,1	11,4	5	20	9	-1
América do Sul e Central	1	0,9	0,9	19	15	27	26
Europa	64	54,4	59,8	19	35	31	4
União Européia (25)	60	-	56,4	-	-	30	3
Comunidade dos Estados Independentes (CIS)	1	0,2	0,5	45	29	44	56
Ásia	23	...	21,1	...	...	...	...
Mundo	**105**	**100,0**	**100,0**	**17**	**27**	**28**	**9**

Quadro 3.2

Fonte: Organização Mundial do Comércio[130]

É visível neste quadro a participação reduzida da América Latina nas exportações internacionais, o que pode ser explicado pela inexistência de significativas empresas nacionais que atuem neste ramo. Entretanto, se a região quase não exporta, aparece o Brasil, segundo dados da OMC de 2005, como o quinto maior importador mundial representado 3,2% das importações dos 15 maiores importadores do setor e movimentando um capital 1,713 bilhões de dólares[131].

No sentido de incentivar a redução tarifária do comércio de tecnologia foi criado, no âmbito da OMC, o Comitê dos Participantes sobre a Expansão do Comércio em Produtos da Tecnologia da Informação. Este conta com a presença de pouco mais de 70 Estados. E representa algo em torno de 97% do comércio

[130] OMC. Exportações mundiais de computadores e serviços de informação. Disponível em: http://www.wto.org/english/res_e/statis_e/its2007_e/section3_e/iii25.xls Acesso em: 13 de agosto de 2009.
[131] OMC. Maiores exportadores e importadores de computadores e serviços de informação Disponível em: http://www.wto.org/english/res_e/statis_e/its2007_e/section3_e/iii26.xls Acesso em: 13 de agosto de 2009.

mundial neste segmento[132]. Entretanto, suas regras são válidas apenas aos que aderirem ao Comitê e, neste caso, o Brasil se encontra fora deste conjunto. O interesse, bem como o princípio que o norteia é a redução de impostos que recaem sobre o comércio destes produtos. Neste sentido prevê a redução a zero de todos os produtos presentes na Declaração, sem exceções, tanto de tarifações quanto de impostos.

Mas, ao se tratar de comércio de bens e serviços relacionados a informática há uma grande dificuldade decorrente do termo ao qual este setor está vinculado, tecnologia da informação. Este termo é utilizado para setores como telecomunicações, eletrônicos, máquinas e equipamentos que não estão associados à área da computação. Por isso, as estatísticas relacionadas e este tipo específico de comércio se tornam raras e, muitas vezes os dados amplos vinculados a Tecnologia da Informação podem mascarar as particularidades dos setores. Portanto, ao se tratar de setores relacionados à informática foca-se no número de usuários, de comércio on-line. Estes dados podem expressar de forma mais clara o desenvolvimento deste segmento.

Segundo a UNCTAD, Agência da ONU para Comércio e Desenvolvimento em 2003 haviam 44, 217 milhões de usuários de Internet na América Latina o que equivalia ao crescimento de 4,19% em relação ao ano de 2002. Dentre os usuários da Internet na América Latina a maioria se encontra no Brasil. Para cada 10000 pessoas existem certa de 832 usuários na região e no Brasil para cada 10000 há 822[133]. O Brasil juntamente com a China, Coréia do Sul, Índia e México representam 61,52% dos usuários de Internet nos países em desenvolvimento. E em 2003 os países em desenvolvimento representavam 36% dos usuários no mundo. Isso demonstra o potencial de crescimento do número de usuários nesses Estados, intensificando ainda mais as possibilidades de comércio on-line.

Portanto, mesmo dispondo de pouco dados é possível fazer um paralelo entre a quantidade de computadores comercializados mundialmente e o crescimento do número de usuários. Estes dados podem, em conjunto, explicar o

[132] OMC. Disponível em: http://www.wto.org/english/tratop_e/inftec_e/inftec_e.htm Acesso em: 23 de agosto de 2009.
[133] UNCTAD. E-commerce and development report 2004. Disponível em: www.unctad.org

aumento de acesso e de transações efetuadas nos sites de compras on-line, tanto internamente, quanto internacionalmente.

Nacionalmente destaca-se o Mercado Livre[134], sendo o E-bay[135] um dos principais acionistas; e internacionalmente, a Amazon.com[136] e o E-bay. O total das transações feitas pela Amazon.com foi de U$1,88 bilhão entre junho de 2008 e junho de 2009, o que representou, em comparação ao período anterior (junho de 2007 a junho de 2008), um crescimento de 78%[137]. Já a rede E-bay comercializou quase U$ 60 bilhões em 2007[138] e, o Mercado Livre teve nos primeiros três meses de 2009 mais de U$32 milhões transacionados.

No cenário internacional os sites de venda são relevantes pela possibilidade de se firmar um contrato internacional, por exemplo, ao adquirir um produto em outro mercado, como nos Estados Unidos por meio do Amazon.com e receber este produto em casa. Esta compra é caracterizada como uma venda internacional que remete a dados na Balança Comercial do Estado. Para este trabalho, é mais importante notar a proteção de modelos SSL e SET e fazem parte do *hall* de usos da criptografia nessas transações.

Porém, quando observado o uso da Internet como forma de promoção de pagamentos é visivel sua limitação. Apenas cerca de 13% das operações on-line relacionadas a vendas dizem respeito realmente a compras on-line. Seu uso

---

[134] MERCADO LIVRE. Criado em 1999 por Marcos Galperín, iniciou com site argentino, seguida pelo brasileiro em outubro de 1999. Atualmente a rede é dona dos maiores sites de compra e vendas da América Latina. Disponível em: http://www.mercadolivre.com.br/brasil/ml/p_loadhtml?as_menu=MPRESS&as_html_code=SML_03 Acesso em: 16 de agosto de 2009.

[135] E-BAY. É um site norte-americano de compra e venda on-line. Foi criado em 1995 por Pierre Omidyar e atualmente possui presença de 39 países. Disponível em: http://news.ebay.com/about.cfm Acesso em: 16 de agosto de 2009.

[136] AMAZON.COM. A empresa norte-americana foi criada em 1995 por Jeff Bezos, atua diretamente em 6 Estados – por meio de site direcionado e envia seus produtos a outros 19 Estados. Disponível em: http://phx.corporate-ir.net/phoenix.zhtml?p=irol-mediaHome&c=176060 Acesso em: 16 de agosto de 2009. E em: http://www.amazon.com/gp/help/customer/display.html/?nodeId=537734 Acesso em: 16 de agosto de 2009.

[137] AMAZON.COM. Dados crescimento. Disponível em: Disponível em: http://phx.corporate-ir.net/phoenix.zhtml?p=irol-mediaHome&c=176060 Acesso em: 16 de agosto de 2009.

[138] E-BAY. Dados crescimento. Disponível em: http://news.ebay.com/about.cfm Acesso em: 16 de agosto de 2009.

principal é como fonte de informação sobre produtos, 82% e, para as empresas entrarem em contato com clientes, disponibilizar contatos.

Muitas empresas utilizam ferramentas on-line como forma de facilitar a logística, para permitir um maior controle sobre seus investimentos. Isso fica mais claro ao observar os dados acima que demonstram que o uso para o comércio on-line[139]. Porém, deve-se ter em mente este cenário mais amplo que pode se tornar um foco para a criptografia. Este foco deriva da necessidade de proteção desses dados que não estão vinculados aos modelos de criptografia SSL e SET, pois estes apenas são utilizados por sites de vendas.

Essas possibilidades, nichos para o governo disponibilizar a ICP-Brasil é muito relevante. Essas empresas que possuem suas informações eletronicamente demandam segurança, mas muitas vezes não possuem conhecimento sobre o tema e sobre a existência de ferramentas como a da criptografia. Para estas empresas o governo precisa achar formas de divulgar e conscientizar sobre o uso da Internet. E uma maneira interessante apresentada pela UNCTAD é o próprio uso dessa tecnologia pela administração pública.

A possibilidade de os governos utilizarem estes meios eletrônicos tanto para a divulgação de notícias e, principalmente, para o comércio é um incentivo para o desenvolvimento do mesmo[140]. Ou seja, as empresas interessadas em participar de licitações e demais formas de compras governamentais passam a demandar a utilização destas tecnologias de segurança de dados. No caso brasileiro há ações no sentido de compras públicas on-line por pregões eletrônicos. Seria, portanto, para a ICP-Brasil uma forma de divulgá-la mantendo o foco na proteção de dados trocados.

As oportunidades de crescimento do comércio on-line não é um tema relativamente relacionada a OMC. Esta não foca no meio utilizado para o comércio, mas nas normas que garantam um comércio mais justo. Assim, todo

[139] UNCTAD. E-commerce and development report 2004. Disponível em: www.unctad.org/en/docs/ecdr2004_en.pdf Acesso em: 15 de agosto de 2009.

[140] UNCTAD. E-commerce and development report 2004. Disponível em: www.unctad.org/en/docs/ecdr2004_en.pdf Acesso em: 15 de agosto de 2009.

comércio estará, mesmo que indiretamente, relacionado aos princípios, normas, regras e procedimentos desta organização.

No caso da ICP-Brasil como uma ferramenta para comércio internacional deverá ser observado estes fundamentos da OMC no sentido de conhecer se a estrutura brasileira, como um serviço a ser oferecido no mercado está de acordo com os princípios da organização.

3.2 – OMC

A Organização Mundial do Comércio foi criada em 1993 na Rodada do Uruguai. O cenário de sua criação decorreu do acirramento dos conflitos internacionais na área comercial, como entre a Comunidade Européia e os Estados Unidos, ou entre estes e o Japão. Estas disputas decorrem do próprio processo de globalização e do aumento da interdependência econômica entre os Estados. Por isso, em 1986 iniciou uma nova rodada de negociações internacionais que revisse não apenas questões de tarifas ou barreiras, mas que criasse uma agenda para novos temas como propriedade intelectual, comércio de serviços entre outros[141].

> A OMC se constitui como um foro para a continuação do processo de negociações na área do comércio, visando sempre uma maior liberalização do comércio de bens e serviços, além de um foro para a discussão de temas relacionados ao comércio, como meio ambiente, investimentos, concorrência, facilitação de comércio, comércio eletrônico e cláusulas sociais".[142] Sendo o seu principal papel "completar o processo de liberalização dos temas que ainda hoje não se concluiu[143].

Desta forma no preâmbulo do Acordo Constitutivo são explicitados seus objetivos que englobam desde o reconhecimento da importância do comércio que deverá ser executado visando à melhoria dos padrões de vida, a sustentabilidade e preservação do meio ambiente. Seus Estados-membros assumem o compromisso de promoverem esforços positivos em relação aos países em

[141] THORSTENSEN, Vera. OMC: as regras do comércio internacional e a nova rodada de negociações multilaterais. P, 26 e 27.
[142] THORSTENSEN, Vera. OMC: as regras do comércio internacional e a nova rodada de negociações multilaterais. P, 43.
[143] RICUPERO, Rubens. O papel da OMC para a governança global. In: AMARAL JUNIOR, Alberto do. OMC e o Comércio Internacional. P, 7.

desenvolvimento, permitindo o crescimento de sua participação internacional. Para tanto, respeitarão todas as regras da organização bem como continuarão a reduzir tarifas e barreiras[144].

Para atingir seus objetivos foi montada uma vasta estrutura que permitisse a continuidade das negociações e participação dos Estados-membros, ao mesmo tempo em que o dia-a-dia não fosse relegado a segundo plano. Desta forma, a OMC possui órgãos que se reúnem periodicamente como a Conferência Ministerial formada por representantes (ministros de Relações Exteriores ou de Comércio Externo) de cada membro e o Conselho Geral que se reúne quando necessário. Para a resolução de possíveis controvérsias entre os Estados existe o Órgão de Solução de Controvérsias. Ele foi uma grande modificação em relação ao GATT (Acordo Geral sobre Tarifas e Comércio), pois suas resoluções são de aplicação obrigatória e não mais facultativa. Para acompanhar a dinamicidade do comércio há o Órgão de Revisão de Política Comercial que examina as políticas de cada membro garantindo que estão cumprindo as regras da OMC, além de manter a transparência do sistema. E para garantir a implementação das regras acordadas foram criados três Conselhos sobre o Comércio de Bens, de Serviços e de Propriedade Intelectual.

E subordinado a cada Conselho há comitês para desenvolver as atividades da OMC. Dentre os quase 30 grupos de trabalho, há um de grande valia a esta pesquisa que é o Comitê dos Participantes sobre a Expansão do Comércio em Produtos da Tecnologia da Informação subordinado ao Conselho sobre o Comércio de Bens[145].

3.2.1 – Consolidação como um regime de Comércio Internacional

O regime de comércio internacional atual iniciou-se com o GATT. Após a Segunda Guerra Mundial o mundo buscou uma forma de manter o comércio internacional, impedindo os acontecimentos do período entre-guerras. Este foi

[144] THORSTENSEN, Vera. OMC: as regras do comércio internacional e a nova rodada de negociações multilaterais. P, 43 e 44.
[145] THORSTENSEN, Vera. OMC: as regras do comércio internacional e a nova rodada de negociações multilaterais. P, 53.

marcado pela desconfiança internacional, onde cada Estado buscou apenas arrecadar divisas impedindo a viabilidade do comércio internacional e, por conseqüência, do próprio desenvolvimento das indústrias locais, o que fora caracterizado como um dos motivos da Segunda Guerra.

Durante seus quase 50 anos de funcionamento ele promoveu oito Rodadas de negociações com o intuito de reduzir tarifas e barreiras ao comércio. Sendo as mais importantes: a de Tóquio (1973-1979) que reduziu as barreiras não-tarifárias e a do Uruguai (1986-1994) que criou a OMC, o GATS (Acordo Geral sobre Comércio de Serviços), reduziu tarifas de áreas tradicionais outrora não significativas dentro do GATT como agricultura, têxteis; entre outros aspectos criados nesta rodada.

Portanto, a OMC nasceu com um corpo de leis (decorrentes do GATT) e com um corpo de membros consistentes. Sua diferença significativa foi a necessidade dos membros terem de acatar a todas as regras pré-estabelecidas, não mais escolher a quais estariam vinculados e que as decisões tomadas pelo órgão de Solução de Controvérsias deveriam ser de fato aplicadas, as decisões deixaram de ser conselhos, mas leis que os Estados deverão acatar.

> De grande importância foi o estabelecimento de um novo mecanismo de solução de controvérsias, de natureza judicial, mais eficiente que o do GATT. Essencialmente, tal mecanismo não permite que as decisões dos 'painéis' estabelecidos para julgar as controvérsias sobre o comércio sejam bloqueadas por uma das partes (o que era possível no GATT)[146].

Esse corpo legal e jurídico de Direito Internacional Público lida com uma série de itens diversos entre si, desde produtos tradicionais como agricultura, têxteis, passando por siderúrgicos, manufaturados, de tecnologia de ponta como aeronaves e vários outros temas que englobam sua atuação. E apesar da grande diversidade há uma série de princípios que norteiam o comércio internacional e conseqüentemente a própria OMC.

[146] AMORIM, Celso. A OMC pós-Seattle. In: AMARAL JUNIOR, Alberto do. OMC e o Comércio Internacional. P, 335.

3.2.1.1 – Princípios da OMC[147]

O primeiro princípio existe desde a criação do GATT que é o comércio não discriminatório. Nele estão incluídas as cláusulas da nação mais favorecida que exprime o compromisso de estender aos demais Estados as vantagens dadas a outro e de igualdade de tratamento. Existe a clara noção de que algumas vantagens são temporárias e voltadas a Estados em desenvolvimento ou outras situações específicas que limitam a extensão da aplicação desta cláusula. Juntamente se encontra a igualdade de tratamento de produtos nacionais e importados.

Esta cláusula impede que sejam aplicadas taxas sobre a logística de produtos internacionais com o objetivo de reduzir a sua competitividade junto ao cenário local. Esta igualdade é aplicada aos produtos e serviços após adentrarem as fronteiras nacionais, ou seja, não estão relacionados à tarifação e as barreiras não-tarifárias.

O segundo princípio refere-se ao livre comércio decorrente da redução gradual e negociada das tarifas. Neste princípio que se visualiza as rodadas de negociações, por meio delas foram possíveis negociar reduções significativas das tarifas de comércio. Entretanto, por vezes outros temas como as barreiras não-tarifárias (quotas de importação) são temas destas negociações. A graduação decorre do tempo dado aos Estados para se adaptarem aos acordos, com a tendência de prazos mais estendidos aos países em desenvolvimento.

A previsibilidade decorre da transparência e, figura como um princípio. Ela pressupõe a possibilidade de criar cenários futuros mais estáveis. Com este conhecimento é incentivado os investimentos, criação de empregos e o aproveitamento das vantagens oferecidas pela concorrência originada dos preços reduzidos e competitividade das mercadorias e serviços nacionais e importados.

[147] OMC. Os princípios estão disponíveis no site da Organização Mundial do Comércio. Disponível em: http://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm Acesso em: 24 de agosto de 2009.

A concorrência é estimulada pelo princípio da livre competição. Entretanto, existem práticas desleais de comércio como o dumping – venda externa de um bem com preço menor que de produção – e o subsídio que é a concessão de capital, crédito a determinados setores pelo Estado. A primeira ação está amplamente relacionada a tentativa de quebrar as empresas do mercado no qual o produto adentra e o segundo possui dupla função, seja na tentativa de tornar o produto mais competitivo internacionalmente; ou nacionalmente na busca de impedir que os importados adquiram uma parcela maior do mercado doméstico. Em ambos os casos é previsto taxas que permitam a redução dos prejuízos oferecidos.

E como último princípio está o incentivo ao desenvolvimento e reforma econômica. Este se direciona aos Estados em desenvolvimento. Com base nele que a OMC toma decisões de ampliar os prazos de adaptação dos países em desenvolvimento no que se refere às leis e reduções tarifárias a serem implementadas. Há também o incentivo que ocorra projetos de cooperação entre os Estados em desenvolvimento que galgam posições mais importantes e de maior alcance. Esse princípio reflete a estrutura da organização, mais de três quartos de seus membros são Estados em desenvolvimento e/ou em transição para o capitalismo.

Portanto, a ICP-Brasil não está em consonância com todos os princípios da OMC. Esta OI busca uma liberalização do comércio, num cenário de concorrência justa, igualdade entre produtos internos e internacionais e com clausulas que impedem distinções entre Estados. Fica evidente que o modelo brasileiro está em relativa dissonância que ganha maior relevância ao notar a postura adotada nos demais Estados. Ou seja, o fato de os outros modelos permitirem o funcionamento concorrencial faz com que o Brasil seja um caso a parte o que intensifica a percepção de dissonância. Se a atitude monopolista fosse um tendência internacional o aspecto da segurança internacional ganharia maior relevância que o econômico e desta forma poderia ser minimizado a importância dos princípios da OMC para o aspecto criptografico.

A ICP-Brasil está situada num cenário de monopólio, isso é contrário ao princípio de livre competição. Com esta medida é o Estado se exime de participação comercial, invalidando as clausulas de nação mais favorecida, igualdade de tratamento, livre comércio.

O modelo brasileiro está em consonância com o princípio da previsibilidade por estar delineado por leis que lhe garantem previamente características de estabilidade ainda dispõem do princípio de transparência. E em termo de cooperação internacional, a ICP-Brasil foi pautada na busca de informações, com aspectos cooperativos; e o CG tem a cooperação como uma de suas funções.

Dessa forma, sob o aspecto insitucional da ICP-Brasil incide a parcialidade dos princípios, ou seja, que é preciso a este momento ver a instituição como uma prestadora de serviço e não apenas o serviço em si. Esta percepção é relevante, pois caso observasse puramente os aspectos técnicos a análise em relação aos princípios da OMC seria parcial. Isso decorre da impossibilidade de separar o serviço da instituição que o oferece. Portanto, a consonância parcial da ICP-Brasil se dá prioritariamente no aspecto institucional, pois que no aspecto técnico ela se encontra devidamente coerente com a idéia de melhoria comercial desenvolvida pela OMC.

Ao se tratar do aspecto tecnológico sob a óptica da OMC é possível observar uma limitação por parte da organização, que necessita lidar com questões outras vivas desde a criação do GATT como agricultura, têxteis e outros bens tradicionais. Mas independente de suas agendas, o conhecimento de seus princípios são relevantes para observar qual seria o possível alcance da ICP-Brasil no cenário internacional, bem como quais são as possíveis criticas que possa vir a enfrentar no futuro.

CONCLUSÃO

A Interdependência Complexa possibilita como teoria observar sem contradições que as empresas são atores importantes nas relações internacionais. E ao se tratar do modelo criptográfico adotado no Brasil são atores determinantes. Elas conseguiram promover uma mudança de foco significativo, saindo da razão de Estado de segurança institucional para favorecer a sociedade como um todo. Esta perspectiva não poderia ter sido explicada pelo Realismo, que também seria inviável ao observar a relevância que o comércio ocupando, como é observado nas vendas on-line.

Essa teoria, Interdependência Complexa, é a base para responder a pergunta inicial sobre a funcionalidade da ICP-Brasil. Como critérios, deverá ser apontado tanto as suas características técnicas, possibilidade de manter em segurança as informações sem permitir que sejam visualizadas e alteradas; quanto a sua consonância com os princípios da OMC pois esta instituição presta um serviço que poderá ocupar um lugar internacionalizado, ou seja, ela pode vir a prestar seus serviços em outros mercados e as oportunidades que o comércio internacional oferece.

Sobre o primeiro aspecto, como foi concluído no capítulo 2, a ICP-Brasil possui o mesmo padrão de funcionalidade técnica das demais empresas e modelos atualmente adotados. Como críticas há tanto o fato do modelo ultrapassar as instâncias do direito ao imputar seus usuários perante à lei. E de forma mais técnica o fato de não possuir uma associação com fabricantes de computadores de modo a colocar seus Auto-certificados. Ambas as críticas devem ser levadas em conta, a primeira o governo promoveu mudanças iniciais para manter características de legalidade do processo. A segunda crítica, entretanto, não foi foco de mudanças e questionamentos e, talvez o seja se houver problemas com os certificados. Antes que isto ocorra e tendo em vista que a amplitude da ICP-Brasil não deverá ocorrer associações deste porte inicialmente. E por último a compração entre os modelos vigentes que mostra ser o Brasil um caso isolado na escolha de um modelo monopolista.

Em relação a OMC ficou observado que a ICP-Brasil possui uma estrutura contrária a vários princípios da organização. Se for observado a razão de Estado como central ao modelo brasileiro é viável aceitar suas limitações. Porém se tomar como base o modelo europeu que não vincula monopólios com a utilização desta tecnologia pelo Estado, o modelo brasileiro perde parte de sua justificativa como razão de Estado. Além do mais essa impossibilidade de competir internamente pode trazer a perda do desenvolvimento tecnológico por não haver competições.

Os princípios da OMC também oferecem a percepção da cooperação internacional que é foco da estrutura brasileira, isso é benéfico para o Brasil por poder comparar o grau de desenvolvimento interno com as empresas internacionais. Também permite que a estrutura nacional possa vir a participar internacionalmente, ou seja, sendo a ICP-Brasil eficiente em termos técnicos, ela poderá ter suas ações expandidas a outros Estados.

Neste sentido, no âmbito de comparações com a OMC o modelo brasileiro em seu aspecto insitucional apresenta funcionalidades por sua possibilidade de auxiliar ao desenvolvimento externo por meio de cooperações, entretanto vislumbra embates em aspectos primordiais para tentativas de crescimento internacional neste setor.

Por fim o último item, as oportunidades. Estas são relevantes, pois como mostrado há dois nichos distintos em que a ICP-Brasil pode focar. O primeiro relacionado ao comércio on-line e neste sentido deverá concorrer com os modelos SSL e SET que estão consolidados no mercado. E o segundo é o das empresas que utilizam as ferramentas computacionais como formas de gerir seus negócios não voltados ao comércio on-line. Neste âmbito a ICP-Brasil tende a ter maior e espaço, primeiro porque não há nenhum modelo consolidado e segundo justamente por ser uma estrutura vinculada ao governo. Isso traz uma maior segurança, algo semelhante a utilização do DES em décadas passadas baseado justamente na percepção da qualidade para o Estado norte-americano adotá-lo.

Dessa forma pode-se concluir que realmente a ICP-Brasil é uma ferramenta funcional ao comércio, pois propicia a segurança necessária aos empresários. Essa funcionalidade é comedida pelas suas diferenças em relação aos princípios do regime de comércio internacional da OMC e poderá sofrer várias críticas quando observada por sua oportunidade de crescimento externo. Dentre elas a própria possibilidade de alteração do modelo.

Ao se tratar de um modelo fundado nas instância do poder Legislativo, a possibilidade de mudanças no sentido de se recriar ou modificar drasticamente a ICP-Brasil pode ser considerada despendiosa, não apenas pelas questões burocráticas envolvidas, mas também por todo o interesse e jogo político das diversas insituições que a desenvolveram. A possibilidade de ocorrer uma mudança tão significativa seria um tema extremamente valioso para um estudo político do desenvolvimento da ICP-Brasil, tanto por sua criação quanto em relação ao futuro que a espera nas possibilidades.

No desenvolvimento desta pesquisa foi observado a dificuldade de achar dados sobre o desenvolvimento da instituição, ou seja, não houve informações disponíveis sobre o número de usuários que possui e nem as perspectivas de crescimento que deseja implementar. Assim como a falta de fontes bibliográficas que relacionassem a ICP-Brasil com a sociedade. Ou seja, ou as fontes diziam respeito puramente a segurança da informação, normalmente relacionada à matemática ou apresentavam a sociedade por suas características comerciais. Foram poucas as fontes que relacionaram a segurança da informação como um investimento empresarial ou mesmo como perspectiva de uso para o crescimento da empresa. Por esses aspectos é possível perceber que há um longo caminho para a ICP-Brasil vir a participar ativamente do comércio internacional e este caminho primeiro perpassa o próprio Brasil, no sentido dela promover seu conhecimento dentro do seu mercado interno.

BIBLIOGRAFIA

Livros

ABC. Diretrizes para a cooperação técnica internacional multilateral e bilateral. Brasília: MRE, 2004.

ABC. Formulação de projetos de cooperação técnica internacional (PCT). 2 ed, Brasília: Agência Brasileira de Cooperação, 2005. Disponível em: <http://www.abc.gov.br> Acesso em: 24 de novembro de 2008.

AMARAL JUNIOR, Alberto do (Cor.). OMC e o Comércio Internacional. São Paulo: Aduaneiras, 2002.

ANGELL, Norman. A grande ilusão. Brasília: Editora UnB, 2002.

BARRA, Marcelo. Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e a formação do Estado eletrônico. Brasília, 2006.

BARRAL, Welber (Org.). O Brasil e a OMC. Curitiba: Juruá, 2002, 2ª ed.

BAUER, Friedrich Ludwig. Decrypted secrets: protocols, algorithms and source code in C/. New York, John Wiley & Sons, 1996.

BOBBIO, Norberto (org.). Dicionário de Política. Brasília: UnB, 1998. 11ª ed.

BRUNO, Gilberto. Considerações sobre a criação da infra-estrutura de chaves públicas brasileira e seu comitê gestor. Disponível em: <http://jus2.uol.com.br/ > Acesso em: 04 de julho de 2009.

BUCHMANN, Johannes. Introdução à criptografia. São Paulo: Berkeley Brasil, 2002.

BULL, Hedley. A sociedade anárquica: um estudo da ordem política mundial. Brasília: UnB, 2002. Clássico IPRI, 5.

CARR, Edward Hallett. Vinte anos de crise: 1919-1939; uma introdução ao estudo das Relações Internacionais. Brasília: UnB, 1981. Clássicos IPRI, 1.

CASTELLS, Manuel. A sociedade em rede. São Paulo: Paz e Terra, 1999. 5ª ed.

CORDEIRO, Luiz Gustavo. Certificação digital: conceitos e aplicações; modelo brasileiro e australiano. Rio de Janeiro: Ciência Moderna, 2008.

COSTA, Marcos da e MARCACINI, Augusto. A urgência e relevância em violentar a Internet brasileira. Disponível em: <http://jus2.uol.com.br/> Acesso em: 05 de julho de 2009.

FILHO, Demócrito Reinaldo. A ICP-Brasil e os poderes regulatórios do ITI e do CG. Disponível em: <http://jus2.uol.com.br>. Acesso em: 05 de julho de 2009.

FRIEDMAN, Thomas. O mundo é plano: uma breve história do século XXI. Rio de Janeiro: Objetiva, 2007.

GODOY, Arnaldo. Notas introdutórias ao Direito Comparado. Disponível em: <http://jus2.uol.com.br/ > Acesso em: 04 de julho de 2009.

GODOY, Max Bianchi. A segurança da informação e importância para o sucesso das organizações. Rio de Janeiro, 2004.

GREENFIELD, Jonathan. Distributed programming paradigms with cryptography applications. Berlin: Springer,

GRIFFITHS, Martin. 50 grandes estrategistas das Relações Internacionais. São Paulo: Contexto, 2004.

KEOHANE, Robert e NYE, Joseph. Power and Interdependence. London: Longman, 2001, 3ª ed.

KUROSE, James e ROSS, Keith. Redes de computadores e a Internet: uma nova abordagem. São Paulo: Addison Wesley, 2003.

LINO, Marcelo. Aplicação de uma política de segurança da informação nas organizações. Brasília, 2005.

DELEGAÇÃO DA COMISSÃO EUROPÉIA NO BRASIL. Livro azul 2008 da cooperação da União Européia no Brasil. Disponível em: <http://www.delbra.ec.europa.eu/pt/downloads/book%20livro%20azul%202008%20completo.pdf> Acesso em:

LOADER, Brian. The governance of cyberspace: politcs, technology and global restructuring

MAGNOLI, Demétrio. União Européia: história e geopolítica. São Paulo: Editora Moderna, 1995.

MAQUIAVEL, Nicolau. O príncipe. São Paulo: Hemus, 1977.

MARCOVITCH, Jacqués (Org.). Cooperação internacional: estratégias e gestão. São Paulo: Edusp, 1994.

MARQUES, Luiz Guilherme. Direito Comparado e jurisprudência. Disponível em: <http://jus2.uol.com.br/ > Acesso em: 04 de julho de 2009.

MATTERLART, Armand. Comunicação-mundo: história das idéias e das estratégias. Petrópolis: Vozes, 1996, 2ª ed.

MEDEIROS, As organizações internacionais e a cooperação técnica

MORAES, Denis (org.). Por uma outra comunicação: mídia, mundialização cultural e poder. Rio de Janeiro: Record, 2003.

MOREIRA, Adriano. Teoria das Relações Internacionais. Lisboa: Almedina, 2002, 4ª ed.

MORGENTHAU, Hans. A política entre as nações: a luta pelo poder e pela paz. Brasília: UnB, 2003. Clássicos IPRI.

MUELLER, Milton. The internet and the global governance: principals and norms for a new regime.

OLIVEIRA, Odete Maria. Relações Internacionais: interdependência e sociedade global. Ijuí: Editora UNIJUÍ, 2003.

REZENDE, Pedro Antônio. Sobre a criação da ICP-Brasil. Disponível em: <http://jus2.uol.com.br/ > Acesso: 05 de julho de 2009.

REZENDE, Pedro Antônio. Sistema de pagamento e ICP-Brasil. Disponível em: <http://www.cic.unb.br/ > Acesso em: 5 de julho de 2009.

SARAIVA, José Carlos. Relações Internacionais: dois séculos de história. Brasília: IBRI, 2001.

SCHAFF, Adam. A sociedade informática: as conseqüências sociais da segunda revolução industrial. São Paulo: Editora Brasiliense, 1995.

SCHNEIER, Bruce. Applied cryptography,

SEMOLA, Marcos. Gestão da segurança da informação: uma visão executiva. Rio de Janeiro: Campus, 2003.

SHOKRANIAN, Salahoddin. Criptografia para iniciantes. Brasília: Editora UnB, 2005.

SNIJDERS, Henricus e WEATHERILL, Stephen. E-commerce law: national and transnational topics and perspectives. London: Kluwer Law International. Disponível em: <http://books.google.com.br/> Acesso em: 7 de maio de 2009.

SOUZA, Claudio Luiz. A teoria geral do comércio exterior: aspectos jurídicos e operacionais. Belo Horizonte: Líder, 2003.

STALLINGS, William. Cryptography and network security: principles and practices. Delhi: Pearson Education, 2006, 4ª ed.

STINSON, Douglas Robert. Cryptography: theory and practice. Boca Rato: Chapman & Hall, 2006.

THORSTENSEN, Vera. OMC: as regras do comércio internacional e a nova rodada de negociações multilaterais

THORSTENSEN, Vera. OMC: Organização Mundial de Comércio. São Paulo: Aduaneiras, 2001, 2ª ed.

VAUDENAY, Serge. A classical introduction to cryptography. Disponível pelo site: <http://books.google.com.br/> Acesso em: 3 de maio de 2009.

WHITE, Gregory. Security + Certification: all-in-one exam guide. Disponível em: <http://books.google.com.br/ > Acesso em: 7 de maio de 2009.

Leis

BRASIL. Decreto 3996, de 31 de outubro de 2001. Disponível em: <www.planalto.gov.br> Acesso em: 10 de agosto de 2009.

BRASIL. Decreto 4553, de 27 de dezembro de 2002. Disponível em: <www.planalto.gov.br> Acesso em: 5 de julho de 2009.

BRASIL. Decreto 5301, de 9 de dezembro de 2004. Disponível em: <www.planalto.gov.br> Acesso em: 6 de maio de 2009.

BRASIL. Medida Provisória 2200, de 28 de junho de 2001. Disponível em: <www.planalto.gov.br> Acesso em: 3 de maio de 2009.

BRASIL. Medida Provisória 2200-1, de 27 de julho de 2001. Disponível em: <www.planalto.gov.br> Acesso em: 3 de maio de 2009.

BRASIL. Medida Provisória 2200-2, de 24 de agosto de 2001. Disponível em: <www.planalto.gov.br> Acesso em: 15 de novembro de 2008.

UNIÃO EUROPÉIA. Diretiva 1999/93CE do Parlamento Europeu e do Conselho. Disponível em: <http://www.scee.gov.pt/> Acesso: 22 de agosto de 2009.

UNIÃO EUROPÉIA. Decisão da Comissão de 6 de novembro de 2000. Disponível em: <http://www.scee.gov.pt/ > Acesso em: 22 de agosto de 2009.

UNIÃO EUROPÉIA. Decisão da Comissão de 14 de julho de 2003. Disponível em: <http://www.scee.gov.pt> Acesso em: 22 de agosto de 2009.

Sites

AMAZON.COM. Media room. Disponível em: Disponível em: <http://phx.corporate-ir.net/phoenix.zhtml?p=irol-mediaHome&c=176060> Acesso em: 16 de agosto de 2009.

AMAZON.COM. Amazon marketplace shipping for buyers. Disponível em: <http://www.amazon.com/gp/help/customer/display.html/?nodeId=537734>
Acesso em: 16 de agosto de 2009.

BANCO MUNDIAL. Data Profile. Disponível em: <http://www.worldbank.org/ > Acesso em: 13 de agosto de 2009.

COMISSÃO EUROPÉIA. Eurostat. Disponível em: <http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home> Acesso em: 2 de maio de 2009.

COMISSÃO EUROPÉIA/PROGRAMAS DE COOPERAÇÃO EXTERNA. @LIS 2. Disponível em: <http://ec.europa.eu/europeaid/where/latin-america/regional-cooperation/alis/index_en.htm> Acesso em: 3 de maio de 2009.

COMITÊ GESTOR. Ata da reunião de 10 de fevereiro de 2009. Disponível em: <http://www.iti.gov.br> Acesso em: 15 de agosto de 2009.

DELEGAÇÃO COMISSÃO EUROPÉIA NO BRASIL. A União Européia. Disponível em: <http://www.delbra.ec.europa.eu/pt/ > Acesso em: 24 e agosto de 2009.

DELEGAÇÃO COMISSÃO EUROPÉIA NO CHILE. Lançamento Projeto @LIS 2. Disponível em:

http://www.delchl.ec.europa.eu/en/whatsnew/EVENTS_2009_03_17_@lis_cepal.htm Acesso em: 3 de maio de 2009.

E-BAY. About e-Bay. Disponível em: <http://www.ebay.com/ > Acesso em: 16 de agosto de 2009.

ECRYPT. European Network of Excellence in Cryptology II. Disponível em: <http://www.ecrypt.eu.org/ > Acesso em: 3 de maio de 2009.

GILC/Eletronic Privacy Information Center. Cryptography and liberty 1999: an international survey of encryption policy. Disponível em: <http://www.gilc.org> Acesso em: 03 de maio de 2009.

FEBRABAN. Pesquisa: o setor bancário em números. Disponível em: <http://www.febraban.org.br/ > Acesso em: 05 de julho de 2009.

ITI. Características mínimas de segurança para as AR da ICP-Brasil: DOC-ICP-03.01. Disponível em: <http://www.iti.gov.br> Acesso em: 07 de julho de 2009.

ITI. Declaração de práticas de certificação da autoridade certificadora raiz da ICP-Brasil. Disponível em: <http://www.iti.gov.br/> Acesso em: 5 de julho de 2009.

ITI. . Notícia divulgação pesquisa IPEA sobre o Governo Federal. Disponível em: <http://www.iti.gov.br/ > Acesso em: 24 de agosto de 2009.

ITI. Estrutura ICP-Brasil. Disponível em: <http://www.iti.gov.br/ > Acesso em: 05 de julho de 2009.

ITI. O que é certificação digital?. Disponível em: <http://www.iti.gov.br/ > Acesso em: 10 de abril de 2009.

PRESIDÊNCIA DA REPÚBLICA/ CASA CIVIL. Termo de referência Comitê Gestor da ICP-Brasil: CG ICP-Brasil. Disponível em: <http://www.planalto.gov.br> Acesso em: 04 de julho de 2009.

ITI. Regimento Interno do Comitê Gestor da ICP-Brasil. Disponível em: <http://www.iti.gov.br/ > Acesso em: 05 de julho de 2009.

MERCADO LIVRE. História. Disponível em: <http://www.mercadolivre.com.br/ > Acesso em: 16 de agosto de 2009.

MRE/ Departamento de temas científicos e tecnológicos (DCT). Institucional. Disponível em: <http://www.dct.mre.gov.br > Acesso em: 2 de maio de 2009.

MRE/Ciência, tecnologia e informação (CTI). Acordos de tecnologia entre o Brasil e os Estados Unidos. Disponível em: <http://www.dctec.mre.gov.br/> Acesso em: 2 de maio de 2009.

MRE/Departamento de Atos Internacionais (DAÍ). Decreto 92.885 de 1986: promulgação do acordo de cooperação técnica entre Brasil e Estados Unidos. Disponível em: <http://www2.mre.gov.br/dai/ > Acesso em: 3 de maio de 2009.

MRE/Sistema de Informação Científica e Tecnológica do Exterior (SICTEX). Informação transferência de tecnologia de países desenvolvidos. Disponível em: <http://www.sictex.mre.gov.br/ > Acesso em: 2 de maio de 2009.

NIST/Computer security division. Cryptographic technology. Disponível em: <http://csrc.nist.gov/ > Acesso em: 6 de maio de 2009.

NIST/FIPS Publications. Standards for security categorization of federal information and information system. Disponível em: <http://csrc.nist.gov/ > Acesso em: 6 de maio de 2009.

NIST/FIPS Publications. Anúncio padrão AES. Disponível em: <http://csrc.nist.gov/ > Acesso em: 6 de maio de 2009.

NIST/U.S DEPARTAMENT OF COMMERCE. Entity authentication using public key cryptography. Disponível em: <http://csrc.nist.gov/ > Acesso em: 6 de maio de 2009.

NIST. Política de acesso e uso de recursos de tecnologia da informação. Disponível em: <http://cio.nist.gov/ > Acesso em: 6 de maio de 2009.

NSA/CSS. Informações criptografia e o CSS. Disponível em: <http://www.nsa.gov/ > Acesso em: 06 de maio de 2009.

NSA/CSS. Introdução sobre as agências secretas. Disponível em: <http://www.nsa.gov/ > Acesso em: 06 de maio de 2009.

OMC. Information Technology Agreement. Disponível em: <http://www.wto.org/ > Acesso em: 23 de agosto de 2009.

OMC. Exportações mundiais de computadores e serviços de informação. Disponível em: <http://www.wto.org/ > Acesso em: 13 de agosto de 2009.

OMC. Maiores exportadores e importadores de computadores e serviços de informação Disponível em: <http://www.wto.org/ > Acesso em: 13 de agosto de 2009.

OMC. Princípios do sistema de comércio. Disponível em: <http://www.wto.org/ > RECEITA FEDERAL DO BRASIL. Manual de orientação para o acesso ao Centro de Atendimento Virtual do Contribuinte – Portal eCAC. Disponível em: <http://www.receita.fazenda.gov.br/ > Acesso em: 24 de agosto de 2009.

UNCTAD. E-commerce and development report 2004. Disponível em: <www.unctad.org> Acesso em: 15 de agosto de 2009.