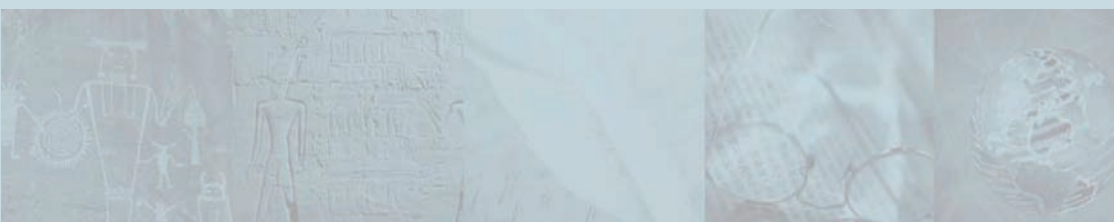
GOVERNANÇA DA INTERNET

QUESTÕES, ATORES E CISÕES

Jovan Kurbalija • *Eduardo Gelbstein*
Tradução de *Renato Aguiar*



GOVERNANÇA DA INTERNET

QUESTÕES, ATORES E CISÕES

Jovan Kurbalija • *Eduardo Gelbstein*

Tradução de *Renato Aguiar*

Versão em português publicada pelo Núcleo de Pesquisa, Estudos e Formação da Rede de Informações para o Terceiro Setor (Nupef/Rits), com o apoio do Centro Internacional de Pesquisas para o Desenvolvimento (IDRC).

Rits - Rede de Informações para o Terceiro Setor
Rua Álvaro Alvim, 21/16º andar
Centro • Rio de Janeiro • RJ • Brasil

Nupef/Rits - Núcleo de Pesquisa, Estudos e Formação da Rits

e-mail: rits@rits.org.br
coordenacao@nupef.org.br

Website: www.rits.org.br
www.nupef.org.br

Coordenação editorial: Graciela Selaimen
Diagramação e montagem: Renata Monteiro
Tradução: Renato Aguiar
Revisão: Ricardo Vaz Monteiro

GOVERNANÇA DA INTERNET

QUESTÕES, ATORES E CISÕES

Jovan Kurbalija • *Eduardo Gelbstein*
Tradução de *Renato Aguiar*

ISBN 99932-53-13-8

Publicado por DiploFoundation e Global Knowledge Partnership

DiploFoundation
Malta: 4th Floor, Regional Building
Regional Rd.
Msida, MSD 13, Malta

Suíça: DiploFoundation
Rue de Lausanne 56
CH-1202 Genebra 21, Suíça

e-mail: diplo@diplomacy.edu
Website: http://www.diplomacy.edu

Secretariado da Global Knowledge Partnership
Level 23, Tower 2, MNI Twins
11, Jalan Pinang
50450 Kuala Lumpur , Malásia

e-mail: gkps@gkps.org.my
Website: http://www.globalknowledge.org

Editado por Dejan Konstantinović e Steven Slavik
Ilustrações: Zoran Marčetić – Marča
Capa: Nenad Došen
Diagramação e montagem: Aleksandar Nedeljkov

ÍNDICE

SEÇÃO 1

Introdução

A Governança da Internet não é um tema simples. Embora diga respeito a um símbolo essencial do mundo DIGITAL, não pode ser tratada numa lógica digital-binária de falso/verdadeiro, bom/mau. Em vez disso, as muitas sutilezas e matizes de significado e percepção exigem uma abordagem ANALÓGICA, capaz de cobrir um continuum de opções e compromissos.

Conseqüentemente, esta brochura não tentará fazer afirmações definitivas sobre questões de Governança da Internet. Antes, o seu objetivo é propor um quadro prático de análise, discussão e resolução dos problemas-chave deste campo.

INTRODUÇÃO

> Em apenas poucos anos, a Internet revolucionou o comércio, a saúde, a educação e certamente a própria estrutura da comunicação e do intercâmbio humano. Além disso, o seu potencial é muito maior do que o que vimos no tempo relativamente curto desde a sua criação. Ao administrar, promover e proteger a sua presença em nossas vidas, *nós devemos ser tão criativos quanto aqueles que a inventaram*. É claro, coloca-se uma necessidade de governança, mas isto não significa obrigatoriamente que tenha de ser feito ao modo tradicional, para algo que é tão diferente.
>
> Kofi Annan – Fórum Global sobre Governança da Internet (Nova Iorque, 24 de março de 2004)

Num tempo relativamente curto, a Internet tornou-se um instrumento essencial para a sociedade atual. Em meados de 2005, estimou-se que a Internet envolvesse:

- cerca de 750 milhões de usuários em todo o mundo;
- um movimento de comércio eletrônico de cerca de um bilhão de dólares americanos, cuja projeção é de crescer rapidamente;
- um impacto social fundamental em educação, saúde, governança e outras áreas de atividade;
- cibercrimes, como fraudes, jogos, pornografia e roubo de identidade;
- maus usos e abusos sob a forma de códigos maliciosos e de *spam*.

A Internet e a estatística não têm tido um convívio fácil. Desde os primeiros dias da Internet, tem sido extremamente difícil obter dados sobre os números exatos de usuários e hospedeiros, volume de tráfego, finanças e assim por diante. Além disso, os números foram freqüentemente usados para superestimar o crescimento da Internet. Alguns pesquisadores atribuem a explosão da bolha das "ponto-com" ao uso de números inflados sobre o crescimento potencial da Internet.

A consciência crescente do impacto social, econômico e político da Internet sobre a sociedade pôs em destaque a questão da Governança da Internet.

No caso da Internet, a governança é necessária, entre outras coisas, para:

- evitar ou pelo menos minimizar o risco de fragmentação da Internet;
- manter a compatibilidade e a interoperabilidade;
- salvaguardar direitos e definir as responsabilidades dos vários atores;

- proteger usuários finais contra maus usos e abusos;
- estimular desenvolvimentos futuros.

O processo de elaborar sobre questões legais e conseqüências sociais de desenvolvimentos tecnológicos vem invariavelmente depois da inovação tecnológica ela mesma. Isto também se aplica à Internet.

Nós estamos hoje na fase inicial das negociações internacionais sobre a Governança da Internet, a qual se caracteriza pela necessidade de estabelecer e pactuar um quadro básico e selecionar os instrumentos apropriados para a discussão das muitas questões que vêm sendo levantadas. Quem são os atores que provavelmente influenciarão o desenvolvimento futuro da Internet? Quais serão as suas políticas e diretrizes em relação a conectividade, comércio, conteúdos, financiamento, segurança e outras questões centrais para a nossa emergente Sociedade da Informação? Estas são algumas das questões-chave que devem ser tratadas no quadro da Governança da Internet.

A EVOLUÇÃO DA GOVERNANÇA DA INTERNET

Um dos aspectos fascinantes da Internet durante o seu desenvolvimento e crescimento iniciais foi a sua governança peculiar. A Internet começou como um projeto de governo. No final da década de 1960, o governo dos Estados Unidos patrocinou o desenvolvimento da Rede da Agência de Projetos de Pesquisa Avançada do Departamento de Defesa (DARPANet), um meio de comunicação resiliente, concebido para resistir a ataques nucleares.

Nos anos 1980, uma comunidade internacional mais ampla estava usando as instalações desta rede, que nesta época passou a ser chamada de Internet. Em 1986, foi fundada a Força-Tarefa de Engenharia da Internet (IETF). A IETF gerenciou o desenvolvimento subseqüente da Internet através de um processo de tomada de decisão cooperativo e consensual, envolvendo uma ampla variedade de indivíduos. Não havia governo central, não havia planejamento central, não havia plano diretor.

Um quadro detalhado da evolução da Governança da Internet está disponível nas páginas 160-161.

Naquela altura dos acontecimentos, a vida era relativamente simples. Não obstante, em 1994, a Fundação Nacional de Ciências dos Estados Unidos (NSF) decidiu envolver o setor privado, terceirizando a administração do Sistema de Nomes de Domínio (DNS) para a Network Solutions Inc. (NSI). A decisão não foi bem recebida pela comunidade da Internet, e assim começou a "Guerra do DNS".

Esta "Guerra do DNS" pôs outros atores em cena: o setor empresarial, organizações internacionais e Estados-nação. Ela terminou em 1998, com o estabelecimento de uma nova organização, a Corporação da Internet para Atribuição de Nomes e Números (ICANN).

Desde 1998 e da fundação da ICANN, o debate sobre a Governança da Internet tem se caracterizado pelo envolvimento mais intensivo de governos nacionais, principalmente através da estrutura da ONU.

NEGOCIAÇÕES INTERNACIONAIS SOBRE GOVERNANÇA DA INTERNET

A Cúpula Mundial sobre a Sociedade da Informação (CMSI), realizada em Genebra em dezembro de 2003, colocou oficialmente a questão da Governança da Internet nas agendas diplomáticas. A Declaração de Princípios e o Plano de Ação adotados na CMSI propunham um certo número de ações no campo da Governança da Internet, inclusive o estabelecimento de um Grupo de Trabalho sobre Governança da Internet (GTGI).

Veja abaixo um extrato da Declaração de Princípios da CMSI sobre Governança da Internet:

> 50. As questões sobre a Governança internacional da Internet devem ser tratadas de maneira coordenada. Nós solicitamos ao Secretário Geral das Nações Unidas a criação de um grupo de trabalho sobre Governança da Internet, num processo aberto e inclusivo que garanta um mecanismo de participação plena e ativa de governos, do setor privado e da sociedade civil tanto dos países em desenvolvimento como dos desenvolvidos, envolvendo organizações e fóruns intergovernamentais e internacionais relevantes, para examinar e formular, até 2005, propostas de ação, conforme apropriado, sobre Governança da Internet.

A seguir, um extrato do Plano de Ação da CMSI sobre Governança da Internet:

> 13. b) Nós solicitamos ao Secretário Geral das Nações Unidas a criação de um grupo de trabalho sobre Governança da Internet, num processo aberto e inclusivo que garanta um mecanismo de participação plena e ativa de governos, do setor privado e da sociedade civil tanto dos países em desenvolvimento como dos desenvolvidos, envolvendo

organizações e fóruns intergovernamentais e internacionais relevantes, para examinar e formular, até 2005, propostas de ação, conforme apropriado, sobre Governança da Internet. O grupo deve, *inter alia*:

i. desenvolver uma definição de trabalho de Governança da Internet;
ii. identificar as questões de políticas públicas que sejam relevantes para a Governança da Internet;
iii. desenvolver uma compreensão comum dos papéis e responsabilidades respectivos de governos, organizações e outros fóruns intergovernamentais e internacionais existentes, bem como do setor privado e da sociedade civil tanto dos países em desenvolvimento como dos desenvolvidos;
iv. preparar um relatório sobre os resultados desta atividade, a ser apresentado para consideração e ações apropriadas na segunda fase da CMSI, em Túnis em 2005.

Com toda a probabilidade, a CMSI e o GTGI abrangem a primeira fase do processo da Governança da Internet, que há de resultar no esclarecimento de questões da Governança da Internet e na definição de uma agenda, bem como na introdução de procedimentos e mecanismos.

Processo de negociação multilateral e Governança da Internet

FASE DE NEGOCIAÇÃO	ATIVIDADE DA CMSI
Pré-negociação	De 1998 até a Cúpula CMSI em Genebra (2003).
Definição de agenda e esclarecimento de questões	Teve início em dezembro de 2003 na Cúpula CMSI em Genebra com a decisão de fundar o Grupo de Trabalho sobre Governança da Internet (GTGI); O GTGI apresentou o seu relatório em junho de 2005; Esta fase do processo foi concluída em Túnis.
A busca de fórmulas	Após Túnis 2005.
Negociação sobre detalhes	
Acordo	
Implementação	

O QUE SIGNIFICA GOVERNANÇA DA INTERNET?

No Fórum Global sobre Governança da Internet, realizado nas Nações Unidas em Nova Iorque em 24-25 de março de 2004, vários oradores deram diversas versões da história dos homens cegos e do elefante.

A moral do poema deixa claro que a discussão do significado de "Governança da Internet" não é apenas um pedantismo ou formalismo lingüístico. Percepções diferentes do significado deste termo desencadeiam diferentes abordagens e expectativas políticas.

Havia seis homens no Industão
A aprender muito inclinados
Eles foram ver o elefante
(Embora da visão todos fossem privados).
.....
E então esses homens do Industão
Discutiram alto e longamente,
Cada qual com sua própria opinião
A avultar-se inflexível e forte.
Embora cada um tivesse parcialmente razão,
E todos estivessem errados!

Extrato do poema "The Blind Men and the Elephant", escrito pelo poeta norte-americano John Godfrey Saxe (1816-1867); o texto integral está disponível no Anexo I.

Especialistas em telecomunicações vêem a questão da Governança da Internet através do prisma do desenvolvimento de infra-estruturas técnicas. Os especialistas em computadores concentram-se no desenvolvimento de vários padrões e aplicações, como XML ou Java. Os especialistas em comunicação destacam a facilitação da comunicação. Ativistas dos direitos humanos vêm a Governança da Internet a partir da perspectiva da liberdade de expressão, da privacidade e de outros direitos humanos básicos. Advogados concentram-se em jurisdição e resolução de disputas legais. Políticos de todo o mundo em geral voltam a sua atenção para a mídia e para questões que impressionem positivamente os seus eleitorados, como o tecno-otimismo (mais computadores = mais educação) e o tratamento das ameaças implicadas (segurança na Internet, proteção à infância). Os diplomatas preocupam-se principalmente com o processo e a proteção de interesses nacionais. A lista de perspectivas profissionais potencialmente conflitantes sobre a questão da Governança da Internet pode estender-se copiosamente.

Cada qual dos termos, "Governança" e "Internet", é objeto de interpretações polêmicas. Alguns autores argumentam que o termo "Internet" não cobre todos os aspectos existentes dos desenvolvimentos da Tecnologia de Informação e Comunicações (TIC). Dois outros termos, "Sociedade da Informação" e "Tecnologia da Informação e Comunicações", são geralmente apresentados como mais abrangentes. Eles incluem áreas que estão fora do domínio da Internet, como a telefonia móvel, por exemplo.

O GTGI propôs a seguinte definição de trabalho do conceito de Governança da Internet: "A Governança da Internet consiste no desenvolvimento e na aplicação por governos, setor privado e sociedade civil, em seus respectivos papéis, de princípios, normas, regulamentos, procedimentos de tomada de decisão e programas compartilhados que modelem a evolução e o uso da Internet."

Esta definição de trabalho constitui um bom ponto de partida para o debate sobre Governança da Internet, que levará inevitavelmente a uma descrição mais detalhada de ambos os termos-chave: "Governança" e "Internet".

Entretanto, o argumento a favor do uso do termo "Internet" tem sido fortalecido pela rápida transição da comunicação global rumo ao uso de TCP/IP como padrão técnico principal das comunicações. A já ubíqua Internet continua a expandir-se numa taxa rápida, não só em termos de número de usuários, mas também em termos dos serviços que oferece, notadamente Voz sobre Protocolo Internet (VoIP), que pode substituir a telefonia convencional.

A outra parte do termo composto, "governança", tem sido causa de controvérsia nos debates recentes, especialmente durante a CMSI. O desentendimento decorre principalmente do uso do termo *governança* como sinônimo de *governo*. Quando o termo "Governança da Internet" foi introduzido no processo da CMSI, muitos países, especialmente os países em desenvolvimento, o vincularam ao conceito de governo. Uma das conseqüências desta abordagem foi acreditar que as questões relativas à Governança da Internet devessem ser tratadas no âmbito intergovernamental, com participação limitada dos outros atores, especialmente os não estatais.

Quais foram as razões principais desta confusão terminológica? É realmente óbvio que "governança" não que dizer "governo"? Não necessariamente. O termo "boa governança" tem sido usado pelo Banco Mundial para promover a reforma de Estados através da introdução de mais transparência, redução da corrupção e aumento da eficiência administrativa. Neste contexto, o termo "governança" estava relacionado com funções centrais de governo.

Outra fonte potencial de confusão é a tradução do termo "*governance*" em outras línguas. Em espanhol, o termo refere-se principalmente a atividades públicas ou governo (*gestión pública, géstion del sector público e función de gobierno*). A referência a atividades públicas/governo também é notável em francês (*gestion d'affaires publiques, efficacité de l'administration, qualité de l'administration e mode de gouvernment*). O português segue um padrão semelhante, referindo-se ao setor público e ao governo (*gestão pública e administração pública*). Esta discrepância na interpretação do termo "governança" pode fornecer uma explicação lingüística do porquê de muitas delegações na CMSI vincularem a questão da Governança da Internet com o setor público, e centrarem as suas deliberações na necessidade de intervenção governamental.

CAIXA DE FERRAMENTAS DA GOVERNANÇA DA INTERNET

O regime de Governança da Internet está em seus primeiríssimos estágios de desenvolvimento. A experiência de outros regimes internacionais (e.g. meio ambiente, transportes aéreos, controle de armas) mostrou que eles tendem a desenvolver uma estrutura comum de referência, valores, percepção das relações de causa e efeito, modos de pensamento, terminologia, vocabulário, jargão e abreviações.

Em muitos casos, a perspectiva comum é influenciada por uma cultura profissional específica (padrões de conhecimento e de comportamento compartilhados pelos membros de uma mesma profissão). O estabelecimento de um quadro comum geralmente ajuda, ao facilitar uma melhor compreensão e entendimento. Não obstante, às vezes os quadros conceituais são usados para proteger o "quintal" de grupos e impedir influências externas. Para citar o lingüista estadunidense Jeffrey Mirel: "Toda língua profissional é uma língua de quintal".

Qualquer regime de Governança da Internet será complexo, pois deverá abranger muitas questões, atores, mecanismos, procedimentos e instrumentos.

As questões atinentes à Internet têm pelo menos cinco dimensões: infraestrutura, legal, econômica, desenvolvimental e sociocultural. Cada uma delas será discutida nos capítulos que seguem. Muitos atores, nos setores privado e público, desempenham papéis em cada uma dessas dimensões. Em sua maioria, eles (superusuários, provedores de serviço de Internet [ISPs], advogados de marcas e patentes, especialistas em desenvolvimento, ativistas da sociedade civil, etc.) têm culturas profissionais muito específicas e bem desenvolvidas.

Cada combinação de questões e atores tem seu propósito, os seus objetivos, a sua terminologia e as suas esferas de colaboração e de influência. Parece que muitas dessas combinações, senão a maioria, estão hoje trabalhando em relativo isolamento das demais. Acrescente-se a isto a multiplicidade de línguas de trabalho que refletem a natureza global dos problemas, e o desafio de juntar estes elementos numa arquitetura de governança coerente se tornará claro! Contudo, com boa-vontade de todas as partes, ele é sem dúvida gerenciável.

A ilustração a seguir, inspirada no artista holandês M. C. Escher, expõe algumas das perspectivas paradoxais associadas à Governança da Internet.

A complexidade ao implementar a Governança da Internet mostra que o pensamento linear, monocausal e "sim-ou-não" não é adequado para lidar com questões da Governança da Internet. Conseqüentemente, postula-se a necessidade de novos instrumentos cognitivos que alcancem esta complexidade e introduzam abordagens e diretrizes comuns.

A proposta essencial de uma Caixa de Ferramentas da Governança da Internet seria:

- organizar as ferramentas atualmente em uso no debate sobre a Governança da Internet;
- criar ferramentas cognitivas adicionais;
- facilitar a natureza inclusiva dos processos de Governança da Internet, fornecendo aos grupos interessados as ferramentas necessárias para compreender as questões, as posições e os desenvolvimentos.

A Caixa de Ferramentas da Governança da Internet consiste em:

- padrões e abordagens;
- diretrizes;
- analogias.

Assim como o processo de Governança da Internet, a Caixa de Ferramentas evolui continuamente. Abordagens, padrões, diretrizes e analogias surgem e desaparecem, dependendo da sua relevância corrente nos processos de negociação.

ABORDAGENS E PADRÕES

Tanto a Governança da Internet como um todo como as questões específicas desta governança têm feito parte, há algum tempo, das discussões políticas e dos intercâmbios acadêmicos. Um certo número de abordagens e padrões emergiu gradualmente, representando pontos em relação aos quais diferenças nas posições de negociação, assim como nas culturas profissionais e nacionais, podem ser identificadas. Identificar abordagens e padrões comuns pode reduzir a complexidade das negociações e ajudar a criar um sistema comum de referências.

Abordagem estreita *versus* abordagem ampla

A governança "estreita" da Internet *versus* a governança "ampla" tem sido uma das questões principais até aqui, refletindo a existência de diferentes abordagens e interesses no processo de Governança da Internet. A abordagem "estreita" concentra-se na infra-estrutura da Internet (Sistema de Nomes de Domínio, Números de IP, superservidores-raiz) e na posição da ICANN como o ator-chave deste campo.

Segundo a abordagem "ampla", as negociações sobre a Governança da Internet deveriam ir além das questões infra-estruturais e lidar com outras questões legais, econômicas, desenvolvimentais e socioculturais. Fazer a distinção entre essas duas abordagens é particularmente importante na fase inicial, de definição de agenda nas negociações da Internet.

A abordagem ampla é apoiada implicitamente pela Declaração da CMSI, que outorga ao GTGI a tarefa de "identificar as questões de política públicas que são relevantes para a Governança da Internet." Esta abordagem também é predominante nas discussões políticas e acadêmicas sobre Governança da Internet.

O atual debate evoluiu da fase "sim-ou-não", passando a preocupar-se com a identificação e o devido equilíbrio entre a abordagem "estreita" (ICANN-questões correlatas a registro de domínios e sua resolução) e a abordagem "ampla" (outros aspectos da Governança da Internet).

Aspectos técnicos *versus* aspectos políticos

Um desafio significativo do processo da Governança da Internet será a integração de aspectos técnicos e políticos, já que é difícil estabelecer uma distinção clara entre eles. Soluções técnicas não são neutras. Em última análise, cada solução/opção técnica promove certos interesses, fortalece o poder de certos grupos e, em certa medida, produz um impacto na vida social, política e econômica.

Em alguns casos, o objetivo político inicial de uma solução técnica acaba se transformando. Por exemplo, a arquitetura de networking ponta-a-ponta e de sistema de comutação por pacotes foi desenhada com o objetivo político de criar uma rede robusta capaz de sobreviver a um ataque nuclear. A mesma arquitetura tornou-se mais tarde a base para o desenvolvimento da criatividade e da liberdade de expressão na Internet.

Outras soluções técnicas, como meios eletrônicos para a proteção do direito autoral, são intencionalmente criadas a fim de substituir ou impor certas diretrizes (neste caso, proteção mais estrita ao direito autoral).

No caso da Internet, durante muito tempo tanto os aspectos técnicos como os políticos foram governados por apenas um grupo social – a comunidade inicial da Internet. Com o crescimento da Internet e o surgimento de novos acionários na década de 1990, principalmente setores empresariais e governos, aquela unidade de tecnologia e de política foi rompida. A reforma da Governança da Internet, inclusive com a criação da ICANN, foi uma tentativa de restabelecer o equilíbrio perdido. A questão resta em aberto, e muito provavelmente vai constituir um dos tópicos potencialmente polêmicos da CMSI/GTGI.

Abordagem "tradicional-realista" *versus* "neocibernética"

Há duas abordagens para quase todas as questões sobre Governança da Internet. A abordagem "tradicional-realista" – ou "vinho novo em odres velhos" – argumenta que a Internet não introduz nada de novo no campo da governança. Que a Internet é apenas mais uma invenção nova, que, do ponto de vista da governança, não é diferente das suas predecessoras: o telégrafo, o telefone ou o rádio.

Em discussões legais, por exemplo, esta abordagem argumenta que as leis existentes podem ser aplicadas à Internet apenas com ajustes menores. Na medida em que envolve comunicação entre pessoas, a Internet não seria diferente do telefone ou do telégrafo, e poderia ser regulamentada como outros dispositivos de comunicação. No campo econômico, esta abordagem argumenta que não há diferenças entre o comércio comum e o comércio eletrônico. Conseqüentemente, não há necessidade de tratamento legal especial para o "e-comércio". A abordagem "realista" também é contra a moratória dos "e-impostos", a moratória fiscal para lojas virtuais.

A abordagem "nova-cibernética" – ou "vinho novo em odres novos" – argumenta que a Internet é um dispositivo fundamentalmente diferente de todos os anteriores. Assim, exige uma governança fundamentalmente diferente. Esta abordagem foi muito popular nos primeiros dias da Internet. Chegou-se até a esperar, então, que os métodos iniciais inovadores de governo da Internet – "consenso aproximado e código funcionando" – pudessem se tornar modelo para a regulamentação de outras áreas da atividade humana. A premissa básica da abordagem "cibernética" é que a Internet desvinculou a nossa realidade social e política do mundo dos Estados soberanos. O ciberespaço é diferente do espaço real, por isto requer uma forma diferente de governança.

A influência desta abordagem foi significativa no processo de criação da ICANN, a qual, por exemplo, minimizou a influência dos governos do mundo "real". A abordagem "cibernética" foi moderada pela reforma da ICANN em 2002, que fortaleceu o papel dos governos e trouxe a ICANN para mais perto da realidade política.

No campo legal, a escola "cibernética" de pensamento argumenta que as leis existentes sobre jurisdição, cibercrime e contratos não pode ser aplicada à Internet e que novas leis devem ser criadas.

Considerando a contínua interação entre essas duas abordagens, o dilema "tradicional-realista" *versus* "neocibernética" provavelmente vai perdurar e influenciar fortemente as negociações sobre a Governança da Internet.

Estrutura descentralizada versus estrutura centralizada de Governança da Internet

Segundo o ponto de vista descentralizador, a estrutura de governança deveria refletir a própria configuração da Internet: uma rede de redes.

Uma configuração tão complexa não caberia, não poderia ser posta sob um único guarda-chuva de governança, como uma organização internacional. Outro argumento é que a ausência de governança centralizada é um dos maiores fatores a permitir o rápido crescimento da Internet. Esta opinião é sustentada principalmente pela comunidade técnica da Internet e pelos países desenvolvidos.

A abordagem centralizadora, por outro lado, baseia-se em parte nas dificuldades práticas sentidas pelos países com limitação de recursos humanos e financeiros para acompanhar as discussões sobre Governança da Internet num cenário altamente descentralizado e multi-institucional. Esses países experimentam dificuldades para comparecer a encontros nos principais centros diplomáticos (Genebra e Nova Iorque), e mais ainda para acompanhar as atividades de outras instituições, como ICANN, W3C e IETF. Essas nações, principalmente entre os países em desenvolvimento, argumentam em favor de um modelo sinérgico, ao estilo do conceito norte-americano de "*one-stop shop*", de preferência no quadro de uma só organização internacional.

Internet e o bem público

A maior parte da infra-estrutura técnica através da qual o tráfego na Internet é canalizado pertence a companhias privadas e estatais, tipicamente operadoras de telecomunicações. Trata-se de algo análogo a uma companhia mercante transportando contêineres. Contudo, as vias de navegação são abertas e reguladas pelo Direito do Mar, que afirma que os mares abertos são *res communis omnium*, ao passo em que a rede de espinhas dorsais (*backbones*) que transporta dados é propriedade de companhias de telecomunicação. Isto levanta um certo número de questões:

- É possível exigir que empresas privadas administrem as suas propriedades privadas – espinhas dorsais de Internet – no interesse público?
- Pode a Internet, ou parte dela, ser considerada como um bem público global?
- Pode o velho conceito romano de *res communis omnium* ser aplicado à Internet, como no caso de alguns aspectos do Direito do Mar?

O principal desafio neste dilema do público *versus* o privado será, por um lado, propiciar ao setor privado um ambiente comercial adequado, mas, por outro lado, garantir o desenvolvimento da Internet como recurso público, consistindo de conhecimentos e informações de propriedade comum. Para mais informações, consulte por favor a página 133.

A geografia e a Internet

Uma das pressuposições iniciais sobre a Internet era de que ela sobrepujaria as fronteiras nacionais e provocaria a erosão do conceito de soberania. Em sua célebre "Declaração de Independência do Ciberespaço", John Perry Barlow enviou a seguinte mensagem a todos os governos: "Vocês não são bem-vindos entre nós. Não exercem nenhuma soberania sobre o lugar onde nos reunimos... Vocês não têm o direito moral de nos impor regras e nem possuem quaisquer meios de coação que devêssemos temer de verdade... O ciberespaço não está dentro das suas fronteiras."

Esta declaração é um exemplo do tecno-otimismo predominante, típico de meados dos anos 1990. Desde a declaração de Barlow, houve muitos desenvolvimentos, inclusive de programas de geolocalização mais sofisticados. Hoje, ainda é difícil identificar exatamente quem está atrás do monitor, mas é bastante simples identificar através de que provedor de serviço de Internet (ISP) que a rede mundial foi acessada. Além disso, mundo afora as leis nacionais mais recentes exigem que os ISPs identifiquem os seus usuários e, se assim solicitados, que forneçam a informação necessária sobre eles às autoridades.

Quanto mais a rede estiver ancorada na geografia, menos peculiar será a Governança da Internet. Por exemplo, com a possibilidade de localizar geograficamente os usuários e transações da Internet, a complexa questão da jurisdição sobre a Internet pode ser mais facilmente resolvida através das leis já existentes.

A abordagem "fazer conforme o que prega"

A abordagem "fazer conforme o que prega" promove o uso de ferramentas online para negociar as questões do mundo online. O processo de negociação da Governança da Internet apresenta um considerável desafio no âmbito da diplomacia internacional, que exige tanto o uso de técnicas comprovadas e eficientes de negociação como a introdução de abordagens inovadoras. Uma das técnicas inovadoras essenciais poderia ser o uso de ferramentas online para as negociações.

Negociações que usassem a Internet como base seriam facilitadas pela participação de um grupo maior de acionários, especialmente aqueles que não podem bancar a sua participação em conferências diplomáticas tradicionais. Uma prioridade seria dar assistência aos países em desenvolvimento a fim de viabilizar a sua participação significativa no processo de Governança da Internet.

DIRETRIZES

As diretrizes representam certos valores e interesses que devem ser promovidos por meio do regime emergente de Governança da Internet. Algumas dessas diretrizes foram adotadas pela CMSI, como a transparência e o seu caráter inclusivo. Outros princípios foram introduzidos, de modo principalmente tácito, através das discussões sobre a Governança da Internet.

"Não reinvente a roda"

Qualquer iniciativa no campo da Governança da Internet deve começar das regulamentações existentes, que podem ser divididas em três grandes grupos:

a) as criadas para a Internet (e.g. ICANN);
b) as que exigem ajustes consideráveis para adquirirem a capacidade de lidar com questões ligadas à Internet (e.g. proteção de marcas e patentes; e-impostos);
c) as que podem ser aplicadas à Internet sem ajustes significativos (e.g. proteção da liberdade de expressão).

O uso de regras existentes incrementaria significativamente a estabilidade legal e reduziria a complexidade do desenvolvimento do regime de Governança da Internet.

"Se não estiver quebrado, não conserte!"

A Governança da Internet deve preservar a funcionalidade e a robustez atuais da rede, ainda que permanecendo flexível o bastante para adotar modificações que a conduzam rumo a mais funcionalidade e maior legitimidade. O consenso geral reconhece que a estabilidade e a funcionalidade da Internet devem constituir um dos princípios diretores da Governança da Internet. A estabilidade da Internet deve ser preservada através da abordagem inicial de "código funcionando", a qual envolve a introdução gradual de modificações suficientemente testadas na infra-estrutura técnica.

Não obstante, alguns atores temem que o uso do *slogan* "Se não estiver quebrado, não conserte" possa servir como um manto protetor contra toda e qualquer mudança na atual Governança da Internet, inclusive aquelas não necessariamente ligadas à infra-estrutura técnica. Uma solução seria usá-lo como critério de avaliação nas decisões especificamente ligadas à Governança da Internet (e.g. introdução de novos protocolos e de outras mudanças nos mecanismos de tomada de decisão).

Governança da Internet e desenvolvimento

O debate em curso salienta a grande relevância desenvolvimental das seguintes questões de Governança da Internet: encargos de interconexão, distribuição de números de IP, proteção de propriedade intelectual e promoção do comércio eletrônico. O processo de Governança da Internet deve orientar-se pelo conjunto dos objetivos para o desenvolvimento da CMSI e pelos chamados Objetivos de Desenvolvimento do Milênio, das Nações Unidas.

Promoção de uma abordagem holística e priorização

Uma abordagem holística facilitará o tratamento não apenas dos aspectos técnicos, mas também das dimensões legais, sociais, econômicas e desenvolvimentais do avanço da Internet. Está abordagem também deverá levar em consideração a convergência crescente das tecnologias digitais, inclusive a migração dos serviços de telecomunicações para os protocolos Internet.

Ao mesmo tempo em que adotam uma abordagem holística para as negociações da Governança da Internet, os acionários devem identificar questões prioritárias ligadas aos seus interesses específicos. Nem os países em desenvolvimento nem os países desenvolvidos são grupos homogêneos. Entre os países em desenvolvimento, há consideráveis diferenças de prioridades, de níveis de desenvolvimento e de implantação de tecnologias da informação (e.g. entre países avançados no âmbito das TICs, como a Índia, a China e o Brasil, e alguns países menos desenvolvidos da África subsaariana).

"A visão das árvores politizadas encobrindo o bosque das questões"

Na agenda da Governança da Internet, a abordagem holística e a noção de priorização devem ajudar os acionários tanto dos países desenvolvidos quanto dos países em desenvolvimento a focalizar um conjunto particular de questões.

Isto levará possivelmente a negociações mais substantivas e menos politizadas. Os acionários se agrupariam em torno de questões, em vez de fazê-lo em torno de linhas divisórias por tradição altamente politizadas (e.g. países desenvolvidos – em desenvolvimento; governos – sociedade civil).

DIRETRIZES DA ICANN

O Documento Estratégico (*White Paper*) dos Estados Unidos sobre Governança da Internet (1998) especifica os seguintes princípios diretores para a fundação da ICANN:

- Estabilidade – o funcionamento da Internet não pode ser interrompido, especialmente na operação das suas estruturas-chave, inclusive os "domínios-raiz";
- Competição – é importante estimular a criatividade e a flexibilidade, as quais contribuirão para o desenvolvimento futuro da Internet;
- Tomada de decisão – o novo sistema deve acomodar algumas das regras e princípios iniciais da Internet, inclusive o estilo gente-comum de organização, a abertura, etc.;
- Representação – o novo quadro deve acomodar os acionários essenciais: tanto geograficamente (diferentes países) como profissionalmente (diferentes comunidades profissionais).

Transformar soluções técnicas tácitas em princípios políticos explícitos

É opinião comum no seio da comunidade da Internet que certos valores sociais, como a liberdade de comunicação, são facilitados pelo modo como a Internet é tecnicamente desenhada (o princípio "ponta-a-ponta"). Esta opinião pode levar à conclusão equivocada de que soluções tecnológicas sejam suficientes para promover e proteger valores sociais. Os últimos desenvolvimentos da Internet, como o uso de tecnologias *firewall* para restringir o fluxo de informação, mostram que a tecnologia pode ser usada de muitas maneiras, inclusive aparentemente contraditórias. Princípios, como a liberdade de comunicação, devem ser claramente afirmados no âmbito das diretrizes e políticas, e não tacitamente presumidos no âmbito técnico.

O princípio da neutralidade tecnológica

Este princípio está estreitamente ligado ao anterior. A noção de neutralidade tecnológica implica que diretrizes e políticas não dependam de dispositivos técnicos ou tecnológicos específicos. Assim, por exemplo, regulamentos para a proteção da privacidade devem especificar o que deve ser protegido (e.g. dados pessoais, registros médicos), e não como deve ser protegido (e.g. acesso a bancos de dados, criptografia e segurança).

A neutralidade tecnológica propicia muitas vantagens de governança. Em primeiro lugar, desvincula a governança de toda e qualquer tecnologia particular, abrindo-a para desenvolvimentos tecnológicos futuros. Em segundo, a neutralidade tecnológica é o princípio regulador mais apropriado para a convergência futura das principais tecnologias (telecomunicações, mídia, Internet, etc.).

A União Européia introduziu a neutralidade tecnológica como uma das pedras fundamentais das políticas de telecomunicações. Ao mesmo tempo em que a neutralidade tecnológica é um principio claramente apropriado, já é possível imaginar as muitas dificuldades que irão ocorrer na transição dos regulamentos de telecomunicação hoje existentes para novos. Eles já são óbvios em áreas como Voz sobre IP.

O risco de gerir a sociedade através de código de programadores

Um aspecto chave da relação existente entre tecnologia e política foi identificado por Lawrence Lessing, que descreveu que, com a sua dependência crescente da Internet, a sociedade moderna podia acabar sendo ordenada por códigos de programação em vez de ser regulada por leis. Algumas funções legislativas de parlamento e governo poderiam ser assumidas *de facto* por companhias informáticas e desenvolvedores de programas. Através de uma combinação de programas e soluções técnicas, eles adquiririam a capacidade de influenciar crescentemente a vida nas sociedades fundadas na Internet. Se a gestão social por códigos em vez de leis vier um dia a acontecer, isto representaria um questionamento essencial da própria base da organização política e social da sociedade moderna.

ANALOGIAS

> Embora analogias sejam freqüentemente equívocas, pelo menos são uma coisa equívoca que possuímos.
>
> *Samuel Butler*

A analogia nos ajuda a compreender desenvolvimentos novos nos termos daquilo que já nos é conhecido. Apesar dos riscos, estabelecer paralelos entre exemplos passados e correntes é um processo mental chave tanto no direito como na política. A maioria das disputas legais envolvendo a Internet é resolvida através de analogias.

O uso de analogias no que diz respeito à Governança da Internet tem algumas limitações importantes. Em primeiro lugar, o termo Internet é muito amplo, e abrange uma variedade de serviços, incluindo *e-mail* (ver a analogia entre Internet e telefone), *web* (ver a analogia entre Internet e televisão), e bases de dados (ver analogia entre Internet e bibliotecas). Uma analogia a qualquer sistema particular pode supersimplificar a compreensão da Internet.

Em segundo, com a convergência crescente de vários serviços de telecomunicações e de mídia, as diferenças tradicionais entre eles estão se diluindo. Por exemplo, com a introdução do serviço Voz sobre IP fica cada vez mais difícil fazer uma distinção clara entre Internet e telefonia.

Apesar dos fatores limitadores, analogias ainda são eficazes, uma ferramenta cognitiva importante para resolver disputas legais e desenvolver um regime de Governança da Internet. Algumas das analogias usadas com mais freqüência serão discutidas a seguir.

Internet – telefonia

Semelhanças: Nos primeiros dias da Internet, esta analogia foi influenciada pelo fato de o telefone ser usado para facultar o acesso discado. Além disso, cabe uma analogia funcional entre o telefone a Internet (*e-mail* e bate-papo), sendo ambos meios de comunicação direta e pessoal.

Uma analogia mais recente entre o telefone e a Internet refere-se ao possível uso do sistema de numeração telefônica como solução para a organização do sistema de nomes de domínio.

Diferenças: A Internet usa pacotes em vez de circuitos (como o telefone). À diferença da telefonia, a Internet não pode garantir serviços; ela só pode garantir o "Melhor Esforço". A analogia destaca apenas um aspecto da Internet: a comunicação via *e-mail* ou bate-papo. Outras aplicações essenciais da Internet, como a Rede Mundial de Computadores (WWW), serviços interativos, etc., não compartilham elementos comuns com a telefonia.

Usada por: Aqueles que se opõem à regulamentação do conteúdo da Internet (principalmente nos Estados Unidos). Se a Internet for análoga ao telefone, o seu conteúdo não poderá ser controlado, como é o caso do telefone.

A analogia também é usada pelos grupos que argumentam que a Internet deveria ser governada como outros sistemas de comunicação (e.g. telefonia, correios), por autoridades nacionais exercendo um papel de coordenação de organizações internacionais, como a União Internacional de Telecomunicações (UIT).

Paul Twomy, o presidente da ICANN, usou a seguinte analogia entre o sistema postal e a função da ICANN: "Se você pensar a Internet como uma agência de correio ou um sistema postal, nome de domínio e endereçamento de IP ali estão essencialmente para garantir que o endereço na parte frontal do envelope funcione. Eles nada têm a ver com o que você põe dentro do envelope, com quem envia o envelope, quem pode ler o envelope, quanto tempo o envelope demora para chegar ou com qual o preço do envelope. Nenhuma dessas questões é importante para as funções da ICANN. Sua função limita-se apenas a garantir que o endereço funcione."

Internet – correios

Semelhanças: Há uma analogia de função, isto é, a entrega de mensagens. O próprio nome "*e-mail*" salienta esta semelhança.

Diferenças: Esta analogia só diz respeito a um serviço da Internet – o e-mail. Além disso, os serviços postais têm uma estrutura intermediária muito mais elaborada entre remetentes e destinatários de mensagens do que o sistema de e-mail, no qual a função ativa de intermediário é desempenhada por ISPs ou um serviço provedor de e-mail, como o Yahoo! ou o Hotmail.

Usada por: A Convenção Postal Universal fez a seguinte analogia entre os serviços postais e o correio eletrônico: "O correio eletrônico é um serviço postal que usa as telecomunicações para transmitir." Esta analogia pode ter conseqüências, por exemplo, no tocante à entrega de documentos oficiais: receber uma comunicação judicial via e-mail teria de ser considerado entrega oficial.

As famílias dos soldados estadunidenses que morreram no Iraque também tentaram fazer uso de uma analogia entre correio (cartas) e correio eletrônico, a fim de obter acesso aos *e-mails* e *blogs* privados dos seus entes queridos, argumentando que deveriam ter o direito de herdar seus *e-mails* e *blogs* como teriam o de herdar suas cartas e diários.

Os provedores de serviço ou de acesso à Internet (ISPs) acharam difícil lidar com este tipo de problema, altamente emocional. Em vez de seguirem acompanhando a analogia entre cartas e *e-mails*, a maioria dos ISPs negou o acesso, baseando-se no acordo de privacidade assinado com os seus usuários.

Internet – televisão

Semelhanças: A analogia inicial dizia respeito à semelhança física existente entre monitores de computadores e de aparelhos televisores. Uma analogia mais sofisticada inspira-se no uso de ambas as mídias – a rede mundial e a televisão – para transmitir sinal.

Diferenças: Assim como com a noção de telefonia, o conceito de Internet é mais amplo do que o de televisão. Além das semelhanças entre as telas de computador e de televisão, existem diferenças estruturais essenciais entre eles. A televisão é um meio "um-para-muitos" de transmissão de sinal para espectadores, ao passo que a Internet facilita muitos tipos deferentes de comunicação (um-para-um; um-para-muitos; muitos-para-muitos).

Usada por: Esta analogia é usada por aqueles que desejam introduzir um controle mais estrito de conteúdos na Internet. Na opinião deles, considerando o seu poder como meio de comunicação de massa similar à televisão, a Internet deveria ser rigorosamente controlada. O governo dos Estados Unidos tentou usar esta analogia no famoso caso Janet Reno contra a União pelas Liberdades Civis Americanas. A causa judicial foi desencadeada pela Lei de Decência nas Comunicações, que estipula controle estrito de conteúdos a fim de evitar que crianças sejam expostas a materiais pornográficos, no caso via Internet. O tribunal recusou-se a reconhecer a analogia com a televisão.

Internet – bibliotecas

Semelhanças: A Internet às vezes é vista como um vasto repertório de informações e o termo "biblioteca" é usado freqüentemente para descrevê-la – "imensa biblioteca digital", "ciberbiblioteca", "Biblioteca de Alexandria do século XXI", etc.

Diferenças: A estocagem de informações e dados constitui apenas um aspecto da Internet, e há consideráveis diferenças entre as bibliotecas e a Internet:

a) bibliotecas tradicionais visam prestar serviço a indivíduos residentes num local particular (cidade, país, etc.), ao passo que a Internet é global;
b) livros, artigos e jornais são publicados mediante procedimentos garantidores de qualidade (editores). A Internet não tem editores;
c) bibliotecas são organizadas segundo esquemas específicos de classificação, que permitem aos usuários localizar os livros em suas coleções. Exceto por uns poucos diretórios, como o Yahoo! e o Google, que só cobrem uma pequena parte da informação disponível em toda a Internet, este tipo de esquema de classificação não existe para a Internet.
d) excetuando-se as descrições por palavras-chave, os conteúdos de uma livraria (textos em livros e artigos) só são acessíveis se o usuário tomar por empréstimo um livro particular. O conteúdo da Internet está imediatamente acessível através de buscadores ou motores de busca.

Usada por: Vários projetos cujo fim é criar um sistema de informação e conhecimento abrangente sobre questões específicas (portais, bancos de dados, etc.).

Internet – vídeo, fotocópia

Semelhanças: Esta analogia centra-se na questão da reprodução e da disseminação de conteúdos (e.g. textos e livros). Os computadores simplificaram a processo de reprodução através do recurso "copiar e colar", o qual, por sua vez, tornou muito mais simples a disseminação através da Internet.

Diferenças: O computador tem uma função muito mais ampla do que apenas copiar materiais, embora cópias em si sejam muitos mais simples na Internet do que com um VCR ou uma focopiadora.

Usada por: Esta analogia foi empregada no contexto da Lei de Direitos Autorais Digitais do Milênio (DMCA), que penaliza instituições que contribuam para a violação de direitos autorais (desenvolvimento de programas que quebrem a proteção a direitos autorais, etc.). O contra-argumento em casos dessa natureza foi que, assim como os fabricantes de VCRs e de máquinas fotocopiadoras, os desenvolvedores de programas não são capazes de prever se seus produtos serão ou não usados ilegalmente. A analogia foi usada nos processos contra desenvolvedores de programas ao estilo Napster de compartilhamento de arquivos entre usuários (P2P ou "*peer-to-peer*"), como a Grokster e a StreamCast.

Internet – rodovia

Semelhanças: Esta analogia vincula-se à cultura norte-americana e à importância que ela dá a rodovias e ferrovias, revelando por meio disto o fascínio nacional por descobertas e novas fronteiras.

Diferenças: A não ser pelo aspecto de transporte da Internet, não há outras semelhanças entre a Internet e rodovias. A Internet trafega materiais intangíveis (dados), ao passo que as rodovias facultam o transporte de bens e de pessoas.

Usada por: A analogia da rodovia foi empregada em meados dos anos 1990, depois que Al Gore introduziu o termo "super-rodovia da informação". O termo "rodovia" também foi usado pelo governo alemão, a fim de justificar a introdução de leis mais rigorosas de controle de conteúdo em junho de 1997: "Trata-se de uma lei liberal que nada tem a ver com censura, mas que estabelece claramente as condições do que o provedor pode ou não pode fazer. A Internet é um meio de transporte e de distribuição de conhecimento... assim como nas rodovias, existe a necessidade de diretrizes para ambos os tipos de tráfego."

A CLASSIFICAÇÃO DAS QUESTÕES DA GOVERNANÇA DA INTERNET

A Governança da Internet é um campo novo e complexo que exige mapeamento e classificação conceituais iniciais. A complexidade da Governança da Internet está ligada à sua natureza multidisciplinar, abrangente de uma variedade de aspectos, incluindo tecnologia, dimensão socioeconômica, desenvolvimento, direito e política.

A necessidade de um mapeamento conceitual inicial é tanto acadêmica quanto prática. No lado acadêmico, produz-se um volume crescente de pesquisas sobre a Governança da Internet, mas centrado principalmente na ICANN e outras questões pertencentes à chamada abordagem "estreita". Ainda falta uma perspectiva teórica mais ampla, particularmente sobre os aspectos internacionais da Governança da Internet. A necessidade prática de classificação ficou claramente demonstrada durante o processo da CMSI. Muitos atores, inclusive Estados-nação, tiveram dificuldades para alcançar a complexidade da Governança da Internet. Um mapeamento conceitual do campo deve contribuir para negociações mais eficientes tanto no contexto da CMSI como no de outros processos de negociação multilateral de questões relacionadas à Internet.

A classificação pode auxiliar os atores da Governança da Internet a:

- identificarem claramente as questões principais que exigem negociação;
- reduzirem o "ruído" causado por interpretações contraditórias de conceitos essenciais durante as negociações;
- evitarem a duplicação de esforços ao lidar com as mesmas questões em múltiplos fóruns;
- manterem um equilíbrio apropriado entre uma perspectiva ampla e questões específicas, evitando deste modo o problema de "a visão das árvores encobrir a visão do bosque".

Em última análise, o mapeamento cuidadoso das questões relativas à Internet há de tornar o processo de negociação da Governança da Internet mais eficiente. Em termos econômicos, reduzirá os custos de transação – ou, em outras palavras, o tempo total exigido para as negociações. Isto traria benefícios particularmente para os países com limitação de recursos humanos e financeiros, viabilizando deste modo a ampliação da sua participação. Processos de negociação obscuros e confusos exigem, proporcionalmente, mais tempo e mais recursos humanos.

A classificação da DiploFoudation da Governança da Internet reúne todas as questões em cinco grupos. Para ajustar-se à linguagem da diplomacia, a DiploFoudation adotou o termo "cesta" (o termo foi introduzido na prática diplomática durante as negociações da Organização para a Segurança e Cooperação na Europa (OSCE). As cinco cestas seguintes vêm sendo usadas desde 1997, quando a DiploFoudation desenvolveu o seu esquema de classificação:

1) infra-estrutura e padronização/normalização;
2) legal;
3) econômica;
4) desenvolvimento;
5) sociocultural.

A classificação da Governança da Internet da DiploFoudation é a base conceitual da abordagem global da fundação neste campo, incluindo treinamento/educação, pesquisa e desenvolvimento de ferramentas. Desde a sua introdução em 1997, a classificação foi usada em cursos freqüentados por mais de 300 estudantes, bem como por muitos pesquisadores. Retornos e comentários regulares sobre este esquema propiciaram ajustes constantes. Conseqüentemente, a classificação em curso baseia-se em numerosas interações, assim como em conhecimentos e experiências agregados.

O modelo das cinco cestas é representado metaforicamente na ilustração "Edifício em construção" na página seguinte.

"Edifício em construção": Estamos construindo uma Torre de Babel do século XXI?

Um quadro de Pieter Brueghel o Velho (1563), exibido no Museu Kunsthistorisches, em Viena, mostra a construção da Torre de Babel (outra pintura, menor, do mesmo ano e sobre o mesmo tema, encontra-se no Museu Boijmans Van Beuningen, em Roterdam). O Livro de Gênesis (11:7) faz referência à construção da Torre de Babel: "Vinde, desçamos, e confundamos ali a sua linguagem, para que um não entenda linguagem do outro."

A analogia da construção da Torre de Babel parece apropriada ao olharmos para os desafios propostos pela Internet. A comparação incitou os autores a considerarem um outro edifício em construção – que não visa alcançar os céus, mas ao menos todos no planeta. A DiploFoudation desenvolveu um quadro para a discussão da Governança da Internet, ilustrado na figura na página anterior. Cada piso daquele edifício será discutido nos capítulos a seguir. É importante compreender que todos os pisos do edifício estão vinculados, e que a construção hoje está em curso e não terá fim.

SEÇÃO 2

A cesta da infra-estrutura e da padronização/ normalização

A CESTA DA INFRA-ESTRUTURA E DA PADRONIZAÇÃO/NORMALIZAÇÃO

A cesta da infra-estrutura e da padronização ou normalização abrange as questões básicas, essencialmente técnicas, relativas ao funcionamento da Internet. Na ilustração "Edifício em construção" da Governança da Internet da DiploFoudation, o térreo representa a infra-estrutura e a padronização (ver pág 30).

As questões desta cesta se dividem em dois grupos. O primeiro, que abrange as questões essenciais sem as quais a Internet e a Rede Mundial de Computadores não poderiam existir, é representada nas três camadas a seguir:

Uma das forças da Internet está nesta arquitetura em camadas. A camada da infra-estrutura de Internet permanece independente da infra-estrutura de telecomunicações (a camada abaixo) e dos padrões de aplicação (a camada acima).

1. a infra-estrutura de telecomunicações, pela qual passa todo o tráfego da Internet;

2. os padrões e serviços técnicos – a infra-estrutura que faz a Internet funcionar (e.g. TCP/IP, DNS, SSL); e
3. os conteúdos e padrões de aplicação (e.g HTML, XML).

O segundo grupo reúne as questões relativas à salvaguarda da operação segura e estável da infra-estrutura, incluindo resolução de domínios, segurança na Internet, criptografia e *spam*.

A INFRA-ESTRUTURA DE TELECOMUNICAÇÕES

A SITUAÇÃO ATUAL

Dados de Internet podem viajar através de uma gama diversificada de suportes: fios telefônicos, cabos de fibra óptica, satélites, microondas e conexões sem fio. Mesmo a rede elétrica básica pode ser usada para retransmitir tráfego de Internet. O rápido crescimento da Internet desencadeou um aumento considerável da capacidade de telecomunicação. Estima-se que, de 1998 para cá, a capacidade de telecomunicação tenha crescido quinhentas vezes, devido a uma combinação de inovações tecnológicas e investimentos em novas instalações de telecomunicação.

Como a camada das telecomunicações suporta o tráfego da Internet, qualquer regulamentação nova vinculada à área das telecomunicações também terá impacto, inevitavelmente, na Internet. A infra-estrutura de telecomunicações é regulamentada tanto no nível nacional como no internacional por uma variedade de organizações públicas e privadas.

Tradicionalmente, as telecomunicações internacionais eram coordenadas pela União Internacional de Telecomunicações (UIT), que desenvolveu regras elaboradas cobrindo a relação entre operadores nacionais, atribuição de faixas de rádio e gestão de posicionamento de satélites.

Finalmente, a abordagem liberal prevaleceu sobre os monopólios das telecomunicações. O processo de liberalização foi formalizado internacionalmente em 1998, através do Acordo sobre Serviços Básicos de Telecomunicações (BTA) da Organização Mundial do Comércio (OMC), em cujos termos mais de cem países deram início a um processo de

liberalização caracterizado pela privatização dos monopólios nacionais de telecomunicação, a introdução da competição e o estabelecimento de agências reguladoras nacionais.

O Regulamento Internacional da UIT, de 1998, facilitou a liberalização internacional dos preços e serviços, e permitiu que serviços básicos, como linhas sob contrato internacional de *leasing*, fossem usados de maneira mais inovadora no campo da Internet.

A OMC moveu-se gradualmente para o centro do regime internacional de telecomunicações, tradicionalmente governado pela UIT. Contudo, os papéis da OMC e da UIT são totalmente distintos. A UIT define padrões técnicos detalhados, regulamentos internacionais específicos da área das telecomunicações, e também dá assistência a países em desenvolvimento. A OMC provê um quadro de regras gerais de mercado.

Depois da liberalização, o quase monopólio da UIT, como principal instituição definidora de padrões para as telecomunicações, foi erodido por outros órgãos e organizações profissionais, como a Instituto Europeu de Padronização das Telecomunicações (ETSI), que desenvolveu padrões GSM, e o Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE), que desenvolveu o TCP/IP e outros protocolos relativos à Internet.

A liberalização dos mercados nacionais de telecomunicação deu às grandes companhias de telecomunicações, como AT&T, Cable and Wireless, France Telecom, Sprint e WorldCom, a oportunidade de estender globalmente a sua cobertura de mercado. Como a maior parte do tráfego é suportado pelas infra-estruturas de telecomunicações dessas companhias, elas têm grande influência nos processos da Governança da Internet.

QUESTÕES

A rede de distribuição ou última milha – separando os loops locais

A conexão entre os provedores de serviço de Internet e seus clientes individuais é chamada de "*loop* local" (ou última milha). Problemas em "*loops* locais" são um obstáculo para a disseminação do uso da Internet em muitos países, principalmente entre aqueles em desenvolvimento. Em geral, isto se deve ao subdesenvolvimento da infra-estrutura de telecomunicações. Em alguns países em desenvolvimento com grandes áreas territoriais, é difícil conectar cidades e povoados distantes através das redes terrestres tradicionais de telecomunicação.

Assim, considera-se cada vez mais que a comunicação sem fio seja a melhor solução de baixo custo para o problema dos "*loops* locais".

Porém, além da disponibilidade crescente de opções técnicas, a solução do problemas dos "*loops* locais" também depende da liberalização deste segmento do mercado das telecomunicações.

A liberalização dos mercados de telecomunicação

Um número considerável de países liberalizou os seus mercados de telecomunicação. Não obstante, muitos países em desenvolvimento com monopólios na área das telecomunicações estão diante de uma difícil escolha: como liberalizar e tornar seus mercados de telecomunicações mais eficientes e, ao mesmo tempo, preservar a importante fonte de arrecadação proveniente exatamente dos monopólios existentes nas telecomunicações?

Os encaminhamentos que têm sido sugeridos para solucionar este complexo problema são: ajuda externa; transição gradual; e vincular o processo de liberalização à proteção do interesse público (como o ocorrido no Brasil através das metas de universalização).

O definição de padrões de infra-estrutura técnica

Cada vez mais, os padrões técnicos vêm sendo implantados por instituições privadas e profissionais. Por exemplo, o padrão WiFi, IEEE 802.11b, foi desenvolvido pelo Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE). A certificação de equipamento compatível com WiFi é feita pela WiFi Alliance. A própria atribuição de definir ou implementar padrões dá a essas instituições uma considerável influência sobre o mercado.

Tecnologia, padrões e política

O debate sobre protocolos de rede ilustra como os padrões podem ser a continuação da política por outros meios. Enquanto outras intervenções de governo no mundo dos negócios e da tecnologia (como regulamentos de segurança e ações antitruste) são prontamente percebidas como carregadas de significância política e social, a adoção de padrões técnicos é geralmente compreendida como socialmente neutra e, por isto, de pouco interesse histórico. Porém, decisões técnicas podem ter conseqüências econômicas e sociais de longo alcance, alterando o equilíbrio de poder entre empresas ou nações competidoras e restringindo a liberdade dos usuários. Os esforços para criar padrões formais trazem as decisões técnicas dos construtores de sistemas privados para a esfera pública; deste modo, as disputas entre padrões podem trazer as suas pressuposições implícitas e os conflitos de interesse para a luz do dia. A paixão com que acionários eventualmente contestam decisões sobre padrões deve nos alertar sobre o significado mais profundo por trás das tecnicidades. (Fonte: Janet Abbate, *Inventing the Internet, MIT Press*)

PADRÕES E SERVIÇOS TÉCNICOS – A infra-estrutura da Internet

É nesta camada que a Internet toma forma. A maioria das questões envolvendo este ponto compõe o núcleo da discussão sobre a Governança da Internet, sendo geralmente catalogadas na definição "estreita" desta governança. Elas se dividem em dois grupos. O primeiro abrange as questões centrais ligadas a **padrões e serviços técnicos:** TCP/IP, DNS e servidores-raiz. A segunda cobre os **aspectos comerciais da infra-estrutura da Internet**, os quais incluem tanto o papel dos provedores de serviço de Internet (ISPs) e das operadoras de Internet banda larga como os aspectos econômicos da conectividade na Internet (preços correntes de conectividade e IXPs – Internet eXchange Points).

A ICANN é provavelmente a organização mais freqüentemente citada no contexto das discussões sobre a Governança da Internet. A razão para isto está na posição central da ICANN na gestão dos endereços numéricos da Internet (números de IP) e dos sistemas de nomes de domínios.

Visões opostas do papel da ICANN na Governança da Internet

ESTREITA – TÉCNICA	AMPLA – POLÍTICA
A ICANN é simplesmente um órgão de coordenação responsável pela administração técnica no campo dos números de IP e dos nomes de domínio. Segundo este ponto de vista, a ICANN apenas coordena, não governa, a Internet. Esta opinião é expressa por: ICANN, Internet Society, governo dos Estados Unidos, governo de outros Estados industriais.	O trabalho da ICANN envolve mais do que apenas coordenação técnica. Embora a ICANN deva preservar a administração de tarefas técnicas centrais, como a gestão de servidores-raiz e a distribuição de números de IP, as diretrizes políticas deveriam ser definidas por um órgão internacional legítimo, representativo de todos os Estados. Isto poderia dar-se tanto no seio da ONU como no de outra estrutura internacional de estabelecimento mais recente. Esta opinião é expressa por: muitos países em desenvolvimento.

PROTOCOLO DE CONTROLE DE TRANSPORTE/PROTOCOLO DE INTERNET (TCP/IP)

A SITUAÇÃO ATUAL

O principal padrão técnico a especificar como os dados são transportados pela Internet é o TCP/IP, que se baseia em três princípios: comutação por pacotes, *networking* ponta-a-ponta e robustez.

A *comutação por pacotes* é o método usado para transmitir dados pela Internet. Todos os dados enviados a partir de um computador são segmentados em pacotes que viajam pela Internet e são então remontados, ao chegarem ao computador destino.

O conceito de *networking ponta-a-ponta* põe toda a sofisticação, inteligência e inovação nos extremos de uma rede. Foi este princípio que tornou possível todas as inovações relacionadas à Internet. A rede entre as pontas finais (*endpoints*) é neutra e não impede o desenvolvimento e a criatividade nas pontas finais. Isto significa que as aplicações que circulam pela Internet podem ser desenhadas nas pontas finais da rede, sem exigência de permissão dos operadores de rede ou de qualquer outra parte.

Alcança-se a *robustez* através da dinamização do *routing*, o processo de entregar uma mensagem na rede através do caminho mais adequado. Inicialmente, a predecessora da Internet, a DARPANet, introduziu o *routing* dinâmico para desenvolver redes de defesa robustas, capazes de sobreviver a potenciais ataques nucleares. O *routing* dinâmico foi utilizado para interconectar um conjunto diverso de redes.

Para a Governança da Internet, o TCP/IP tem dois aspectos importantes: a) a introdução de novos padrões; e b) a distribuição de números de IP.

Os padrões de TCP/IP são estabelecidos pela Força-Tarefa de Engenharia da Internet (IETF). Dada a sua relevância central para a Internet, eles são cuidadosamente gerenciados pela IETF.

Números de IP são endereços numéricos que cada computador conectado à Internet precisa ter. Números de IP são exclusivos; dois computadores conectados à Internet não podem ter o mesmo número de IP. Isto faz com que os números de IP sejam recurso potencialmente escasso.

O sistema de distribuição de números de IP é organizado hierarquicamente. No topo da pirâmide está a Autoridade da Internet para Atribuição de Números (IANA – Internet Assigned Numbers Authority), uma subsidiária da ICANN que distribui blocos de IP para os Registros Regionais de Internet (RIRs).

Os RIRs vigentes são: ARIN (American Registry of Internet Numbers); APNIC (Asia Pacific Network Information Centre); LANIC (Latin American and Caribbean IP Address Regional Registry); e RIPE NCC (Réseaux IP Européens Network Coordination Centre – cobrindo a Europa e o Oriente-Médio). Um registro africano, o AFRINIC, também já está implementado.

Os RIRs distribuem números IP para um grande número de ISPs, bem como para Registros de Internet nacionais e internacionais. ISPs de menor porte, empresas e indivíduos estão situados um nível abaixo na escala.

QUESTÕES

Há números de IP suficientes?

O total corrente de números de IP em IPv4 (Protocolo Internet, versão 4) chega a 4 bilhões e pode esgotar-se com a introdução de dispositivos ativados via Internet, como telefones móveis, organizadores pessoais, consoles de jogos e aparelhos domésticos.

A preocupação de que os números de IP pudessem esgotar-se e finalmente inibir o desenvolvimento da Internet levou a comunidade técnica a empreender duas ações principais:

- A primeira foi a racionalização do uso do conjunto existente de números de IP. Isto foi alcançado através da introdução da Tradução de Endereço de Rede (NAT), capaz de conectar uma rede privada (e.g. empresa ou universidade) através de apenas um IP. Sem a NAT, cada computador dentro de uma rede privada precisaria ter o seu próprio número de IP.
- A segunda ação foi a introdução do IPv6 (uma nova versão do Protocolo Internet), que provê um total muito maior de números de IP (430.000.000.000.000.000.000).

A resposta da comunidade técnica da Internet ao problema da escassez potencial de números de IP é um exemplo de administração rápida e proativa. A abordagem "melhor prevenir do que remediar" (conhecida como "princípio de precaução" na linguagem da diplomacia ambiental) foi adotada, ainda que o prazo até os números de IPv4 se esgotarem fosse incerto.

De qualquer modo, poderia ter havido uma escassez "artificial" se os responsáveis pela atribuição de números de IP no âmbito local, como os ISPs, decidissem abusar do seu poder e condicionassem as atribuições, por exemplo, à compra de outros serviços, afetando deste modo a oferta e o preço de números de IP.

Modificações no TCP/IP e segurança na Internet

A segurança não era uma questão essencial para os desenvolvedores originais da Internet, na medida em que, na época, a Internet era formada por uma rede fechada de instituições de pesquisa. A segurança era garantida principalmente pela limitação do acesso físico às redes e aos computadores conectados. Computadores eram usados por um pequeno número de especialistas em informática. Os dados eram permutados sem nenhum tipo particular de proteção.

A expansão da Internet viu a sua base de usuários crescer muito além das expectativas da sua comunidade inicial, até cerca de um bilhão de usuários em todo o mundo. E a Internet também se tornou um importante instrumento comercial.

Tudo isto coloca a questão da segurança no alto da lista das questões da Governança da Internet. A segurança aumentou progressivamente através de várias soluções, principalmente *ad hoc*. Algumas delas, como programas *firewalls*, antivírus e de criptografia têm sido substancialmente efetivas.

Como a Internet não foi inventada tendo a segurança em vista, incorporar a noção de segurança intrínseca exigirá modificações substanciais na própria base da Internet, no TCP/IP. Um novo protocolo (o IPv6) oferece algumas melhoramentos de segurança, mas ainda está aquém de uma solução abrangente. Tais proteções exigirão modificações consideráveis no TCP/IP.

Modificações no TCP/IP o problema da limitação da Largura de Banda

Para facilitar a distribuição de conteúdos multimídia (e.g. telefonia por Internet ou vídeo sob demanda) é necessário uma Qualidade de Serviço (QoS) capaz de garantir um nível mínimo de desempenho. A QoS especifica a disponibilidade (*uptime*), largura de banda (vazão de dados), latência (atraso) e indicação de erro, o que é particularmente importante em aplicações sensíveis a atrasos, como eventos transmitidos ao vivo. Congelamento, imagens em câmara lenta ou ecos no áudio são as conseqüências de limitação na largura de banda. A introdução da QoS exigirá modificações nos protocolos de Internet, inclusive fazer concessões referentes a um dos princípios centrais da Internet, o *networking* ponta-a-ponta.

POSSÍVEIS DESENVOLVIMENTOS FUTUROS

São esperadas pressões crescentes para modificar a presente arquitetura da Internet. Algumas soluções voltadas para os problemas de segurança e de ampliação de largura de banda não poderão ser alcançadas sem modificações fundamentais no Protocolo Internet.

Outra solução emergente é a construção de várias opções de rede por cima do atual TCP/IP. É muito provável que empresas privadas continuem a desenvolver inovações, as quais haverão de contornar tanto as limitações da rede atual quanto o presente desconforto dos órgãos de normalização em relação a modificar princípios centrais da Internet, principalmente o *networking* ponta-a-ponta.

O SISTEMA DE NOMES DE DOMÍNIO (DNS)

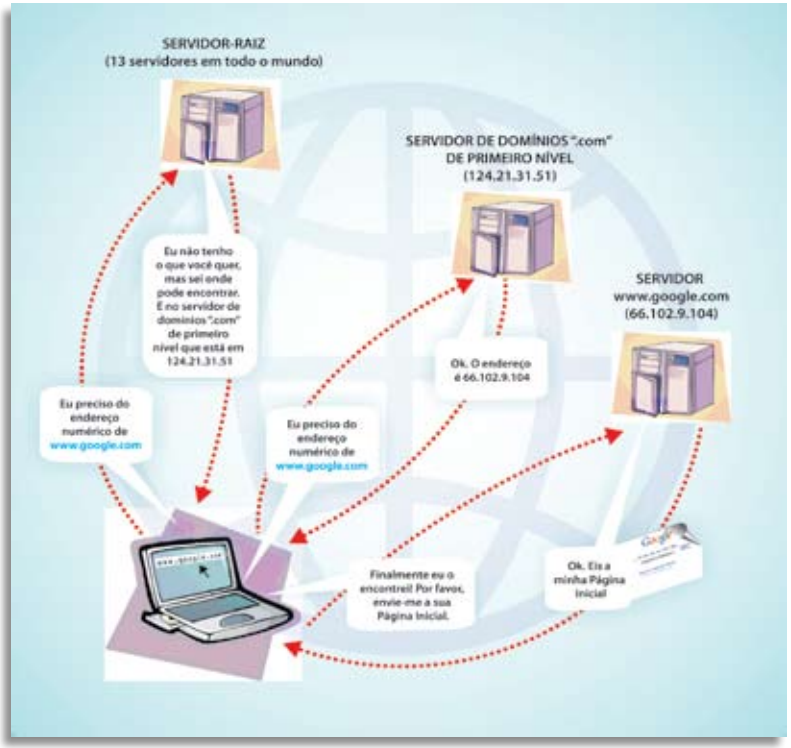
A SITUAÇÃO ATUAL

O DNS lida com endereços de Internet (como www.google.com) e o converte em números de IP. Assim, para ter acesso a um site particular, qualquer computador deve primeiro acessar um servidor de DNS. Este servidor de DNS localiza então o endereço numérico do site em questão (196.23.121.5 no caso do Google). O DNS consiste em servidores-raiz, servidores de primeiro nível e de um certo número de servidores de DNS distribuídos em todos o mundo. A gestão do DNS tem sido uma questão polêmica no debate sobre a Governança da Internet. Uma das principais controvérsias diz respeito à organização hierárquica do DNS e à autoridade final que o governo dos Estados Unidos (através do Departamento de Comércio, DoC) tem sobre ele.

O DNS envolve dois tipos diferentes de domínios de primeiro nível. Um é genérico; o outro se baseia em códigos de países. Os domínios genéricos de primeiro nível (gTLD) incluem:

- .com, .edu, .gov, .mil, e .org (em 1984);
- .net; e .int (acrescentados em 1995); e
- .biz; .info; .name; .pro; .museum; .aero; e .coop (acrescentados em 2000).

Para cada gTDL há um registrador que mantém uma lista de endereços. Por exemplo, os endereços ".com" gTDL são gerido pela VeriSign. A função de "vendedor" é desempenhada por agentes de registro chamados de *Registrars*. A ICANN faz a coordenação geral do Sistema de Nomes de Domínio concluindo acordos e credenciando registradores e *Registrars*. Ela também define o valor de atacado pelo qual o registrador "aluga" nomes de domínio aos agentes de registro, e estabelece certas condições para os serviços oferecidos pelo registrador e pelos agentes de registro. Quer dizer, a ICANN atua como reguladora econômica e legal no negócio dos nomes de domínio para gTLDs.



Uma parte importante da gestão de domínios diz respeito à proteção das marcas registradas e à resolução de disputas. O registro de nomes de domínio é baseado no princípio "Primeiro a chegar, primeiro a ser servido" [*First Come, First Served* – FCFS], em que qualquer um pode registrar qualquer nome, o domínio será concedido ao primeiro requerente que satisfizer as exigências.

Contudo, o valor potencial de nomes de domínio desencadeou um fenômeno conhecido como *cybersquatting*, a prática de registrar nomes de domínios que pudessem ser vendidos depois. A impossibilidade de haver dois domínios com o mesmo nome levou a um debate sobre registro de direitos. O problema era particularmente relevante para nomes de domínio que usassem nomes de marcas famosas (e.g. Microsoft, Nike, Toyota, Rolex, etc.).

A reforma da gestão do DNS, com a adoção da Diretriz Uniforme para a Resolução de Disputas de Nomes s de Domínio (UDRP), introduziu mecanismos que reduziram significativamente o *cybersquatting*. A UDRP só está disponível para domínios .com; .net; e .org, e não cobre domínios de país. A jurisdição de UDRP é automaticamente reconhecida quando um indivíduo, companhia ou organização assina um acordo de registro de nome de domínio. A UDRP oferece algumas vantagens aos demandantes de nomes já registrados, geralmente proprietários de marcas tradicionais, como a resolução rápida de conflitos através de arbitragem e a implementação simples das decisões através de mudanças diretas no DNS (evitando processos que podem se arrastar na justiça).

Outro elemento importante no exame da organização corrente da governança do DNS é a gestão dos domínios de primeiro nível com código de país (ccTDLs). Hoje, os códigos de país são geridos por uma variedade de instituições que foram credenciadas nos primeiros dias da Internet, época em que alguns governos sequer se interessavam por isto. Figuram entre essas organizações: instituições acadêmicas, associações técnicas, ONGs e até indivíduos privados. Em muitos casos, a responsabilidade pela gestão de códigos de país foi atribuída com base no princípio *Primeiro a chegar, primeiro a ser servido* (FCFS).

QUESTÕES

A criação de um novo Domínio Genérico de Nomes

Em meados dos anos 1990, um dos fundadores da Internet, Jon Postel, tentou sem sucesso acrescentar um certo número de novos domínios à lista básica existente (.com; .edu;. .org; e .int). A principal oposição que sofreu teve origem no setor empresarial, cuja preocupação era de que aumentar o número de domínios complicaria a proteção das suas marcas registradas. A abordagem restritiva prevaleceu, e somente uma pequena quantidade de novos domínios foi introduzida pela ICANN no ano 2000 (.biz; info; .name; .pro; .museum; .aero; e .coop).

Outro problema associado com a questão de novos domínios envolve a vinculação de nomes de domínios a conteúdos. Por exemplo, o congresso estadunidense aprovou uma lei introduzindo o domínio "kids.us", reservado a conteúdos favoráveis à infância. A principal dificuldade gerada por esta proposta diz respeito à definição de que conteúdos infantis seriam ou não "favoráveis". Problemas relativos a controle de conteúdos poderiam daí decorrer. Até aqui, o domínio "kids" tem sido usado apenas como parte do domínio de país dos Estados Unidos.

A gestão de Domínios de País

A gestão de domínios de país de primeiro nível envolve três questões importantes. A primeira diz respeito à decisão, amiúde politicamente controversa, de *que códigos de país devem ser registrados* quando lidamos com países e entidades cujo *status* internacional é indefinido ou contestado (e.g. países recentemente independentes, movimentos de resistência, etc.). Jon Postel defendeu a alocação de nomes de domínio segundo os padrões da Organização Internacional de Normalização (ISO), que é uma fonte comum de abreviações de duas letras para países e outras entidades. A abordagem de Postel mostrou-se bem-sucedida e continua a ser praticada, apesar do fato de a lista da ISO identificar "diferentes áreas econômicas" em vez de nações soberanas.

A segunda questão diz respeito a *quem deve gerir os códigos de país*. Muitos países têm tentado obter o controle dos seus domínios de país, que são considerados como recurso nacional. Por exemplo, a África do Sul usou o seu direito de soberania como argumento para recuperar o seu domínio de país. Uma lei recentemente promulgada especifica que o uso do domínio de país fora dos parâmetros especificados pelo governo sul-africano será considerado crime. O modelo brasileiro de gestão de domínio de país é comumente citado como um exemplo bem-sucedido de uma abordagem multipartite ou multi-acionária. O órgão nacional encarregado dos domínios brasileiros está aberto a todos os atores-chave, incluindo agências governamentais, o setor empresarial e a sociedade civil. A transferência da gestão do domínio de país no Camboja de não governamental para governamental é freqüentemente citada como exemplo de transição malsucedida. A intervenção do governo diminuiu a qualidade dos serviços e produziu aumento de preços, o que tornou o registro de domínios cambojanos muito mais difícil.

Em alguns casos, domínios de país foram usados de maneira indevida para registrar domínios genéricos de primeiro nível, conforme discriminado na tabela abaixo:

CÓDIGO DE PAÍS	PAÍS	ÁREA DE DOMÍNIO
tv	Tuvalu	Estações de TV
mu	Maurício	Música
md	Moldova	Medicina e saúde
fm	Federação da Micronésia	Rádio
tm	Turcomenistão	Marcas Registradas

A maioria dos países acima mencionados tem tentado recuperar o controle dos seus domínios de país. Maurício, por exemplo, iniciou uma intensa campanha de *lobby* diplomático nesta direção.

A terceira questão relaciona-se à *relutância de muitos operadores de domínio em passar a fazer parte do sistema da ICAAN*. Até agora a ICANN não conseguiu reunir todos os operadores de domínio sob o seu guarda-chuva. Alguns operadores de domínio de país começaram a criar as suas próprias organizações regionais, como a CENTR (Conselho de Registros Nacionais Europeus de Primeiro Nível).

O problema das línguas: Nomes de domínio multilíngüe

Um dos principais limites para o desenvolvimento futuro da Internet é a ausência de funções miltilíngües para operar a infra-estrutura da Internet. Os nomes de domínio são registrados e utilizados em inglês. Mesmo caracteres não ASCII em francês ou alemão não podem ser usados em endereços de Internet (e.g. café transforma-se em cafe). A situação complica-se ainda mais com escritas não latinas, como o japonês, o árabe ou o chinês.

Entre as várias soluções para a questão dos nomes de domínio multilíngües, as mais relevantes são os sistemas Nome de Domínio Internacionalizado (IDNS) e Endereço de Internet em Língua Nativa (NLIA). O IDN, uma solução técnica proposta pela IETF, está se tornando a solução dominante. O IDN traduz nomes nativos para nomes de domínio em inglês na máquina do cliente e envia nomes de domínio em inglês para resolução no DNS. Outro obstáculo para o uso mais amplo do IDN é a integração técnica interna dos principais navegadores da Internet, como o Internet Explorer, que apenas após a sua versão 7.0 passou a resolver domínios IDNS.

Além das dificuldades técnicas, o desafio seguinte, e talvez mais complexo, será o desenvolvimento de diretrizes e de procedimentos administrativos. Há uma pressão crescente para que o IDN seja gerido por países ou grupos de países falantes de uma mesma língua. Por exemplo, o governo chinês indicou em várias ocasiões que o IDN em chinês deveria ser gerido pela China. Conseguir introduzir uma política de IDN será um dos principiais desafios da ICANN, e também um teste para a dimensão inclusiva da sua abordagem internacional.

SERVIDORES-RAIZ

Situados no topo da estrutura hierárquica do sistema de nomes de domínio, os servidores-raiz chamam muito a atenção. São parte integrante da maioria dos debates políticos e acadêmicos sobre as questões da Governança da Internet.

A SITUAÇÃO ATUAL

A função e a robustez do DNS podem ser ilustradas com uma análise da preocupação de que a Internet entraria em colapso se os servidores-raiz viessem, por algum motivo, a ser desativados. Primeiramente, há 13 servidores-raiz distribuídos em todos o mundo (10 nos Estados Unidos e 3 em outros lugares; dos 10 que se encontram nos Estados Unidos, vários são operados por agências do governo estadunidense). Se um desses servidores parar de funcionar, os 12 remanescentes continuariam a funcionar. Mesmo que os 13 servidores-raiz deixassem de funcionar simultaneamente, a resolução dos nomes de domínio (principal função dos servidores-raiz) continuaria em outros servidores de domínio, distribuídos hierarquicamente por toda a Internet.

Por essa razão, milhares de servidores de nomes de domínio contêm cópias do arquivo raiz da zona, e colapsos imediatos catastróficos da Internet não podem ocorrer. Levaria algum tempo antes que quaisquer conseqüências funcionais pudessem ser notadas, período durante o qual seria possível reativar os servidores originais ou criar novos.

Além disso, o sistema de servidores-raiz é consideravelmente fortalecido pelo esquema *Anycast*, que duplica servidores-raiz através de mais de 80 localidades em todo o mundo. Isso propicia muitas vantagens, inclusive o incremento da robustez do sistema DNS e a resolução mais rápida de endereços de Internet (com o esquema Anycast, o servidores de determinação estão mais próximos dos usuários finais).

Os 13 servidores-raiz são geridos por uma diversidade de organizações: instituições acadêmicas/públicas (seis servidores); companhias comerciais (quatro servidores); e instituições governamentais (três servidores).

As instituições que administram servidores-raiz recebem um arquivo da zona raiz proposta pela IANA (ICANN) e aprovada pelo governo dos Estados Unidos (Departamento de Comércio, DoC). Uma vez o conteúdo aprovado pelo DoC, ele é inserido no servidor-raiz mestre operado pela VeriSign, sob contrato com o DoC. O arquivo no servidor-raiz mestre é então automaticamente duplicado em todos os outros servidores-raiz. Assim, é possível o governo estadunidense introduzir modificações unilaterais no DNS. Isto constitui uma preocupação importante para muitos governos.

QUESTÕES

A supervisão das políticas dos servidores-raiz deve ser internacionalizada?

Muitos países expressaram as suas preocupações sobre o arranjo vigente, em cujos termos a decisão última sobre os conteúdos dos servidores-raiz resta responsabilidade do Departamento de Comércio dos Estados Unidos, e sugeriram a adoção de uma "Convenção-Raiz", que encarregaria a comunidade internacional da supervisão das diretrizes e políticas dos servidores-raiz ou, pelo menos, garantiria às nações-Estado direitos sobre os seus próprios nomes de domínio nacionais. Não é muito provável que as instituições estadunidenses (especialmente o Congresso) aceitem tais propostas. Um compromisso potencial entre as partes poderia basear-se em dois elementos:

- transferência do controle dos servidores-raiz do Departamento de Comércio para a ICANN, tal como inicialmente imaginado;
- reforma substantiva da ICANN, levando à criação de uma organização internacional *sui generis*, que constituísse um quadro institucional aceitável para todos os países.

Qual é a possibilidade de se criar um servidor-raiz alternativo (por exemplo uma Internet B)?

Como discutimos anteriormente, criar um servidor-raiz alternativo é tecnicamente simples. A questão essencial é quantos "seguidores" terá um servidor alternativo ou, mais precisamente, quantos computadores na Internet apontarão para eles depois que eles se tornarem nomes de domínios resolvedores? Sem usuários, qualquer DNS alternativo torna-se inútil. Foram feitas algumas tentativas de criar DNSs alternativos: Open NIC; New.net e Name.space, por exemplo. A maioria fracassou, por causa da pequena porcentagem de usuários da Internet.

PROVEDORES DE SERVIÇO DE INTERNET (ISPs)

Os ISPs fazem a conexão dos usuários finais com a Internet e hospedam sites. É por isto que os ISPs são, para muitos governos, a opção mais simples e direta para a impor a observância do controle governamental e de regras legais sobre a Internet. No presente texto, quando mencionamos ISPs queremos dizer tanto as empresas que provêm acesso a usuários individuais quanto Provedores de Serviço de Internet institucionais, como universidades, departamentos governamentais, etc.

Durante o boom da Internet na década de 1990, os ISPs eram isentos de responsabilidades em relação a conteúdos ou eventuais violações de direitos autorais. Pensava-se que pressões adicionais sobre os ISPs pudessem obstruir o desenvolvimento futuro da Internet. Com a relevância comercial crescente da Internet e o aumento das preocupações de segurança, muitos Estados começaram a concentrar seus esforços de impor a execução legal aos ISPs.

QUESTÕES

Mercado de ISPs e monopólio das telecomunicações

Nos países em que há monopolização na área das telecomunicações, os monopólios presentes também forneçam o acesso à Internet. Eles impedem a entrada de outros ISPs e inibem a competição. Isto resulta em preços mais elevados, freqüentemente em qualidade inferior dos serviços, e leva a fracassos quanto ao imperativo de reduzir a cisão digital. Em alguns casos, os monopólios das telecomunicações toleram a existência de outros ISPs, mas interferem no âmbito operacional (e.g. fornecendo larguras de banda inferiores ou provocando interrupções nos serviços).

A responsabilidade dos ISPs sobre direitos autorais

O princípio de que um prestador de serviços de Internet não pode ser responsabilizado por hospedar materiais que violem direitos autorais se disto não tiver consciência é comum à maioria dos sistemas legais. A principal diferença está nas ações legais empreendidas depois que o ISP foi informado de que o material eventualmente hospedado viola a lei dos direitos autorais.

As leis dos Estados Unidos e da União Européia prevêem um procedimento chamado "*notice-take down*", que exige que o ISP retire o material infrator da rede para evitar ser processado. As legislações estadunidense e união-européia dão uma proteção mais vigorosa ao detentor do direito autoral, sem oferecer nenhuma oportunidade ao usuário do material de defender-se. A lei japonesa adota uma abordagem mais equilibrada, através do procedimento chamado "*notice-notice-take down*", que dá ao usuário do material o direito de queixar-se sobre a exigência de retirada.

O papel dos ISPs na política de conteúdos

"Não mate o mensageiro", eis a resposta dos ISPs à crescente pressão oficial exercida sobre eles para que cumpram as diretrizes de conteúdo. Com alguma relutância, os provedores de serviço de Internet estão se envolvendo gradualmente com a questão. Dois caminhos apresentam-se a eles. No primeiro, eles executam as leis do governo. No segundo, baseado na noção de auto-regulamentação, cabe ao próprio ISP decidir que conteúdos são ou não apropriados. Esta opção, por sua vez, coloca um risco de privatização da política de conteúdos.

Em muitos países, foram adotadas legislações nas quais os ISPs são sobrecarregados com responsabilidades adicionais relativas às políticas de conteúdo: tanto pelo que está disponível nos sites por eles hospedados como pelo que é acessado pelos clientes por eles servidos. Esta abordagem pode criar despesas adicionais para os ISPs e, em última análise, produzir aumento de custos de acesso para os usuários.

PROVEDORES DE BANDA PASSANTE (IBPs)

A arquitetura do acesso à Internet consiste em três níveis ou camadas. Os ISPs que conectam usuários finais constituem a Camada 3. As Camadas 1 e 2 consistem nos fornecedores de banda passante. A Camada 1 (espinhas dorsais de Internet) geralmente é administrada por grandes companhias, como MCI, AT&T, Cable Wireless e France Telecom. No campo das operadoras de espinhas dorsais, as companhias de telecomunicações tradicionais ampliaram a sua presença no mercado internacional de Internet. Os provedores da Camada 2 geralmente operam nos níveis nacional ou regional.

QUESTÕES

A infra-estrutura da Internet deve ser considerada serviço público?

Dados de Internet podem passar por quaisquer meios de telecomunicação. Na prática, porém, instalações como as das espinhas dorsais de Camada 1 tornaram-se críticas para a operação da Internet. A sua situação central dentro da rede da Internet garante aos seus proprietários poder de mercado suficiente para impor preços e condições no fornecimento dos seus serviços. Dois casos correlatos foram mencionados num relato recente da OSCE (Organização para a Segurança e Organização na Europa).

No primeiro caso, um processo foi aberto contra uma página de Internet com questionável conteúdo nazista, hospedada pela Flashback, na Suécia. Os tribunais decidiram que a página não violava as leis antinazistas suecas. Não obstante, um ativo militante antinazista articulou uma importante campanha pública contra a Flashback, por meio disto colocando pressão no ISP da Flashback, o Air2Net, e sobre a principal operadora de espinha dorsal, a MCI/WorldCom. Sob a pressão da campanha, a MCI/WorldCom decidiu desconectar a Flashback, apesar da inexistência de qualquer base legal para fazê-lo. As tentativas da Flashback de encontrar um servidor alternativo fracassaram, pois a maioria deles também se conectava à rede através da espinha dorsal operada pela MCI/WorldCom.

O segundo caso ocorreu na Holanda, onde um pequeno ISP holandês, Xtended Internet, foi desconectado por seu provedor *upstream* baseado nos Estados Unidos por pressão do *lobby* da Cientologia.

Em última análise, o funcionamento da Internet pode depender de decisões tomadas pelos proprietários das espinhas dorsais centrais. Tem a comunidade global da Internet o direito de exigir das principais operadoras de telecomunicações garantias de funcionamento confiável da infra-estrutura crítica da Internet? Operam essas empresas uma instalação pública ou de serventia pública?

A liberalização das telecomunicações e o papel dos ISPs

Existem opiniões opostas sobre até que ponto os provedores de serviço de Internet (ISPs) devem sujeitar-se aos regulamentos existentes da OMC. Os países desenvolvidos argumentam que as regras liberalizadas garantidas pela OMC às operadoras de telecomunicações também podem ser estendidas aos ISPs. A interpretação restritiva salienta o fato de que o regime de telecomunicações da OMC só se aplica ao mercado de telecomunicações, e que, portanto, a regulamentação dos ISPs postula a necessidade de a OMC formular novas regras.

MODELO ECONÔMICO PARA A CONECTIVIDADE NA INTERNET

A SITUAÇÃO ATUAL

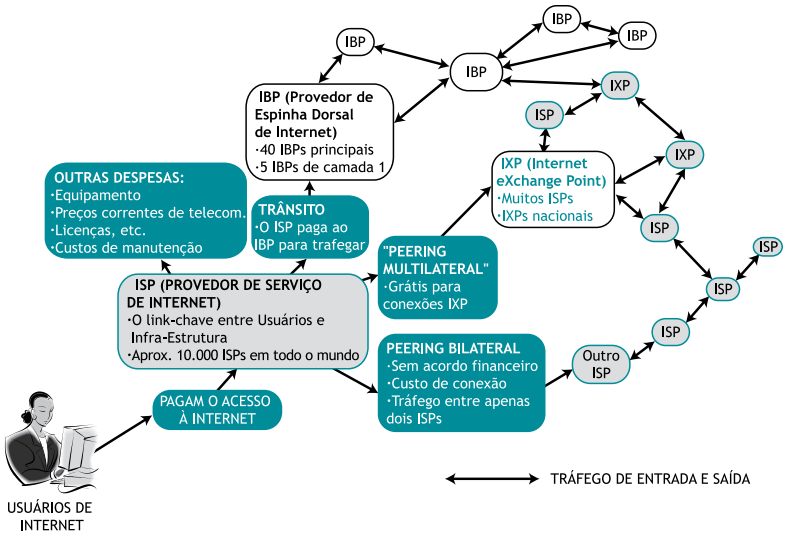
Muito freqüentemente, qualquer discussão sobre questões de governança acaba numa análise da distribuição do dinheiro e das fontes de renda. Qual é o fluxo de recursos na Internet? Quem paga a Internet?

Há muitas transações financeiras entre as diversas partes envolvidas com a Internet.

- Assinantes individuais e companhias pagam aos Provedores de Serviço de Internet (ISPs).
- Os ISPs pagam o serviço das operadoras de telecomunicações e pela banda passante da Internet.
- Os ISPs pagam aos fornecedores de equipamentos, programas e manutenção (inclusive ferramentas de diagnóstico, apoio aos membros da equipe para operação de instalações, suporte e apoio técnico [*help desk*] e serviços administrativos).

- Os interessados que registram nomes de domínio junto a agentes de registro não pagam apenas os serviços do agente, mas também aqueles da IANA.
- ISPs pagam os Registros Regionais de Internet (RIRs) por endereços IP.
- RIRs pagam à ICANN.
- As operadoras de telecomunicações pagam a fabricantes de cabos e satélites e aos prestadores de serviços de telecomunicação para prover os *links* necessários. Como freqüentemente estão em débito, elas também pagam juros a vários bancos e consórcios.

Mas a lista não acaba aí, e a verdade é: "Essa história de almoçar de graça não existe." Em última análise, os custos da cadeia são cobertos pelos usuários finais da Internet, sejam eles indivíduos ou instituições.



QUESTÕES

Quem deve arcar com os custos dos links entre países em desenvolvimento e países desenvolvidos?

Hoje em dia, esses custos são cobertos pelos países em desenvolvimento. Comparado com o sistema tradicional de telefonia, em que o preço de cada chamada internacional é dividido entre dois países, o modelo da Internet põe todo o encargo de um lado só, os países em desenvolvimento, que precisam conectar as espinhas dorsais, principalmente situadas

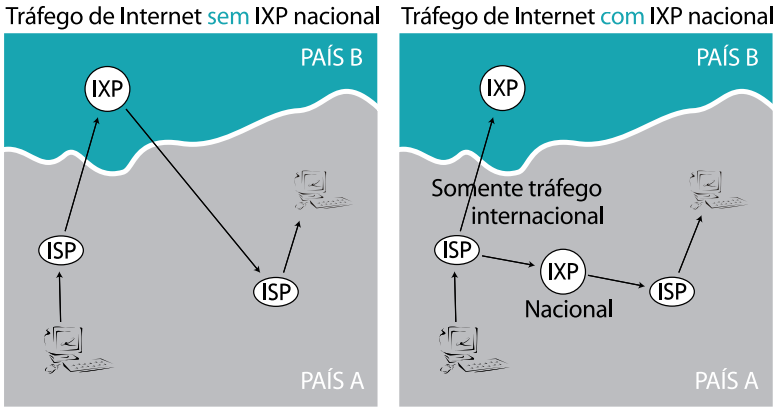
nos países desenvolvidos. Paradoxalmente, pode-se argumentar que, ao fazê-lo, os países pobres estariam subsidiando o sistema da Internet nos países desenvolvidos.

O problema dos acordos financeiros é particularmente relevante para os países mais pobres, que contam com a renda das telecomunicações internacionais como importante fonte de arrecadação. A situação complicou-se ainda mais com a introdução do protocolo de voz sobre IP (VoIP), que desloca o tráfego telefônico das telecomunicações nacionais para os operadores de Internet.

A União Internacional de Telecomunicações (UIT) iniciou discussões sobre possíveis melhorias no sistema de acordos sobre despesas de Internet com o objetivo principal de distribuir de maneira mais equilibrada os custos de acesso à Internet. Devido à oposição dos países desenvolvidos, a resolução UIT adotada, a D.50, é praticamente sem efeito.

A redução dos custos de acesso através do uso de Internet eXchange Points (IXPs)

Os IXPs (também chamados de PPT, Ponto de Troca de Tráfego) são instalações técnicas através das quais diferentes ISPs permutam tráfego de Internet. Os IXPs são em geral instalados a fim de manter o tráfego de Internet no interior dos limites de comunidades menores (e.g. cidades, região, país), evitando o roteamento (ou encaminhamento) por locais geograficamente mais remotos.



Os IXPs também podem desempenhar um papel importante na redução da cisão digital. Por exemplo, no caso de um país sem IXPs nacionais, uma

parte considerável do tráfego entre clientes no interior das fronteiras do país tem de ser roteada ou encaminhada através de um outro país. Isto aumenta o volume de tráfego internacional de dados a longa distância e os custos de fornecimento do serviço de Internet.

PADRÕES DA REDE MUNDIAL

No final dos anos 1980, a batalha sobre a padronização/normalização da rede já estava acabada. O TCP/IP tornara-se gradualmente o principal protocolo da Internet, marginalizando todos os demais padrões, como o X-25 (parte da arquitetura do Open Systems Interconnection), apoiado pela UIT, e muitos outros padrões proprietários, como o SNA da IBM. Ao mesmo tempo em que a Internet facilitou a comunicação normal entre uma variedade de redes via TCP/IP, o sistema ainda carecia de padrões comuns de aplicação.

A solução foi desenvolvida por Tim Berners-Lee e seus colegas do Centro Europeu de Pesquisa Nucleares, o CERN, em Genebra, e consistia num novo padrão para compartilhar informações na Internet, chamado HTML (HyperText Mark-up Language, na verdade apenas uma simplificação do padrão ISO existente, chamado SGML). O conteúdo exibido na Internet tinha primeiro de ser organizado segundo os padrões HTML. Como base para a Rede Internacional de Computadores (www), o HTML pavimentou o caminho para o crescimento exponencial da Internet.

Desde a sua primeira versão, o HTML tem sido constantemente atualizado (*upgraded*) com novas características. A relevância crescente da Internet colocou em foco o problema da padronização do HTML. Isto foi particularmente relevante durante a "Guerra dos Navegadores" entre a Netscape e a Microsoft, oportunidade em que cada companhia buscou fortalecer a sua posição no mercado influenciando os padrões HTML. Enquanto o HTML básico só tratava de textos e fotos, as novas aplicações da Internet exigiam tecnologias mais sofisticadas para gerir bancos de dados, vídeo e animação. Uma tal variedade de aplicações exigia consideráveis esforços de padronização, a fim de garantir que os conteúdos da Internet pudessem ser vistos adequadamente pela maioria dos navegadores de Internet.

A padronização de aplicações entrou numa nova fase com o surgimento do XML (eXtended Mark-up Language), que permite uma maior flexibilidade no estabelecimento de padrões para os conteúdos de Internet. Novos conjuntos de padrões XML também foram introduzidos. Por exemplo, o padrão para a distribuição de conteúdo sem fio é chamado Wireless Mark-up Language (WML).

A padronização de aplicações é levada a efeito principalmente no quadro do Consórcio da Rede Mundial (W3C), dirigido por Tim Berners-Lee. É interessante observar que, apesar da sua grande relevância para a Internet, até aqui o W3C não chamou muito a atenção no debate sobre a Governança da Internet.

CÓDIGO ABERTO

Programas de código aberto são oferecidos gratuitamente e podem ser modificados por seus usuários. Aplicações de código aberto são desenvolvidas por programadores em todo o mundo, trabalhando num mesmo código.

Ao ser introduzido, o código aberto prometia ser uma alternativa eficiente ao caros programas proprietários. A iniciativa mais conhecida de código aberto é o Linux. Contudo, a proliferação de programas de código aberto foi mais lenta do que esperava-se, principalmente por causa da falta de suporte técnico adequado. A recente decisão de alguns atores-chave, como a IBM e a Intel, de usarem o Linux, a principal plataforma de código aberto existente, pode levar a um desenvolvimento bem-sucedido dessa abordagem.

Além disso, há um interesse renovado por códigos abertos sob um novo nome e um conceito ligeiramente modificado, intitulado Free/Libre Open Source Software (FLOSS). A principal diferença entre código aberto e FLOSS é que o FLOSS dá acesso livre ao código sem qualquer necessidade de registro.

A proposta de código aberto é freqüentemente apresentada como solução para o desenvolvimento de capacidades em tecnologia da informação e comunicações (TICs). Na CMSI, o esforço da sociedade civil e de alguns países em desenvolvimento para mencionar, no documento final, o código

aberto e o FLOSS como solução para superar a cisão digital, acabou diluído numa referência geral a "diferentes modelos de programa, inclusive proprietário, código aberto e software livre."

CONVERGÊNCIA: INTERNET-TELECOMUNICAÇÃO-MULTIMÍDIA

O uso amplo e preponderante de Protocolos de Internet desencadeou um processo de convergência das telecomunicações, da multimídia e dos sistemas de entretenimento. Hoje, é possível fazer chamadas telefônicas, ouvir o rádio, assistir televisão e compartilhar músicas pela Internet. No campo das telecomunicações tradicionais, o principal ponto de convergência é o Voz sobre Protocolo de Internet (VoIP). A popularidade crescente do VoIP é função do seu preço inferior, da possibilidade de integrar linhas de comunicação de dados e de voz, bem como de usar ferramentas avançadas baseadas em PC. O TCP/IP também está se tornando dominante no campo da multimídia e do entretenimento. Ao passo que a convergência técnica progride em ritmo veloz, as decorrências econômicas e legais desse avanço vão precisar de tempo para amadurecer.

QUESTÕES

As implicações econômicas da convergência

No plano econômico, a convergência deu inicio a uma reformulação dos mercados tradicionais, colocando companhias que antes operavam em domínios separados em competição direta. Resta a saber quem vai assumir a liderança neste mercado crescentemente convergente, se companhias de telecomunicações, como a MCI, por exemplo, ou companhias de TIC, como a IBM.

O mesmo se aplica ao mercado de multimídia, embora neste campo poucas companhias tenham reagido ao desafio proposto pela convergência desenvolvendo tecnologias de Internet e de mídia/entretenimento ou formando parcerias. A Sony é uma companhia que desenvolveu capacidades tanto de TIC como de mídia/entretenimento. A fusão da American Online e a Time Warner tinha por objetivo esta combinação de telecomunicações com mídia/entretenimento. Hoje, a AOL/Time Warner reúne provedores

de serviço de Internet, televisão, música e desenvolvimento de programas sob o mesmo guarda-chuva corporativo.

A necessidade de um quadro jurídico

O sistema legal foi o mais lento a ajustar-se às mudanças causadas pelas convergências tecnológica e econômica. Cada um desses segmentos, telecomunicações, mídia/entretenimento e TIC, tem o seu próprio quadro regulador especial.

Esta convergência abre diversas questões sobre governança e regulamentação: O que vai acontecer com os regimes nacionais e internacionais existentes em campos como a telefonia e a radiodifusão de sons e imagens? Serão desenvolvidos novos regimes centrados principalmente na Internet? Deve a regulamentação desta convergência ser efetuada por autoridades públicas (Estados e organizações internacionais) ou através de auto-regulamentação?

Alguns países, como a Malásia e a Suíça, bem como a União Européia, começaram a responder essas questões. A Malásia adotou a Lei das Telecomunicações e da Multimídia em 1998, estabelecendo uma perspectiva geral para a regulamentação da convergência. As novas diretrizes da União Européia, que agora estão sendo transpostas em leis nacionais, também avançam nesta direção, assim como as leis e regulamentações suíças de telecomunicações.

O risco de convergência entre operadores de cabo e ISPs

Em muitos países, a Internet banda larga foi introduzida via redes de cabos. Este é especialmente o caso dos Estados Unidos, onde a Internet via cabo é muito mais disseminada do que a linha ADSL, a outra opção principal de Internet banda larga. Que riscos associam-se a esta convergência?

Há grupos que argumentam que a intermediação de operadoras de cabo entre os usuários e a Internet poria em questão o princípio do *networking* ponta-a-ponta.

A principal diferença entre o acesso discado tradicional e o cabo é que o cabo não é regulamentado pelas regras do assim chamado "suporte comum". Essas regras, aplicáveis ao sistema de telefonia, especificam que o acesso deve ser não discriminatório. As operadoras de cabo não estão sujeitas a tais regras, o que lhes dá controle total sobre o acesso dos seus assinantes à Internet. Elas podem bloquear o uso de certas aplicações e controlar o acesso a certos materiais. A possibilidade de vigilância e,

conseqüentemente, a capacidade de violar a privacidade são muito maiores na Internet via cabo, já que o acesso é controlado através de um sistema semelhante ao das redes locais, que possibilita um alto nível de controle direto dos usuários.

Num ensaio sobre esta questão, a União pelas Liberdades Civis Americanas dá o seguinte exemplo sobre o risco dos monopólios da Internet via cabo: "É como se uma companhia telefônica fosse autorizada a ter restaurantes e então prestasse serviços de boa qualidade e desse sempre sinal aos clientes que ligassem para a Domino's, e sinais freqüentemente ocupados, quedas de linha e ruídos para os que ligassem para a Pizza Hut."

Este problema de convergência será resolvido quando uma decisão for tomada sobre o *status* da Internet via cabo, se é um "serviço informático" ou um "serviço de telecomunicação". Se for um serviço de telecomunicações, ela deverá ser regulamentada pelas regras que se aplicam aos suportes comuns, as companhias de telecomunicações.

SEGURANÇA NA INTERNET

A SITUAÇÃO ATUAL

A questão da segurança passou a ser encarada com mais rigor devido à rápida expansão da base de usuários da Internet. A Internet demonstrou o que há muito tempo muitos suspeitavam: a tecnologia pode ser tão promissora quanto ameaçadora. O que pode ser usado em vantagem da sociedade, também o pode para seu prejuízo.

O efeito colateral da rápida integração da Internet em quase todos os aspectos das atividades humanas aumenta a vulnerabilidade da sociedade moderna. Infra-estruturas críticas, inclusive redes elétricas, sistemas de transporte e serviços de saúde são parte de uma rede global potencialmente exposta a ciberataques. Como é sabido que ataques contra estes sistemas causam falhas graves e têm um impacto financeiro potencialmente alto, as infra-estruturas críticas tornaram-se alvos freqüentes.

As questões de segurança na Internet podem ser classificadas segundo três critérios: tipo de ação; tipo de perpetrador; e tipo de alvo.

A classificação segundo o tipo de ação incluiria: interceptação de dados, interferência nos dados, acesso ilegal, *spywares* e roubo de identidade. Os possíveis perpetradores seriam *hackers*, cibercriminosos ou ciberterroristas.

Os alvos potenciais são inúmeros, desde indivíduos, companhias privadas e instituições públicas até infra-estruturas essenciais, governos e instalações militares.

A segurança da informação é discutida em mais detalhe em outras brochuras desta série:

- *Good Hygiene for Data and Personal Computers* [A higiene dos dados e computadores pessoais]
- *Information Security and Organizations* [Segurança da informação e organizações]
- *Hacktivism, Cyber-terrorism and Cyberwar* [Hackerismo, ciberterrotismo e ciberguerra]

INICIATIVAS NO CAMPO DA SEGURANÇA NA INTERNET

São muitas as iniciativas regionais, nacionais e globais cujo foco é a segurança na Internet.

É crescente o volume de legislações e de jurisprudências lidando com segurança na Internet no âmbito nacional. As iniciativas mais destacadas são dos Estados Unidos, ligadas à autoridade mais ampla do Estado em sua luta contra o terrorismo. O Departamento de Segurança Interna, equivalente ao nosso Ministério do Interior, é a principal instituição a lidar com questões de segurança na Internet. É difícil encontrar um país, principalmente entre os desenvolvidos, que não desenvolva iniciativas relativas à segurança na Internet.

No âmbito internacional, as organizações mais ativas têm sido a OCDE, que produziu as Diretrizes de Segurança da Informação, e a UIT, que produziu um grande número de estruturas, arquiteturas e padrões de segurança, inclusive o X.509, que provê a base da Infra-Estrutura de Chaves Públicas (PKI), usada, por exemplo, na versão segura do HTTP (HTTPS).

O G8 também propôs algumas iniciativas no campo da segurança na Internet, como incrementar a cooperação entre agências encarregadas de impor a execução da lei. Ele formou um Subgrupo de Combate a Crimes de Alta Tecnologia, para estabelecer um serviço de comunicação permanente, vinte e quatro horas por dia, sete dias por semana, entre os centros de cibersegurança e os Estados membros, e para assessorar o treinamento de equipes e o desenvolvimento de sistemas legais das nações-Estado em vista de combater o cibercrime e promover a cooperação entre a indústria TIC e as agências encarregadas da execução da lei.

A Assembléia Geral das Nações Unidas aprovou várias resoluções anuais sobre "desenvolvimentos no campo da informação e das telecomunicações no contexto da segurança internacional", especificamente as resoluções 53/70 em 1998; 54/49 em 1999; 55/20 em 2000; 56/19 em 2001; 57/239 em 2002 e 58/199 em 2003. Desde 1998, todas as resoluções subseqüentes tiveram conteúdo semelhante, sem qualquer aperfeiçoamento significativo. Elas não refletem as mudanças consideráveis que ocorreram no campo da segurança na Internet desde 1998.

Um importante instrumento legal internacional para a segurança na Internet é a Convenção do Conselho da Europa sobre o Cibercrime, que entrou em vigor em 1º de julho de 2004.

Alguns países concluíram arranjos bilaterais. Os Estados Unidos têm acordos bilaterais de cooperação legal em matéria criminal com mais de vinte países. Esses acordos também são usados em casos de cibercrimes.

A Minuta de Convenção de Stanford sobre a Proteção contra o Cibercrime e o ciberterrorismo representa uma tentativa do mundo acadêmico e de atores não estatais de esboçar um acordo internacional sobre a matéria. Ela recomenda o estabelecimento de um órgão internacional, a Agência para a Proteção da Infra-Estrutura de Informação (AIIP).

QUESTÕES

Arquitetura da Internet e segurança

A própria natureza da organização da Internet, a maneira como ela se organiza, afeta a sua segurança. Devemos nós persistir na abordagem atual de construir a segurança a partir de uma base pré-existente não segura, ou mudar alguma coisa na base da infra-estrutura da Internet? Como uma mudança de tal natureza afetaria outras características da Internet, especialmente a sua abertura e a sua transparência? Até aqui, a maioria dos desenvolvimentos de padrões de Internet objetivou incrementar desempenhos ou introduzir novas aplicações. A segurança não tem sido uma prioridade.

Não está claro se a IETF será capaz de mudar os padrões de e-mail em vista de assegurar autenticação e, em última análise, reduzir os abusos e maus usos da Internet (e.g. spam, cibercrimes). Considerando as controvérsias em torno de quaisquer modificações nos padrões básicos da Internet, é provável que os aperfeiçoamentos relacionados à segurança do Protocolo de Internet básico seja lenta e gradual. O setor empresarial e outras partes interessadas em soluções mais rápidas podem começar a desenvolver novas

camadas, a "Internet inteligente", o que facilitaria, entre outras coisas, uma comunicação mais segura na Internet.

Comércio eletrônico e segurança na Internet

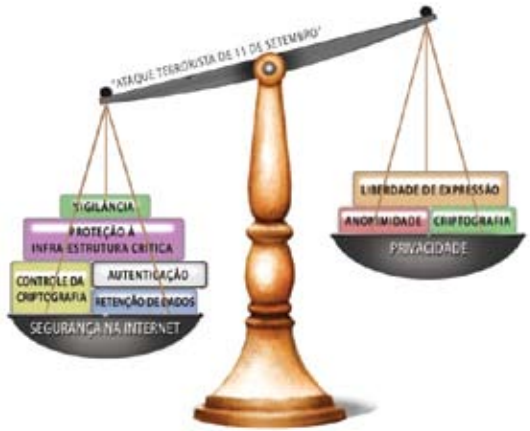
A segurança é muito freqüentemente mencionada como uma das pré-condições para um crescimento mais rápido do comércio eletrônico. Sem uma Internet segura e confiável, os clientes continuarão a relutar em fornecer informações confidenciais online, tal como números de cartões de crédito. O mesmo se aplica aos bancos online e ao uso do dinheiro eletrônico.

Privacidade e segurança na Internet

Outra questão debatida é o vínculo existente entre segurança e direitos humanos. Ter mais segurança na Internet requer algum nível de perda de privacidade? Como deve ser regulamentado o uso de programas de criptografia, que tanto podem ser usados para a proteção legítima da privacidade como para a proteção de comunicações ilegais de terroristas e criminosos? O ponto de equilíbrio entre segurança na Internet e direitos humanos está em mutação constante.

Na esteira dos acontecimentos de 11 de setembro, a segurança tornou-se prioridade nos Estados Unidos, o que se refletiu na aprovação de várias leis nacionais, especificando, entre outras coisas, níveis mais altos de vigilância na Internet. A reação da sociedade civil concentrou-se nos perigos decorrentes para a privacidade e a para o conceito de liberdade de expressão.

A questão do equilíbrio entre tecnologia da informação e privacidade foi destacada nas discussões sobre a possibilidade de estender a Convenção do Conselho da Europa sobre o Cibercrime ao nível global. A principal objeção dos ativistas dos direitos humanos é que a convenção trata de questões de segurança na Internet às expensas da proteção da privacidade e outros direitos humanos.



CRIPTOGRAFIA

Um dos pontos centrais na discussão sobre segurança na Internet é a criptografia, que lida com ferramentas que podem ser usadas para a proteção de comunicações de dados.

Programas de criptografia embaralham a comunicação (*e-mail*, imagens) através de algoritmos matemáticos, tornando-a ilegível. A questão do equilíbrio entre a necessidade de manter a informação confidencial e a necessidade dos governos de monitorem criminosos potenciais e atividades terroristas através dos seus serviços de inteligência resta em aberto.

Os aspectos internacionais das políticas e diretrizes de criptografia são relevantes para a discussão sobre a Governança da Internet, pois a regulamentação da criptografia deve ser global, ou pelo menos envolver os países capazes de produzir ferramentas de criptografia.

Por exemplo, a política do governo dos Estados Unidos de exportar *softwares* de controle de criptografia não foi muito bem-sucedida, pois ele não poderia controlar a distribuição internacional de *softwares* de criptografia. Os fabricantes de programas estadunidenses, por sua vez, deram início a uma pesada campanha de *lobby*. O seu argumento era de que controles de exportação não fortalecem a segurança nacional, mas apenas solapam os interesses da comunidade empresarial dos Estados Unidos.

REGIMES INTERNACIONAIS PARA FERRAMENTAS DE CRIPTOGRAFIA

O problema da criptografia tem sido abordado em dois contextos: o Acordo de Wassenaar e a OCDE. O Acordo de Wassenaar é um regime internacional adotado por 33 países industrializados a fim de restringir a exportação de armas convencionais e de tecnologias de "dupla utilidade" para países em guerra ou considerados "Estados párias". O acordo estabeleceu um secretariado em Viena. O *lobby* dos Estados Unidos junto ao Grupo de Wassenaar visava ampliar a "Abordagem Clipper" internacionalmente, isto é, controlar os programas de criptografia através da custódia de chaves por agências designadas. Muitos países resistiram à proposta, especialmente o Japão e os países escandinavos.

Um acordo foi alcançado em 1998 através da introdução de diretrizes de criptografia, entre as quais uma lista de controle de equipamentos e programas de criptografia de dupla utilidade acima de 56 bits. Esta extensão abrangia ferramentas de Internet, como navegadores e *e-mail*. É interessante observar que este acordo não cobria transferências "intangíveis", como baixar informações na Internet. O fracasso em introduzir uma versão internacional da tecnologia "Clipper" contribuiu para a retirada dessa proposta internamente, nos próprios Estados Unidos. Neste exemplo do vínculo entre as arenas nacionais e internacionais, os desdobramentos internacionais tiveram um impacto decisivo sobre os nacionais.

A OCDE foi o outro fórum de cooperação internacional no campo da criptografia. Ainda que a OCDE não produza documentos legalmente obrigatórios, as suas diretrizes sobre várias questões são altamente respeitadas. Elas resultam de uma abordagem especializada e de um consenso baseado num processo de tomada de decisão. A maior parte das suas diretrizes acabam finalmente incorporadas nas leis nacionais. A questão da criptografia foi um tópico altamente polêmico nas atividades da OCDE. Ela foi inicialmente abordada em 1996, com uma proposta estadunidense de adoção do critério de custódia de chave como norma internacional. Semelhantemente ao que ocorreu em Wassenaar, as negociações sobre a proposta dos Estados Unidos de adoção da custódia de chaves com padrões internacionais sofreu forte oposição do Japão e dos países escandinavos. O resultado foi um compromisso especificando os principais elementos da política de criptografia.

As poucas tentativas de desenvolver um regime internacional de criptografia, principalmente no contexto do Acordo de Wassenaar, não resultaram no desenvolvimento de nenhum regime internacional efetivo. Ainda é possível obter poderosos programas de criptografia na Internet.

SPAM

A SITUAÇÃO ATUAL

O *spam* é geralmente definido como *e-mail* não solicitado, enviado para uma grande quantidade de usuários da Internet. O *spam* é usado princi-

palmente para promoção comercial. Entre outros dos seus usos estão o ativismo social, campanhas políticas e a distribuição de materiais pornográficos. O *spam* está incluído na cesta da infra-estrutura, porque impede o funcionamento normal da Internet por exercer pressão sobre uma das principais aplicações da Internet, o *e-mail*. O *spam* é uma das questões relativas à Governança da Internet que afeta quase todos os que se conectam à Internet. Segundo as últimas estatísticas, de cada 13 mensagens de *e-mail*, 10 podem ser classificadas como *spam*. Além do fato de ser aborrecido e irritante, o *spam* também causa perdas econômicas consideráveis, tanto em termos da largura de banda empregada como em termos de perda de tempo em verificá-lo e apagá-lo. Um estudo recentemente encomendado pela União Européia sobre o *spam* relata que, apenas e tão somente em termos de capacidade de banda, a perda anual situa-se na faixa dos 10 bilhões de euros.

O *spam* pode ser combatido tanto através de meios técnicos como de meios legais. No lado técnico, muitas aplicações para filtrar mensagens e detectar *spam* estão disponíveis. O principal problema com os sistemas de filtragem é que sabe-se que eles também deletam mensagens não *spam*. A indústria anti-*spam* é um setor crescente, com aplicações cada vez mais sofisticadas, capazes de distinguir *spams* de mensagens regulares. Os métodos técnicos têm apenas um impacto limitado e têm de ser completados com medidas legais específicas.

No lado legal, muitas nações-Estado reagiram introduzindo novas leis anti-*spam*. Nos Estados Unidos, a Lei Cam-Spam envolve um delicado equilíbrio entre permitir promoções baseadas em *e-mail* e evitar o *spam*. Embora a lei prescreva sentenças severas por distribuição de *spam*, inclusive penas de até cinco anos de prisão, algumas das suas disposições, segundo os críticos, toleram e poderiam até estimular a atividade dos distribuidores de *spam*. A posição "default" inicial estabelecida na lei é que o spam é permitido até que o destinatário diga "pare" (usando a solicitação de remoção). Como a lei foi adotada em dezembro de 2003, as estatísticas sobre *spam* ainda não evidenciam decréscimos do número de mensagens *spam*.

Em julho de 2003, a União Européia introduziu a sua própria lei anti-*spam* como parte das suas diretivas sobre privacidade e comunicações

eletrônicas. Apesar da exigência da UE de que os Estados membros implementassem essa legislação anti-*spam* até o final de 2003, nove Estados membros não observaram esse prazo. A lei da União Européia estimula a auto-regulamentação e iniciativas do setor privado que conduzam a uma redução da prática de *spam*.

A RESPOSTA INTERNACIONAL

Tanto as leis anti-*spam* adotadas pelos Estados Unidos como aquelas da União Européia têm uma fraqueza: a falta de uma cláusula impedindo o envio de *spam* através de fronteiras. Esta questão é particularmente relevante para países como o Canadá, onde, segundo as últimas estatísticas, em cada 20 *spams*, 19 são provenientes do exterior. A ministra da indústria canadense, Lucienne Robillard, afirmou recentemente que o problema não podia ser resolvido numa base de "país por país". Chegou-se a uma conclusão semelhante num estudo recente sobre a lei anti-*spam* união-européia, levado a cabo pelo Instituto para a Lei da Informação, na Universidade de Amsterdã: "O simples fato de que a maior parte do *spam* venha de fora da UE restringe consideravelmente a Diretivas da União Européia." Uma solução global é necessária, implementada através de tratados internacionais ou de algum mecanismo semelhante.

Spam e desenvolvimento

O spam está causando dificuldades sérias, mas ainda administráveis, nos países desenvolvidos, mas está praticamente incapacitando a infra-estrutura da Internet de muitos países em desenvolvimento. Dada a infra-estrutura subdesenvolvida de baixa velocidade da Internet, o spam ameaça o acesso básico à Internet para muitos usuários dos países em desenvolvimento. Esses países carecem geralmente dos recursos e da especialidade necessárias para combater o spam. Conseqüentemente, o spam amplia a cisão digital existente entre os países desenvolvidos e os países em desenvolvimento.

Um Memorando de Entendimento assinado entre a Austrália, a Coréia e o Reino Unido é um dos primeiros exemplos de cooperação internacional na campanha anti-*spam*.

A OCDE criou uma Força-Tarefa sobre a questão do *spam* e preparou uma caixa de ferramentas anti-*spam*. A UIT também tem sido proativa, organizando o Encontro Temático sobre Contra-*Spam* (de 7 a 9 de julho de 2004) e analisando várias possibilidades de instituir um Memorando de Entendimento Global sobre o Combate ao *Spam*. No âmbito regional, a União Européia instituiu uma Rede de Agências de Repressão Anti-*Spam*, e a Cooperação Econômica Ásia-Pacífico (CEAP) preparou um conjunto de Diretrizes para o Consumidor.

Outra possível abordagem anti-*spam* foi desenvolvida pela principais empresas que lideram a hospedagem de contas de *e-mail* na Internet: America Online, British Telecomm, Comcast, EarthLink, Microsoft e Yahoo! Elas fundaram a Aliança Técnica Anti-*Spam* (ASTA), cuja principal tarefa é coordenar as atividades anti-*spam* nos campos da tecnologia e das políticas e diretrizes.

QUESTÕES

Diferentes definições de *spam*

As diferentes compreensões do que é o *spam* afetam a campanha anti-*spam*. Nos Estados Unidos, o interesse geral pela proteção da liberdade de expressão e a Primeira Emenda também afetam as campanhas anti-*spam*. Os legisladores estadunidenses consideram que spam seja apenas o "*e-mail* comercial não solicitado", deixando de lado outros tipos de *spam*, inclusive os oriundos do ativismo político e da pornografia. Na maioria dos demais países, o *spam* é definido como "todo *e-mail* não solicitado", independentemente do seu conteúdo. Como a maior parte do *spam* é gerada a partir dos Estados Unidos, estas diferenças de definição limitam seriamente qualquer possibilidade de introdução de mecanismos anti-*spam* efetivos.

Spam e autenticação de *e-mail*

Um dos fatores estruturais causadores do *spam* é a possibilidade de enviar mensagens de *e-mail* com falsos endereços de remetente. Há uma solução técnica para este problema, a qual exigiria mudanças nos padrões vigentes na Internet para *e-mail*. A IETF está trabalhando na introdução de mudanças no protocolo de *e-mail*, o qual passaria a resguardar a autenticação do *e-mail*. Este é um exemplo de como questões técnicas (padrões e normas) podem afetar políticas e diretrizes. O possível compromisso, que a introdução da autenticação do *e-mail* implicaria, seria aceitar um nível de restrição da anonimidade na Internet.

A necessidade de uma ação global

Conforme foi afirmado acima, a maior parte dos *spams* tem origem no estrangeiro. Trata-se de um problema global que exige uma solução global. Há várias iniciativas que podem levar a uma melhor cooperação global. Algumas delas, como os Memorandos de Entendimento bilaterais (MOUs), já foram mencionadas. Outras ações incluem construção de capacidades e troca de informação. Uma solução mais abrangente envolveria algum tipo

de instrumento global anti-*spam*. Alguns participantes no último encontro da UIT propuseram a adoção de um MOU multilateral ou a adoção de um instrumento no contexto da CMSI. Até aqui, os países desenvolvidos têm preferido fortalecer as suas legislações nacionais em articulação com campanhas anti-*spam* regionais ou bilaterais. Considerando a sua desvantajosa posição de receber "lixo público global" originário principalmente dos países desenvolvidos, a maioria dos países em desenvolvimento está interessada em formular uma resposta global ao problema do *spam*.

SEÇÃO 3

A cesta legal

A CESTA LEGAL

Quase todos os aspectos da Governança da Internet têm um componente legal, mas a formulação de uma resposta legal ao rápido desenvolvimento da Internet ainda está na sua infância. As duas abordagens prevalecentes dos aspectos legais da Internet são:

a) A abordagem "direito real" (em oposição a "direito virtual" ou "ciberdireito), segunda a qual o tratamento a ser recebido pela Internet não é essencialmente diferente daquele recebido pelas tecnologias de telecomunicações anteriores, desde os sinais de fumaça até o telefone. Embora mais rápida e mais abrangente, a Internet continua a envolver comunicação à distância entre indivíduos, as regras legais existentes podem ser aplicadas a ela.

b) A abordagem "ciberdireito", que se baseia na presunção de que a Internet introduz novos tipos de relacionamentos sociais no ciberespaço. Conseqüentemente, coloca-se a necessidade de formular novas "ciberleis" para o ciberespaço. Um dos argumentos desta abordagem é que o volume e velocidade tremendos das comunicações facilitadas pela Internet através das fronteiras dificulta a aplicação das regras legais existentes.

Embora ambas as abordagens tenham elementos válidos, a abordagem do direito real vem ganhando predominância tanto na análise teórica como em termos de polícias e diretrizes. O pensamento geral é que uma parte considerável da legislação existente pode ser aplicada à Internet. Em certos casos, contudo, como a proteção de marcas registradas, por exemplo, a regras do direito real teriam de ser adaptadas para poderem ser aplicadas ao *mundo ciber*. Outros casos, como o *spam*, devem ser regulamentados por regras novas, concebidas especificamente. A analogia "mundo real" mais próxima do *spam* é a correspondência publicitária, que não é ilegal.

A discussão sobre as preocupações legais divide-se em duas partes: mecanismos legais e questões legais.

MECANISMOS LEGAIS

Os seguintes mecanismos legais ou bem já foram aplicados na Governança da Internet ou então poderão sê-lo:

- Legislação;
- Normas sociais (costumes);
- Auto-regulamentação;
- Regulamentação através do código (solução através de *software*) [ver p. 23];
- Jurisprudência (decisões de tribunais);
- Direito internacional.

Legislação

Toda peça de legislação consiste em regras e sanções. As regras estipulam certos comportamentos aceitos (não cometer crimes, pagar impostos) e sancionam punições específicas nos casos em que as regras não são observadas (e.g. multa, prisão, pena de morte).

Independentemente de qual das duas abordagens – "real" ou "ciber" – seja mais apropriada, o princípio geral resta o mesmo: **leis não tornam comportamentos proibidos impossíveis, mas apenas puníveis**. O fato de a fraude ser proibida tanto no mundo "real" quanto no "ciber" não significa que, como resultado, as fraudes serão erradicadas. A distinção é relevante porque um dos argumentos freqüentes a favor de leis "ciber" separadas é que comportamentos proibidos (fraudes, crimes, etc.) já prevalecem no ciberespaço, onde as regulamentações do direito "real" não podem ser eficazmente aplicadas.

A atividade legislativa se intensificou progressivamente no campo da Internet. Este foi especialmente o caso no seio dos países da OCDE, onde as TICs são disseminadas é tem um alto grau de impacto sobre as relações econômicas e sociais. No que diz respeito a dados, as áreas prioritárias têm sido privacidade, proteção de dados, propriedade intelectual, impostos e cibercrime.

Contudo, as relações sociais são demasiado complexas para serem regulamentadas apenas por legisladores. A sociedade é dinâmica e a legislação anda sempre a reboque da mudança. Esta é uma particularidade notável desta época, dos dias que correm, em que o desenvolvimento tecnológico modifica a realidade social muito mais rápido do que os legisladores podem reagir. Ocasionalmente, regras tornam-se obsoletas antes mesmo de poderem ser adotadas. O risco da obsolescência legal é um consideração importante na questão da regulamentação da Internet.

Governança da Sociedade da Informação

A lei está sempre a reboque da tecnologia

Normas sociais (costumes)

Assim como a legislação, as normas sociais prescrevem um certo comportamento. À diferença da legislação, contudo, nenhum poder do Estado impõe o cumprimento dessas normas. Elas são impostas pela comunidade atrás da pressão dos próprios indivíduos entre si. Nos primeiros tempos da Internet, o seu uso era governado por um conjunto de normas sociais chamado "netiqueta", em que a pressão dos pares e a eventual exclusão da comunidade eram as sanções principais. Durante esse período, em que a Internet era usada principalmente por comunidades acadêmicas relativamente pequenas, as regras sociais eram amplamente observadas. Mas o crescimento da Internet tornou essas regras ineficazes. Este tipo de regulamentação continua a poder ser usado, porém, apenas no interior de grupos restritos com laços comunitários fortes.

Auto-regulamentação

O Documento Estratégico (*White Paper*) dos Estados Unidos sobre Governança da Internet propõe a auto-regulamentação como mecanismo regulador preferido para a Internet. A auto-regulamentação tem elementos comuns com as normas sociais descritas anteriormente. A principal diferença é que, à diferença das normas sociais, que tipicamente envolvem um sistema regulador difuso, a auto-regulamentação se baseia numa abordagem intencional e bem organizada. As regras de auto-regulamentação são geralmente estabelecidas em códigos de prática ou boa conduta.

A tendência rumo a auto-regulamentação é particularmente notável entre os provedores de serviço de Internet (ISPs). Em muitos países, os ISPs estão sob pressão crescente das autoridades governamentais para impor a observância de regras relativas a diretrizes de conteúdo. Os ISPs usam cada vez mais a auto-regulamentação como método para impor certos padrões de comportamento ou, em última análise, obstar a interferência do governo nas suas atividades.

Ao mesmo tempo em que a auto-regulamentação pode ser uma técnica reguladora útil, restam alguns riscos em utilizá-la para regulamentar áreas de alto interesse público, como as diretrizes de conteúdos. Resta a ver até em que medida os ISPs serão capazes de regulamentar conteúdos hospedados em seus sites. Podem eles tomar decisões no lugar das autoridades legais? Pode um ISP julgar o que seja um conteúdo aceitável? Outras questões também devem ser tratadas: liberdade de expressão e privacidade.

Jurisprudência

Jurisprudência e decisões de tribunais constituem um elemento importante do sistema legal estadunidense, o primeiro a lidar com questões legais atinentes à Internet. Neste sistema, precedentes criam leis, especialmente nos casos que envolvem e regulamentação de questões novas, como a Internet. Os juízes têm de julgar casos mesmo que não disponham das ferramentas necessárias – regras legais.

A primeira ferramenta legal que os juízes usam é a analogia legal, em cujos termos algo novo é correlacionado a algo conhecido ou familiar. A maioria dos casos concernentes à Internet são resolvidos através de analogias. Uma lista de analogias está disponível nas páginas 25-29.

Regulamentação Internacional

Uma opinião comum sobre a Governança da Internet é que a natureza global da Internet postula a necessidade de uma regulamentação global. A necessidade de uma abordagem global é freqüentemente confirmada pela ineficácia de medidas nacionais tomadas contra o *spam*, cibercrimes ou outras atividades indesejáveis. O regime da aviação civil é geralmente mencionado como exemplo de regime universal bem-sucedido no combate ao crime. "Desde a adoção dos tratados da aviação civil, as sabotagens e os atos de interferência ilegal declinaram constantemente." Uma das principais razões para isto é que, com a cobertura legal universal da aviação civil, os criminosos não conseguem mais encontrar facilmente um "refúgio seguro". Ao mesmo tempo, a importância de uma abordagem global não significa que algumas questões não possam ou não devam ser regulamentadas nos âmbitos nacional e regional.

A regulamentação global exigirá um consenso universal, o qual só será alcançável, se assim o for, através de um longo processo de negociações. Vários mecanismos legais internacionais devem ser usados no desenvolvimento de um regime de Governança da Internet. Segundo o Estatuto da

Corte Internacional de Justiça, os recursos legais internacionais dividem-se em: tratados, costumes e princípios gerais. Por cima desse conjunto estão as chamadas regras da "*soft law*" ou direito brando, um recurso cada vez mais importante do direito internacional.

Direito dos Tratados. Presentemente, a única convenção que focaliza diretamente questões relacionadas à Internet é a Convenção do Conselho da Europa sobre o Cibercrime. Outras convenções e tratados são apenas parcialmente aplicáveis à Internet. Um exemplo é o *corpus* das convenções sobre direitos humanos. A liberdade de expressão é protegida pelo Artigo 19 do Pacto dos Direitos Civis e Políticos. Outros direitos relativos à Internet, como a privacidade e o direito à informação, são regulamentados por instrumentos globais e regionais de direitos humanos. No campo da resolução de disputas, um dos principais instrumentos e a Convenção de Nova Iorque sobre Arbitragens, de 1958.

A abordagem dominante da Governança da Internet (nacional versus internacional; direito brando *versus* direito duro) influenciará em última análise o tipo e a forma da convenção da Governança da Internet, se um dia ela for acordada. Há quem argumente que a Internet exigirá um instrumento legal abrangente, como a Convenção de Direito do Mar. Esta analogia não é apropriada, pois a negociação do Direito do Mar envolvia, por um lado, a codificação de leis costumeiras existentes e, por outro, a integração de quatro convenções existentes.

Com a Internet, não existe nenhuma lei costumeira. Ela está em formação constante. Muitas abordagens e experiências de tentativa-e-erro foram feitas. Em vez de um tratado abrangente sobre a Internet, o mais provável é que vários instrumentos separados sejam adotados.

Direito Costumeiro. O desenvolvimento do direito costumeiro geralmente requer um longo espaço de tempo, para a cristalização de algumas práticas legalmente obrigatórias. Isto foi possível no passado. Entretanto, o desenvolvimento tecnológico após a Segunda Guerra Mundial exigiu um desenvolvimento rápido dos marcos reguladores internacionais, haja vista as profundas conseqüências econômicas e políticas que as mudanças então experimentadas induziram num espaço muito curto de tempo. A Internet é uma boa ilustração desta tendência. Não é muito provável que o direito costumeiro venha a jogar um papel dominante no seio do regime de Governança da Internet que ora está emergindo.

Direito brando ("*soft law*"). O direito brando relaciona-se geralmente a vários documentos políticos, como declarações, diretrizes e leis modelo.

O critério lingüístico para identificar uma lei "branda" é o uso freqüente da expressão "deveria", em contraste com a expressão "deve", geralmente associada à abordagem mais legalmente obrigatória codificada no direito duro (por exemplo, em tratados).

Muitos casos de arranjos de direito brando têm sido observados por Estados partícipes. Alguns têm importância considerável, como a Lei de Helsinque de 1975, que estabeleceu o arcabouço das relações oriente-ocidente. O direito brando é usado pelos Estados por várias razões, como o fortalecimento da confiança recíproca, o estímulo aos desenvolvimentos em curso e a introdução de novos mecanismos legais e governamentais. O direito brando pode ser uma técnica legal potencialmente aplicável à Governança da Internet.

JURISDIÇÃO

INTRODUÇÃO

A jurisdição é a questão da Governança da Internet que exige a mais urgente atenção. O número de disputas relacionadas à Internet têm crescido constantemente. A confusão sobre a jurisdição pode engendrar duas conseqüências potenciais:

- a incapacidade do Estado de exercer o seu poder legal como entidade responsável pela regulamentação das relações sociais no interior do seu território;
- a incapacidade dos indivíduos e das entidades legais de exercerem o seu direito à justiça (negação de justiça).

Outras conseqüências potenciais da jurisdição ambígua podem ser:

- insegurança legal na Internet;
- desenvolvimento mais lento do comércio eletrônico;
- compartimentação da Internet em zonas legais seguras.

Que relação existe entre jurisdição e Internet?

A noção de jurisdição se baseia predominantemente na divisão geográfica do globo em territórios nacionais. Cada Estado tem o direito soberano de exercer jurisdição sobre o seu território. Não obstante, a Internet faculta consideráveis intercâmbios transfronteiriços, difíceis (embora não seja impossível) de monitorar através dos mecanismos tradicionais de governo. A questão da jurisdição sobre a Internet expõe um dos dilemas-chave associados à questão da Governança da Internet: como é possível "ancorar" a Internet no seio da geografia legal e política existente?

Jurisdição – Técnicas básicas

Há três aspectos principais da jurisdição:

- Que tribunal ou Estado tem a autoridade apropriada? (jurisdição processual);
- Que regras devem ser aplicadas? (jurisdição material);
- Como as decisões dos tribunais devem ser implementadas? (jurisdição penal).

Os seguintes critérios principais são usados para estabelecer a jurisdição em casos específicos:

- Vínculo territorial – o direito de um Estado de exercer governo sobre pessoas e propriedades no interior do seu território;
- Vínculo pessoal – o direito de um Estado exercer governo sobre cidadãos onde quer que eles estejam;
- Vínculo de efeito – o direito de um Estado de exercer governo sobre os efeitos econômicos e legais sobre um território particular, oriundo de atividades conduzidas alhures.

Outro importante princípio do direito internacional moderno é o princípio da jurisdição universal em casos envolvendo brechas na normas legais internacionais essenciais (*ius cogens*), como genocídio e pirataria.

A SITUAÇÃO ATUAL

Os problemas de jurisdição surgem quando as disputas envolvem algum componente extra-territorial (e.g. envolvendo indivíduos de Estados diferentes, ou transações internacionais). Ao colocar um conteúdo na Internet, é difícil saber que lei nacional, se for o caso, pode estar sendo violada. Todo conteúdo da Internet pode ser acessado a partir de qualquer lugar no mundo. Neste contexto, quase toda atividade de Internet tem um aspecto internacional passível de ser encaminhado para muitas jurisdições, o assim chamado efeito de transbordamento.

Os exemplos mais ilustrativos e mais freqüentemente citados a exemplificar esta questão da jurisdição são o caso CompuServe, na Alemanha em 1996, e o caso Yahoo!, na França em 2001.

No caso CompuServe, um tribunal alemão exigiu que a CompuServe proibisse o acesso a materiais pornográficos. Para cumprir a lei alemã, a CompuServe teve de remover o referido material do seu servidor de rede central nos Estados Unidos. Como resultado, inviabilizou-se o acesso para cidadãos que viviam em países em que o acesso à pornografia não era proibido por lei (e.g. os Estados Unidos). A CompuServe teve de aceitar a legislação mais restritiva neste campo. Este caso desencadeou o temor de que toda a Internet tivesse de ajustar-se às legislações mais restritivas (o princípio do mínimo denominador comum).

Uns poucos casos recentes, inclusive o do Yahoo!, julgados nos tribunais franceses, reiteraram a grande relevância do problema das múltiplas jurisdições. O caso Yahoo! foi incitado por causa de uma brecha nas leis francesas sobre a distribuição de materiais nazistas. Essas leis proibiam que qualquer pessoa na França acessasse um determinado site no Yahoo! que exibia *memorabilia* nazista, mesmo que o site estivesse hospedado nos Estados Unidos, onde a exibição do material era e continua a ser legal.

A abordagem "direito real" argumenta que nada havia de novo em casos como o da CompuServe, já que muitos exemplos do efeito de transbordamento já haviam ocorrido no mundo não-Internet. Um exemplo bem conhecido é o estabelecimento, na Comissão da União Européia, de condições estritas para a fusão, por outro lado aprovada pelos Estados Unidos, da Boeing com a McDouglas. Apesar de nenhuma das companhias terem fábricas na Europa, elas ainda assim tiveram de observar a lei de competição da União Européia, a fim de poder continuar vendendo aviões na União Européia.

Ao mesmo tempo em que o raciocínio "direito real" é confiável em princípio, ele de fato apresenta sérias falhas práticas, as quais limitariam a aplicabilidade da lei existente à Internet. O principal problema é o tremendo volume de casos potenciais relacionados à Internet, com quase todos os sites e serviços da rede sendo passíveis de ações legais em algum lugar do mundo. Assim, o aspecto quantitativo (o número de processos) pode pôr em questão o princípio legal e incitar a criação de novas soluções.

SOLUÇÕES POTENCIAIS

Soluções potenciais para o problema das jurisdições múltiplas para a Internet podem ser encontradas em:

- modernizações do direito privado internacional;
- harmonização de leis nacionais, o que tornaria a questão das jurisdições múltiplas menos relevante;
- uso de arbitragens;
- uso de soluções técnicas para identificar a origem dos usuários (principalmente, programa de geolocalização) [ver p. 135].

A modernização do direito privado internacional

Nos procedimentos legais tradicionais, as cortes nacionais decidem se podem ou não julgar um caso e que regras devem ser aplicadas. Decisões envolvendo tanto a jurisdição processual como a jurisdição material são baseadas no direito privado internacional. ("*conflict of laws*" nos sistemas legais anglo-saxãos). Essas regras especificam os critérios para estabelecer a jurisdição, tal como o vínculo existente entre o indivíduo e a jurisdição nacional (e.g. nacionalidade, domicílio), ou o vínculo entre uma transação particular e a jurisdição nacional (e.g. , onde o contrato foi assinado, onde teve lugar o intercâmbio). A Internet torna a aplicação desses critérios mais complexa do que nos casos tradicionais, mas não impossível.

Devido à sua complexidade, à sua lentidão e ao seu alto custo, a abordagem tradicional raramente é usada nas disputas relacionadas à Internet. Ela tampouco se adequa ao *modus operandi* da Internet, que é rápido, simples e pragmático. Os principais mecanismos internacionais do direito privado foram desenvolvidos num tempo em que a interação além-fronteiras era muito menos freqüente e intensiva. Proporcionalmente, menos casos envolviam indivíduos e entidades de diferentes jurisdições. Com o advento da Internet, a interação transfronteiriça tornou-se lugar-comum. Comunicações, intercâmbios e disputas entre instituições e indivíduos de diferentes países são hoje muito mais freqüentes e intensas do que jamais o foram até então.

Uma solução potencial pode ser a modernização do direito privado internacional, a fim de termos processos mais rápidos a custos inferiores para a indicação de jurisdições nacionais em casos de Internet. Entre as possíveis melhorias estariam a simplificação dos procedimentos para identificar a jurisdição nacional apropriada, a opção por deliberações *online*, e arranjos flexíveis para aconselhamento legal.

No âmbito regional, a União Européia adotou a Convenção de Bruxelas, que simplifica o processo de tomada de decisão sobre jurisdições e favorece a proteção aos clientes no caso do comércio eletrônico.

No âmbito global, o foro mais importante do desenvolvimento do direito privado internacional vem sendo a Conferência de Haia. As negociações em curso têm sido dominadas pelos Estados Unidos. Em 1992, os Estados Unidos iniciaram negociações sobre questões de jurisdição com o objetivo principal de fortalecer a proteção à propriedade intelectual através da execução global das decisões dos tribunais estadunidenses. Desde 1992, o crescimento da Internet e do comércio eletrônico modificou a paisagem da negociação. Operar num ambiente de múltiplas jurisdições é cada vez mais arriscado para o interesse das companhias de Internet dos Estados Unidos. Tanto o caso da CompuServe (na Alemanha) como o do Yahoo! (na França) demonstraram como conteúdos hospedados nos Estados Unidos podem desencadear processos em tribunais de outros países.

"Bandeiras de conveniência" da Internet

Outra conseqüência potencial da falta de harmonização será a migração de "dados" e materiais de rede para países com níveis mais baixos de controle de conteúdo. Usando a analogia do Direito do Mar, alguns países podem virar "Bandeiras de conveniência" ou "paraísos" do mundo da Internet.

Se a proposta inicial da Convenção de Haia fosse adotada, representaria um risco considerável para o sistema legal estadunidense. Os tribunais dos Estados Unidos seriam obrigados a executar as decisões de tribunais estrangeiros, o que implicaria que sites de Internet hospedados nos Estados Unidos poderiam vir a representar, em última análise, uma ameaça à liberdade de expressão celebrada na Constituição dos Estados Unidos. A iniciativa teve, assim, uma conseqüência involuntária, a mudança da posição dos Estados Unidos, que reduziram as suas ambições em relação à reforma do sistema do direito privado internacional. A inexistência de progressos na modernização do direito privado internacional a nível global pode fortalecer outras opções de solução para os conflitos jurisdicionais.

A harmonização das leis nacionais

A harmonização das leis nacionais deve resultar no estabelecimento de um conjunto de regras equivalentes no âmbito global. Com regras idênticas implantadas, a questão das jurisdições deve tornar-se menos relevante. A harmonização pode ser alcançada em áreas em que já existe um nível alto de consenso, por exemplo, a pornografia infantil, a pirataria, a escravidão, o terrorismo e o cibercrime. As opiniões estão convergindo em outras questões também, como o *spam* e a segurança na Internet. Não obstante, em alguns campos, inclusive o das políticas e diretrizes de conteúdo, não é muito provável que um consenso global sobre regras básicas seja alcançado.

Outra opção para resolver o problema da jurisdição é a arbitragem, que será discutida a seguir.

ARBITRAGEM

A arbitragem é uma alternativa de solução de disputa que pode ser usada em lugar de procedimentos jurídicos, os quais em geral são lentos e complexos. Nas arbitragens, as decisões são tomadas por um ou mais indivíduos independentes, escolhidos pelos disputantes. A arbitragem internacional no setor empresarial tem um longa tradição. O mecanismo de arbitragem é geralmente definido num contrato privado entre partes que concordem em resolver quaisquer disputas futuras através de arbitragem. É ampla a variedade de contratos de arbitragem disponíveis, especificando questões como local da arbitragem, procedimentos e escolha de leis.

Uma das principais vantagens da arbitragem sobre os tribunais tradicionais é que ela supera o problema da seleção das jurisdições processual e material. Ambas são escolhidas previamente pelos disputantes.

Arbitragens *online* são usadas para resolver não apenas disputas de Internet, mas também disputas comerciais comuns. A arbitragem *online* é conduzida inteiramente pela Internet, inclusive a apresentação de provas e as decisões finais.

A arbitragem oferece vantagens particulares quanto a uma das tarefas mais difíceis nos processos envolvendo a Internet, a execução das decisões (o arbítrio ou sentença). A execução de uma decisão de arbitragem é regulamentada pela Convenção de Nova Iorque sobre o Reconhecimento e a Execução de Sentenças Arbitrais Estrangeiras, assinada pela maioria dos países. Segundo esta convenção, os tribunais nacionais são obrigados a executar as sentenças arbitrais. É mais simples impor a observância de sentenças arbitrais do que de tribunais estrangeiros.

A arbitragem tem sido usada extensivamente para preencher a lacuna produzida pela incapacidade do direito privado internacional atual de lidar com casos relacionados à Internet. Um exemplo particular de uso da arbitragem em casos envolvendo a Internet é a Diretriz Uniforme para Resolução de Disputas de Nomes de Domínio (UDRP). A UDRP foi desenvolvida pela Organização Mundial da Propriedade Intelectual (OMPI) e implementada pela ICANN como procedimento-chave para resolução de disputas. A UDRP é estabelecida previamente como mecanismo de resolução de disputas em todos os contratos envolvendo registro de gTLDs (.com; .edu; .org; .net). O aspecto único é que as sentenças são diretamente aplicadas mediante mudanças no Sistema de Nomes de Domínio sem recorrer à execução através de tribunais nacionais.

Em termos gerais, a arbitragem possibilita um meio mais rápido, mais simples e mais barato de resolver disputas. Não obstante, o uso da arbitragem como principal mecanismo de resolução de disputas relacionadas à Internet tem algumas limitações sérias.

Em primeiro, considerando o fato de que a arbitragem é geralmente estabelecida por acordo prévio, ela não cobre a vasta área de casos em que verifica-se impossível as partes alcançarem acordos por antecedência (calúnia, vários tipos de responsabilidades, cibercrimes).

Segundo, muitos consideram a prática corrente de anexar uma cláusula de arbitragem a contratos regulares como desvantajosa para o lado mais fraco no contrato (geralmente o usuário da Internet ou o cliente do comércio eletrônico).

Terceiro, alguns se preocupam com o fato de que a arbitragem estenda globalmente o direito baseado em precedentes e suprima gradualmente outros sistemas legais nacionais. No caso do direito comercial, isto pode mostrar-se mais aceitável, dado o nível já alto de unificação das regras materiais. Entretanto, a proposição seria mais delicada ao lidar com aspectos socioculturais, sobre os quais os sistemas legais nacionais refletem conteúdos culturais específicos.

Quarto, a jurisprudência existente relacionada à Internet sugere que arbitragens, como as baseadas na UDRP, têm sido mais receptivas aos interesses do setor empresarial do que aos interesses individuais. Veja a seguir, por exemplo, o tratamento de dois casos semelhantes. No primeiro, um tribunal ordinário francês pronunciou sentença contra a empresa francesa "Danone" e a favor de um empregado que, descontente, havia registrado o domínio "jeboycottedanone.com" (eu boicoto Danone).

Num segundo caso, contudo, a arbitragem da OMPI, que se baseia na UDRP, aceitou o pedido da Vivendi Universal para remover o site "vivendiuniversalsucks.com" (Vivendi Universal é uma droga). Em ambos os casos, nomes de domínio foram usados como meio de protesto e de crítica. O tribunal ordinário na França aceitou este tipo de protesto, enquanto a OMPI não o aceitou.

DIREITOS DE PROPRIEDADE INTELECTUAL

Conhecimentos e idéias são recursos-chave na economia global. A sua proteção, através dos Direitos de Propriedade Intelectual (DPIs), está se tornando uma das questões mais importantes da Internet, com conseqüências políticas e legais consideráveis. A questão dos DPIs diz respeito a vários aspectos da Governança da Internet. Como conhecimentos e idéias são uma parte importante da herança cultural e da interação social, encerram um valor especial para muitas sociedades. OS DPIs também estão no centro do debate sobre desenvolvimento. Os DPIs relacionados à Internet incluem marcas registradas, direitos autorais e patentes.

MARCAS REGISTRADAS

A relevância das marcas registradas para a Internet relaciona-se ao registro dos nomes de domínio. Na fase inicial do desenvolvimento da Internet, o registro de nomes de domínio seguia o princípio "Primeiro a chegar, primeiro a ser servido" [*First Come, First Served* – FCFS]. Isto levou ao *cybersquatting*, a prática de registrar nomes de empresas e depois revendê-los a preços elevados. Com o crescimento da importância da Internet, este tornou-se um problema maior, pois as empresas tornaram-se suscetíveis de serem mal representadas ou distorcidas na Internet. Os remédios legais através dos sistemas judiciários comuns não eram muito práticos, pois os casos demoravam tempo demais para serem resolvidos.

Esta situação obrigou o setor empresarial a colocar a questão da proteção das marcas registradas no centro da reforma da Governança da Internet,

levando à fundação da ICANN em 1998. No Documento Estratégico (*White Paper*) sobre a ICANN, o governo dos Estados Unidos postula que a ICANN desenvolva um mecanismo para a proteção de marcas registradas no campo dos nomes de domínio. Logo depois da sua formação, a ICANN introduziu a Diretriz Uniforme para Resolução de Disputas de Nomes de Domínio (UDRP), desenvolvida pela OMPI.

A utilização da UDRP como mecanismo para resolução de disputas é uma estipulação compulsória em todos os contratos de registro de domínio para domínios do primeiro nível, como .com; .org; e .net. Os proprietários de marcas registradas estimulam a extensão da UDRP ao domínios de países.

A questão das marcas registradas também é tratada nas seguintes partes desta brochura:

- O sistema de nomes de domínio (DNS) (p. 45);
- Diretriz Uniforme para Resolução de Disputas de Nomes de Domínio (UDRP) (p. 86).

DIREITOS AUTORAIS

O conceito tradicional de direito autoral foi questionado de numerosas maneiras pelos desenvolvimentos da Internet, desde de simples operações de "cortar e colar" textos a partir da rede até atividades mais complexas, como a distribuição de arquivos de música e de vídeo pela rede. Materiais podem ser copiados e distribuídos mundialmente através da Internet, sem custos significativos.

O direito autoral protege apenas a expressão de uma idéia conforme materializada sob diversas formas, como livro, CD, arquivo de computador, etc. A idéia em si mesma não é protegida pelo direito autoral.

Esses desenvolvimentos colocam em perigo o delicado equilíbrio existente entre o interesse dos autores de materiais protegidos e o interesse público por criatividade, conhecimento público e bem-estar geral crescentes. Impedir a cópia ilimitada de materiais e, ao mesmo tempo, salvaguardar o acesso via Internet a esses materiais é um dos enigmas da Governança da Internet. Até aqui, representados pelas

principais companhias gravadoras e de multimídia, os proprietários de direitos autorais têm sido mais proativos na proteção dos seus interesses. O interesse público foi apenas vagamente percebido e não suficientemente protegido.

Um dos desenvolvimentos divisor de águas no campo dos direitos autorais, desencadeador de uma resposta ativa dos proprietários desses direitos, foi o compartilhamento de músicas através de redes de usuários (P2P ou "*peer-to-peer*"). Estima-se que o Napster, o primeiro e principal exemplo, tenha produzido perdas de 4,3 bilhões de dólares para a indústria fonográfica. A reação da indústria de gravação musical evidenciou a existência de muitas armadilhas, analogias equivocadas e insuficiências no sistema legal vigente. O caso também ilustra a situação atual da proteção aos direitos autorais na Internet e as numerosas questões atinentes que ainda permanecem em aberto.

A SITUAÇÃO ATUAL

Proteção mais rigorosa aos direitos autorais nos âmbitos nacional e internacional

As indústrias fonográficas e do entretenimento têm feito *lobby* intensivamente nos âmbitos nacional e internacional para fortalecer a proteção ao direito autoral. Nos Estados Unidos, a proteção mais rigorosa ao direito autoral foi introduzida através da Lei de Direitos Autorais Digitais do Milênio (DMCA), de 1998. No âmbito internacional, a proteção de artefatos digitais foi introduzida pelo Tratado do Direito Autoral da OMPI (1996). Este tratado também contém cláusulas para apertar o regime de proteção ao direito de autor, como disposições sobre limitações aos direitos exclusivos do autor, a proibição de fraudar as proteções tecnológicas aos direitos autorais e outras medidas correlatas.

O número crescente de processos

Somente em 2003, cerca de mil intimações baseadas na DMCA foram emitidas contra ISPs, exigindo que interrompessem as atividades de compartilhamento de arquivos de seus assinantes, e foram abertos mais de quinhentos processos contra indivíduos.

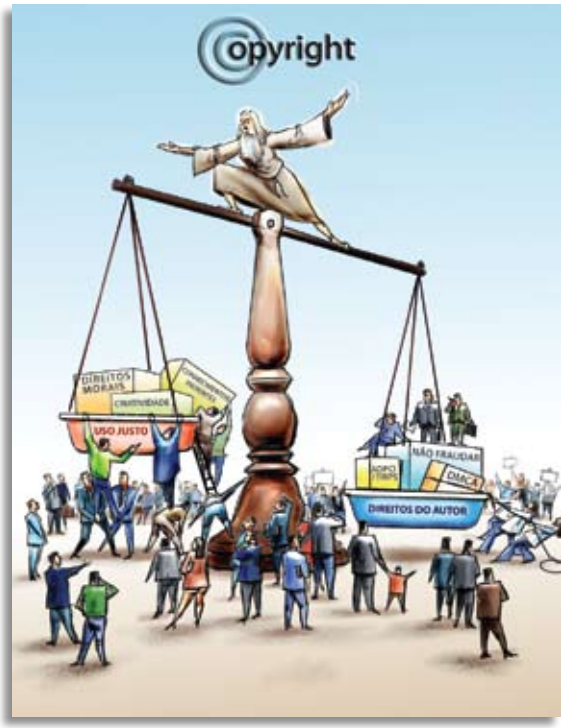
Um caso particularmente relevante para o futuro dos direitos autorais na Internet foi o processo contra a Grokster e a StreamCast, duas companhias que fabricam programas de compartilhamento de arquivos P2P. Seguindo a disposições da DMCA, a Associação de Gravadoras dos Estados Unidos

exigiu que essas companhias desistissem do desenvolvimento da tecnologia de compartilhamento de arquivos, que contribui para a violação de direitos autorais. Inicialmente, sob reserva de circunstâncias razoáveis, os tribunais norte-americanos optaram por não responsabilizar a Grokster e a StreamCast pela eventual violação dos direitos autorais. Não obstante, em junho de 2005, a Suprema Corte dos Estados Unidos determinou que os desenvolvedores de softwares eram responsáveis por quaisquer possíveis maus usos ou abusos dos programas por eles desenvolvidos.

Software contra a violação do direito autoral

As mesmas ferramentas que são usadas pelos infratores também podem ser usadas pelos defensores dos direitos autorais. Tradicionalmente, as autoridades estatais e as empresas desempenharam as suas responsabilidades através de mecanismos legais. Contudo, é crescente o uso de ferramentas "alternativas" de *software* pelo setor empresarial contra violadores de direitos autorais.

Um artigo no *International Harold Tribune* dá uma lista das seguintes táticas baseadas em programas, usadas por empresas gravadoras/de entretenimento para proteger seus direitos autorais:



- um *Trojan Horse* que redireciona os usuários para sites onde podem comprar legalmente a canção que estavam tentando baixar;
- programas "freeze", que bloqueiam o computador por um período de tempo e exibem uma advertência sobre baixar músicas pirateadas;
- programas "silence", que escaneiam o disco duro e tentam remover quaisquer arquivos pirateados encontrados;

- programas "interdiction", que impedem o acesso à Rede daqueles que tentam baixar músicas pirateadas.

O professor Lawrence Lessig, da Escola de Direito de Stanford, advertiu que tais medidas podem ser ilegais. Ele observou que as medidas especificadas acima não estão incluídas entre as aprovadas para lidar com a violação de direitos autorais. Estariam as companhias que tomaram tais medidas de auto-ajuda infringindo a lei?

Tecnologias para a gestão dos direitos digitais

Numa abordagem de mais longo prazo e mais estrutural, o setor empresarial introduziu várias tecnologias de gestão do acesso a materiais com proteção de direitos autorais. A Microsoft introduziu o programa Gerenciamento de Direitos Digitais (DRM), para gerir o *download* de arquivos de som, filmes e outros materiais com proteção de direito autoral. Sistemas semelhantes foram desenvolvidos pela Xerox (ContentGuard), Philips e Sony (InterTrust).

O uso de ferramentas tecnológicas para proteção de direitos autorais recebeu apoio tanto no âmbito internacional (Tratado do Direito Autoral da OMPI) como no nacional, com a Lei de Direitos Autorais Digitais do Milênio (DMCA), nos Estados Unidos. Além disso, a Lei DMCA criminalizou atividades voltadas para fraudar a proteção tecnológica de materiais com proteção de direitos autorais.

QUESTÕES

Desenvolver novos mecanismos de direito autoral ou aperfeiçoar os existentes?

Como devem os mecanismos de direitos autorais serem ajustados para refletirem as profundas mudanças levadas a efeito pelos desenvolvimentos das TICs e da Internet? A resposta sugerida pelo Documentos Estratégico do governo dos Estados Unidos sobre *Propriedade intelectual e a infra-estrutura nacional de informação* é de que apenas mudanças menores são necessárias, principalmente através da "desmaterialização" dos conceitos de direito autoral de "fixação", "distribuição", "transmissão" e "publicação". Esta abordagem foi seguida pelos principais tratados internacionais de direitos autorais, incluindo a ADPCI/TRIPS (Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio) e as Convenções de Direitos Autorais da OMPI.

Entretanto, a opinião oposta argumenta que as mudanças no sistema legal têm de ser profundas, considerando que os direitos autorais na era digital já não dizem mais somente respeito ao "direito de impedir cópias", mas

também ao "direito de impedir acesso". Na verdade, com as possibilidades técnicas sempre crescentes de impedir o acesso a materiais digitais, pode-se indagar se a proteção aos direitos autorais é mesmo necessária. E resta a examinar como o interesse público, a segunda parte da equação dos direitos autorais, será protegido.

Proteção do interesse público – "uso justo" de materiais com proteção de direitos autorais

O direito autoral foi inicialmente concebido para estimular a criatividade e a invenção. É por esta razão que combina dois elementos: a proteção dos direitos do autor e a proteção dos interesses públicos. O principal desafio foi estipular como o público poderia consultar materiais protegidos por direitos autorais, de modo a deixar aumentar a criatividade, o conhecimento e o bem-estar globais. Operacionalmente falando, este interesse público foi protegido pelo conceito de "uso justo" de materiais protegidos. Define-se geralmente o uso justo como o uso para fim de pesquisa acadêmica e outros propósitos não comerciais.

Direito autoral e desenvolvimento

Qualquer restrição ao uso justo pode enfraquecer a posição dos países em desenvolvimento. A Internet fornece aos pesquisadores, estudantes e outros interessados dos países em desenvolvimento uma ferramenta poderosa de participação nos intercâmbios acadêmicos e científicos. Um regime de direitos autorais restritivo pode ter um impacto negativo sobre a construção de capacidades nos países em desenvolvimento.

Outro aspecto é a digitalização crescente das habilidades artísticas e culturais dos países em desenvolvimento. Paradoxalmente, os países em desenvolvimento podem acabar tendo de pagar para ter acesso à sua própria herança artística e cultural quando ela se for digitalizada, reacondicionada e protegida por companhias de entretenimento e de mídia.

OMPI e ADPCI/TRIPS

Dois regimes internacionais principais existem para a proteção de direitos autorais. A Organização Mundial da Propriedade Intelectual (OMPI) gerencia o regime tradicional de Direitos de Propriedade Intelectual (DPIs), baseado nas convenções de Berna e de Paris. Outro regime emergente é gerido pela OMC e baseado nos ADPCI/TRIPS (Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio). A mudança da coordenação dos DPIs internacionais da OMPI para a OMC foi levada a cabo

em vista de fortalecer a proteção aos DPIs, especialmente no campo da execução legal. Este foi um dos maiores ganhos dos países desenvolvidos durante a Rodada Uruguaia das negociações da OMC.

Muitos países em desenvolvimento se preocupam com este desdobramento. Os mecanismos rigorosos de execução da OMC podem reduzir o seu espaço de manobra e a possibilidade de equilibrar as suas necessidades de desenvolvimento com a proteção internacional, principalmente baseada nos Estados Unidos, dos direitos de propriedade intelectual. Até agora, o foco principal da OMC e da ADPCI tem estado nas várias interpretações dos DPIs de produtos farmacêuticos. É muito provável que as discussões futuras se estendam para a questão da relação entre DPIs e Internet.

A responsabilização dos ISPs por violações de direitos autorais

Os mecanismos de execução internacional no campo da propriedade intelectual foram fortalecidos quando os ISPs passaram a ser responsabilizados por hospedarem materiais que violem direitos autorais, se o material não for removido imediatamente após a notificação da infração. Isto tornou o regime anteriormente vago dos provedores de serviços de Internet diretamente executável no campo da Internet.

PATENTES

Tradicionalmente, a patente protege um novo processo ou produto de natureza principalmente técnica ou manufatora. Só recentemente patentes começaram a ser concedidas a programas de computador. E decorre que mais registros de patentes resultam em mais processos nos tribunais entre as companhias de *software* estadunidenses.

Para a Governança da Internet, o principal desenvolvimento foi a concessão flexível da proteção de patentes para processos comerciais na Internet, como o "1-Click" usado pela Amazom.com. A principal crítica a esta decisão é que a Amazon só teria protegido a idéia (o uso de um clique) e não um processo comercial particular.

O registro bem-sucedido da patente de "1-Click" desencadeou uma onda de registros, inclusive de algumas propostas ridículas, como uma patente do *download* na Internet. Outro caso polêmico foi o pedido da British Telecom de pagamento de licença à sua patente do *link* de hipertexto, registrada nos anos 1980. Se a British Telecom ganhar este caso, os usuários de Internet terão de pagar uma taxa cada vez que um *link* de hipertexto for criado ou usado. Se não ganhar, o caso entra para a história junto com outros casos do mesmo tipo, como uma tentativa de patentear a roda.

É importante sublinhar que a prática de conceder patentes a programas e procedimentos relacionados à Internet não é apoiada na Europa e na maioria dos demais países.

CIBERCRIME

A tecnologia é desenvolvida para ser **usada**, mas muito freqüentemente ela é **mau usada** ou mesmo **abusada**. Em geral, o cibercrime diz respeito a abusos da informação e da tecnologia de comunicações. Ao passo que o componente "crime" do termo foi claramente definido, (e.g. roubo, pornografia infantil, etc.), as opiniões sobre o significado de "ciber" variam e são abundantes.

Na discussão sobre o cibercrime, existe uma dicotomia entre direito "ciber" e direito "real". A abordagem do direito real enfatiza que o cibercrime é apenas um crime *off-line*, isto é, fora de linha, cometido com computadores. O crime é o mesmo, apenas as ferramentas são diferentes. A abordagem do ciberdireito destaca que os elementos únicos do cibercrime justificam um tratamento específico, especialmente no que diz respeito à execução legal e à prevenção.

Os minutadores da Convenção do Conselho da Europa sobre o Cibercrime estavam mais próximos da abordagem do ciberdireito, salientando que o único aspecto específico do cibercrime era o uso das TICs como meio para cometer o crime. A convenção, que entrou em vigor em 1º de julho de 2004, é o principal instrumento internacional neste campo.

A convenção regulamenta fraudes relacionadas a computadores, como violação de direitos autorais, pornografia infantil e segurança da rede.

O protocolo recentemente adotado pela convenção acrescenta a distribuição de conteúdos racistas ou xenófobos como mais um crime por ela regulamentado.

A convenção especifica vários mecanismos processuais para as atividades de repressão ao crime desenvolvida pelos Estados, como compartilhar dados relacionados ao cibercrime, inclusive os registros de tráfego na Internet. Responsabilidades especiais foram atribuídas aos provedores de serviço de Internet neste regime de combate ao cibercrime, incluindo a obrigação de manter os arquivos *log* de conexões dos usuários da Internet e facilitar a sua interceptação legal para subsidiar eventuais coletas de provas. Resta a saber se a convenção será ou não ratificada pelo congresso dos Estados Unidos; tal ratificação seria um passo importante na direção de uma ação global da Convenção.

Além do Conselho da Europa, o G8 adotou um Plano de Ação que especifica ações coordenadas no caso dos seguintes crimes relacionados à Internet: pedofilia e exploração sexual, tráfico de drogas, lavagem de dinheiro, fraude eletrônica, assim como espionagem industrial ou de assuntos de Estado.

Em 2003, a OCDE produziu diretrizes para dar assistência aos governos no combate a fraudes relacionadas à Internet. A União Européia iniciou um processo de adoção de uma Decisão-Quadro sobre Cibercrime, fortalecendo medidas práticas e a cooperação no campo do cibercrime.

QUESTÕES

Definição de cibercrime

A definição de cibercrime é uma das questões centrais a ter impacto legal prático. Muitas diferenças sérias ocorrem na interpretação do cibercrime, e isto pode ter conseqüências diretas sobre a eficácia do regime internacional de combate ao cibercrime.

Por exemplo, se o foco das definições do cibercrime for o método – como acessos não autorizados a sistemas protegidos de computadores – há um risco potencial de confusão entre cibercrime e hackerismo (uma forma de desobediência civil digital).

Cibercrime *versus* direitos humanos

A Convenção sobre o Cibercrime fortaleceu a discussão sobre o equilíbrio entre segurança e direitos humanos. Muitas preocupações vieram à tona,

expressas principalmente pela sociedade civil, de que a convenção estivesse dando poderes excessivos às autoridades estatais, inclusive o direito de controlar computadores de *hackers*, de vigilância das comunicações e assim por diante. Poderes de tal modo amplos teriam o potencial de colocar em perigo alguns direitos humanos, particularmente a privacidade e a liberdade de expressão.

Coleta e preservação de provas

Um dos principais desafios no combate ao cibercrime é a coleta de provas para apresentação em tribunais. A velocidade das comunicações hoje em dia exige uma resposta rápida das agências encarregadas da execução das leis. Uma possibilidade de preservar provas encontra-se nos registros de conexão com a rede, os quais informam quem acessou tal ou qual recurso particular da Internet, e quando o fez. Algumas cláusulas da Convenção sobre Cibercrime lidam com esta questão.

ASSINATURAS DIGITAIS

Em termos gerais, assinaturas digitais estão ligadas à autenticação de indivíduos na Internet, o que produz impactos sobre muitos aspectos da Internet, inclusive jurisdição, cibercrime e comércio eletrônico. O uso de assinaturas digitais deve contribuir para construir ou fortalecer a confiança na Internet.

A assinatura digital faz parte em geral do quadro do comércio eletrônico. Ela aí está para facilitar as transações e-comerciais mediante a conclusão de contratos eletrônicos. Por exemplo, é um contrato válido e obrigatório se for fechado via *e-mail* através de um site da Internet? Em muitos países, a lei exige que contratos devam ser "por escrito" ou "assinados". O que significa isto em termos de Internet?

Confrontados a estes dilemas e forçados por pressões a estabelecer um ambiente favorável ao comércio eletrônico, muitos governos começaram a adotar legislações sobre assinaturas digitais. O principal desafio é que muitos governos não estão regulamentando problemas existentes, como cibercrimes ou violações de direitos autorais, mas criando um novo

ambiente no qual não têm nenhuma experiência prática. Isto tem resultado numa série interminável de soluções e numa vagueza generalizada das disposições legais sobre as assinaturas digitais.

Surgiram três abordagens principais para a regulamentação das assinaturas digitais. A primeira é uma abordagem "minimalista", especificando que assinaturas eletrônicas não podem ser recusadas com base no fato de estarem sob forma eletrônica. Esta abordagem especifica um uso muito amplo de assinaturas digitais e foi adotada por países praticantes do direito consuetudinário: Estados Unidos, Canadá, Nova Zelândia e Austrália.

A segunda abordagem é "maximalista" e estabelece um quadro e procedimentos para as assinaturas digitais, inclusive a criptografia e o uso de identificadores de chave públicos. Esta abordagem geralmente especifica o estabelecimento de autoridades certificadoras exclusivas que possam legitimar futuros usuários de assinaturas digitais. Ela prevalece em países europeus, como a Alemanha e a Itália.

A terceira abordagem, adotada pela Diretiva da União Européia sobre Assinatura Digital, combina as duas abordagens acima mencionadas. Ela contém disposições minimalistas quanto ao reconhecimento de assinaturas fornecidas por meio eletrônico. O enfoque maximalista também é contemplado na confirmação de que "assinaturas eletrônicas avançadas" terão um efeito legal mais importante (e.g. essas assinaturas são de comprovação mais fácil em processos legais).

A regulamentação da União Européia sobre assinaturas digitais foi uma das respostas à questão no âmbito multilateral. Embora tenha sido adotada por todos os Estados membros da UE, restam diferenças no *status* legal da assinatura digital. Só oito países implementaram a exigência da Diretiva de que assinaturas digitais fossem tratadas da mesma maneira que assinaturas ordinárias.

No âmbito global, a UNCITRAL 2001 (Comissão das Nações Unidas para o Direito Mercantil Internacional) adotou a Lei Modelo sobre Assinaturas Eletrônicas. Esta lei outorga o mesmo *status* a assinaturas eletrônicas e manuscritas, desde que certas exigências técnicas sejam cumpridas.

A Câmara de Comércio Internacional (CCI) publicou o documento "Uso Geral para Comércio Digital Internacionalmente Assegurado" (GUIDEC), que apresenta um estudo sobre as melhores práticas e regulamentações, bem como questões de certificação.

Diretamente ligadas à questão das assinaturas digitais estão as iniciativas de infra-estrutura de chave pública (PKI). Duas organizações, a UIT e a IETF, estão envolvidas na padronização da PKI.

QUESTÕES

A necessidade de padrões detalhados de implementação

Embora muitos países desenvolvidos tenham adotado legislações amplas sobre assinatura digital, em si mesmas elas carecem de padrões e de procedimentos detalhados de implementação. Considerando a novidade da questão, muitos países estão esperando para ver em que direção os padrões concretos vão desenvolver-se. As iniciativas de padronização ou normalização ocorrem em vários níveis, inclusive organizações internacionais (UIT) e associações profissionais (IETF).

O risco de incompatibilidade

A variedade de abordagens e padrões no campo das assinaturas digitais pode levar a incompatibilidades entre diferentes sistemas nacionais. As soluções fragmentárias podem restringir o desenvolvimento do comércio eletrônico na escala global. Seria desejável que a necessária harmonização fosse promovida através de organizações regionais e globais.

DIREITO TRABALHISTA

Menciona-se freqüentemente que a Internet está mudando "a maneira como nós trabalhamos". Embora este problema requeira uma elaboração mais ampla, os seguintes aspectos têm relevância direta para a Governança da Internet:

- A Internet introduziu um nível elevado de empregos temporários de curto prazo. O termo "permatemp" foi cunhado por empregados que são mantidos por longos períodos mediante contratos de prestação temporários regularmente renovados. Isto engendra um nível mais baixo de proteção social para a força de trabalho.
- O teletrabalho está se tornando cada vez mais relevante com o desenvolvimento das telecomunicações, especialmente com o acesso de banda larga à Internet.
- A terceirização a outros países no setor de serviços das TICs, como centrais de chamadas ou unidades de processamento de dados, está crescendo. Um volume considerável desta atividade já foi transferido para países com mão-de-obra barata, principalmente na Ásia e na América Latina.

As TICs diluiram os contornos da rotina tradicional de trabalho, lazer e sono (8+8+8 horas). É cada vez mais difícil distinguir onde o trabalho começa e onde acaba. Essas mudanças nos padrões de trabalho podem exigir a formulação de uma nova legislação trabalhista, para tratar de questões como horas de trabalho e a proteção dos interesses e da remuneração laborais.

No campo do direito trabalhista, a questão da privacidade no local de trabalho é importante. Tem o empregador direito de monitorar o uso da Internet por seus empregados (como conteúdos de mensagens de *e-mail* e acesso a sites)? A jurisprudência vem se desenvolvendo gradualmente neste campo, oferecendo uma variedade de novas soluções.

Na França, em Portugal e na Grã-Bretanha, as diretrizes legais e alguns casos específicos tenderam a restringir a vigilância do correio eletrônico dos empregados. O empregador é obrigado a notificar previamente quaisquer atividades de monitoramento. Na Dinamarca, os tribunais julgaram um caso de demissão de um empregado por envio de mensagens de *e-mail* particulares e acesso a sites sexualmente orientados. O tribunal decidiu que a demissão não era legal, pois o empregador não dispunha de uma diretriz de uso da Internet que proibisse o seu uso extra-oficial. Um outro argumento utilizado pela corte dinamarquesa foi o fato de o uso da Internet pelo empregado não afetar o seu desempenho profissional.

O direito trabalhista tem sido, tradicionalmente, uma questão nacional. Contudo, a globalização em geral e a Internet em particular levaram a uma internacionalização das questões trabalhistas. Com um número crescente

de indivíduos trabalhando para entidades estrangeiras e interagindo com equipes de trabalho em bases globais, coloca-se crescentemente a necessidade de mecanismos reguladores internacionais apropriados. Este aspecto foi reconhecido na declaração da CMSI, que, em seu Parágrafo 47, reivindica o respeito a todas as normas internacionais relevantes no campo do mercado de trabalho das TICs.

PRIVACIDADE E PROTEÇÃO DE DADOS

Privacidade e proteção de dados são questões estreitamente inter-relacionadas de Governança da Internet. A proteção de dados é um mecanismo legal que assegura a privacidade.

O que é a privacidade? A definição de privacidade depende de perspectivas individuais. Alguns indivíduos não se importam de revelar algum nível de informação privada, enquanto outros guardam a sua privacidade mais rigorosamente. A privacidade também é determinada pelas culturas nacionais. Embora a questão da vida privada seja importante nas sociedades ocidentais, ela pode ter menos importância em outras culturas.

Não obstante, tendo em mente essas reservas, a noção de privacidade tem de ser definida antes de poder ser usada como um conceito legal. O espectro de definições é amplo. Uma definição tradicional descreve a privacidade como "o direito de ser deixado em paz". Definições modernas de privacidade concentram-se no caráter privado das comunicações (nenhuma vigilância sobre comunicações) e da informação (nenhuma manipulação de informações sobre indivíduos). Tradicionalmente, ligava-se a privacidade, principalmente, à relação entre os cidadãos individuais e o Estado. Hoje em dia, porém, o quadro do respeito à privacidade se ampliou e agora também abrange o setor empresarial, conforme refletido na ilustração na página seguinte.

Proteção à privacidade: indivíduos e Estados

A informação sempre foi uma mercadoria essencial para a supervisão, pelas autoridades do Estado, do seu território e da sua população.

Isto pode ser visto nos registros escritos mais antigos, a maioria dos quais trata de funções do Estado. As tecnologias de informação aumentaram imensamente as capacidades do Estado de reunir e analisar informações. Isto inclui a informação gerenciada tanto por órgãos do governo (registros fiscais, de propriedade, previdência social, saúde, fichas criminais, etc.) como empresas licenciadas por governos para fornecer serviços essenciais (eletricidade, água, telecomunicações).

Toda essa informação é coletada com a aquiescência implícita mas involuntária dos cidadãos, pois lhes é impossível optarem por desfiliarem-se desses arranjos, a menos que emigrassem para outros países, onde de todo modo seriam confrontados ao mesmo problema.

Tecnologias, tais como o armazenamento de dados, são usadas para agregar e relacionar dados de muitos sistemas individuais (por exemplo, imposto de renda, registro de imóveis, propriedade de automóveis) em vista de conduzir análises sofisticadas em busca de padrões, incoerências, padrões inusuais e outras revelações deste tipo. Elas podem ter um impacto dramático sobre a sociedade e, na maioria dos casos, ainda permanecer no âmbito da Declaração Universal dos Direitos Humanos.

Terrorismo, espionagem e outras atividades contra o Estado deram lugar a um aumento da vigilância exercida sobre indivíduos suspeitos (sejam eles

nacionais do Estado em questão ou não). Os ativistas dos direitos civis têm advertido sobre a erosão gradual da privacidade pessoal, decorrente da introdução de medidas de segurança nacional cada vez mais restritivas.

Há poucos anos, a proposta de equipar computadores pessoais com um processador que lhes daria uma identidade exclusiva, o *chip* "Clipper" (que, coincidentemente ou não, também poderia ser usado para servir de porta traseira para a vigilância por governos), causou considerável exaltação pública. A batalha do Clipper foi ganha pelos partidários do livre-arbítrio, mas hoje a balança pende novamente para o lado do fortalecimento da segurança nacional.

Depois de 11 de setembro, a Lei Patriota nos Estados Unidos e legislações comparáveis em outros países introduziram uma perspectiva de controle mais rigoroso das comunicações eletrônicas, inclusive uma cláusula prevendo o conceito de Interceptação Legítima. Este conceito também foi incluído na Convenção do Conselho da Europa sobre o Cibercrime de 2001 (Artigos 20 e 21) para fundamentar a coleta de indícios.

Ferramentas de vigilância mais poderosas surgirão à medida da evolução da tecnologia. Elas podem vir a fortalecer o papel do Estado e, ao mesmo tempo, reduzir a privacidade dos indivíduos.

Proteção da privacidade: indivíduos e empresas

A segunda relação neste triângulo da privacidade, que ganha cada vez mais importância, é aquela existente entre os indivíduos e o setor empresarial. Numa economia da informação, as informações sobre clientes, incluindo as suas preferências e perfis de compra, tornam-se uma mercadoria importante. Vender dados sobre clientes é um negócio muito lucrativo na Internet.

Um tipo diferente de "vigilância" existe entre os indivíduos e as empresas, e muito particularmente no caso do comércio eletrônico.

Neste caso, milhões de indivíduos revelam voluntariamente um volume considerável de informações pessoais para organizações empresariais: números de cartões de crédito, endereços detalhados e outras informações que, se usadas de maneira imprópria, podem levar a sérias conseqüências, como fraudes ou roubos de identidade.

O sucesso e a sustentabilidade do comércio eletrônico, tanto de empresas com indivíduos como de empresas com empresas, depende do estabelecimento de uma confiança extensiva tanto na política de privacidade das empresas como nas medidas de segurança por elas implantadas para proteger as informações confidenciais dos seus clientes contra roubos e abusos.

Organizações empresariais também exploram tecnologias de armazenamento de dados para adquirir um nível de controle dos hábitos e preferências dos seus clientes. Supermercados utilizam esquemas de cartões de fidelidade para levantar os hábitos de compra dos seus clientes, os dias/horas da semana em que preferem fazer compra, quanto gastam, que produtos compram (pois o armazém de dados também está conectado ao terminal de caixa).

Os resultados dessas análises são usados em seguida para orientar iniciativas de *marketing* dirigidas a domicílios individuais. Se não houver uma legislação funcional de proteção de dados, a informação coletada sobre indivíduos por empresas pode ser vendida e usada em outros contextos.

Proteção da privacidade: Estado e empresas

Este terceiro lado do triângulo é o que tem a menor publicidade e possivelmente a maior relevância. Ambos os pólos, Estado e mundo empresarial, coletam volumes consideráveis de dados sobre indivíduos. Assinalou-se o intercâmbio de uma parcela desses dados no contexto das atividades antiterrorismo. Não obstante, em algumas situações, como no caso da Diretiva da União Européia sobre Proteção de Dados, o Estado supervisiona e protege dados mantidos por empresas privadas sobre indivíduos.

Proteção da privacidade: entre indivíduos

O último aspecto da proteção da privacidade, que não está representado no esquema do triângulo, é o risco potencial produzido por indivíduos. Hoje, a tecnologia facultou a indivíduos o uso de ferramentas poderosas de vigilância. Mesmo um simples telefone celular com câmera pode tornar-se uma ferramenta de vigilância. Hoje em dia, os mais sofisticados mini câmeras e microfones podem ser comprados a preços razoáveis. Para citar *The Economist*, a tecnologia "democratizou a vigilância". Muitos casos de invasão de privacidade foram documentados, de simples voyerismo até o uso mais sofisticado de câmeras para registrar números de cartões bancários em caixas eletrônicos e outras formas de espionagem.

O principal problema é que a legislação se concentra nos riscos à privacidade provenientes de eventuais intervenções do Estado. Confrontados com esta nova realidade, alguns governos começam a dar os primeiros passos. O congresso estadunidense adotou a Lei de Prevenção ao Voyeurismo por Vídeo, proibindo a tomada de fotos ou cenas de pessoas despidas sem autorização. Leis semelhantes de defesa da privacidade, restringindo a vigilância individual, também foram adotadas na Alemanha e em alguns outros países.

A regulamentação internacional da privacidade e da proteção de dados

O principal documento internacional sobre privacidade e proteção de dados é "Diretrizes da OCDE para a Proteção da Privacidade e do Fluxos Transfronteiriços de Dados Pessoais", de 1981. Essas diretrizes e o trabalho desenvolvido em seguida inspiraram a formulação de muitas regulamentações regionais e internacionais neste campo. Os princípios propostos pelas Diretrizes OCDE foram amplamente aceitos, as principais diferenças estando na forma como foram implementados.

Uma abordagem, adotada nos Estados Unidos, baseia-se na auto-regulamentação. As políticas de privacidade são definidas pelas próprias corporações comerciais. Cabe às companhias e aos indivíduos decidirem por si mesmos as políticas e diretrizes de privacidade que lhe interessem. A principal crítica feita a esta abordagem é que, em seus termos, os indivíduos acabam ficando numa posição mais fraca.

Conforme uma segunda abordagem, promovida pela União Européia, a proteção da privacidade deve ser garantida pelas autoridades públicas. Esta abordagem, promovida pela Diretiva Européia de 1995 sobre Proteção de Dados (95/46/EC), cobre a proteção de indivíduos quanto ao processamento de dados pessoais e a livre movimentação de tais dados. Além da Diretiva Européia, que é o principal mecanismo, a abordagem européia da questão da privacidade e da proteção de dados também é constituída por outros instrumentos regionais, como a Convenção do Conselho da Europa sobre a Proteção de Indivíduos em relação a Processamento Automático de Dados Pessoais (1981).

Essas duas abordagens – EEUU e UE – da privacidade e da proteção de dados começaram a entrar em conflito. Os principais problemas decorrem do uso de dados pessoais por companhias comerciais. Como pode a União Européia impor a sua regulamentação, por exemplo, a uma fabricante de programas baseada nos Estados Unidos? Como pode a UE garantir que os dados sobre seus cidadãos estejam protegidos segundo as regras especificadas na sua Diretiva sobre Proteção de Dados? Segundo que regras (estadunidenses ou união-européias) os dados transferidos da rede de uma companhia união-européia para uma companhia estadunidense serão manuseados? A UE ameaçou bloquear a transferência de dados para qualquer país que não fosse capaz de garantir o mesmo nível de privacidade discriminado na sua diretiva. Esta exigência levou inevitavelmente a um choque com a abordagem de auto-regulamentação dos Estados Unidos.

Esta divergência profunda tornou qualquer possível acordo mais difícil de alcançar. Além disso, ajustar as leis dos Estados Unidos à diretiva da União Européia não teria mesmo sido possível, pois exigiria mudar alguns princípios importantes do sistema legal estadunidense. A ruptura do cerco se deu quando o embaixador norte-americano sugeriu a fórmula do "Porto Seguro". A proposta reformulou toda a questão e propiciou uma saída para o impasse nas negociações.

Alcançou-se uma solução em cujos termos a regulamentação da União Européia podia ser aplicada a empresas estadunidenses que aceitassem situar-se dentro de um "porto seguro" legal. As empresas estaduniden-ses que manuseassem dados sobre cidadãos união-europeus poderiam assinar voluntariamente um compromisso de observância das exigências de proteção à privacidade da União Européia. Tendo assinado, elas eram obrigadas a observar os mecanismos formais de execução acordados entre a UE e os EEUU.

As visões conflitantes sobre proteção à privacidade eletrônica da União Européia e dos Estados Unidos confirmaram que a interdependência crescente engendrada pelo comércio eletrônico pode pôr em questão alguns princípios básicos, ancorados nas respectivas histórias sociais e culturais. A globalização fará esta questão surgir e ressurgir à medida da participação de outras sociedades. O "Acordo Porto Seguro" deve ser visto como um precedente valioso e uma ferramenta útil para a formulação de compromissos semelhantes entre a União Européia e outros países, inclusive o Canadá e a Austrália.

SEÇÃO 4

A cesta econômica

A CESTA ECONÔMICA

A importância do aspecto econômico da Governança da Internet é ilustrado pelo título do documento que deu início à reforma da Governança da Internet e fundou a ICANN: "Estrutura para a Administração do Comércio Eletrônico Global" (1997). O documento afirma que "o setor privado deve conduzir" o processo da Governança da Internet, e que a principal função desta governança será "executar a observância de um ambiente legal previsível, minimalista, coerente e simples para o comércio eletrônico." Esses princípios são o alicerce do regime da Internet baseado na ICANN.

Vários mecanismos políticos e reguladores de grande importância para o e-comércio estão classificados em outras cestas.

A cesta da infra-estrutura e da padronização

- A introdução do acesso *banda larga* e da *qualidade de serviço* é uma pré-condição para o crescimento mais rápido do comércio eletrônico no campo da multimídia (e.g. na distribuição de filmes e canções).
- A *segurança na Internet* deve incrementar a confiabilidade e a robustez do ambiente do comércio eletrônico. Ela também deve ajudar a fortalecer a confiança dos clientes no e-comércio.
- A *criptografia* é crucial para a proteção das comunicações, especialmente das transações financeiras.

A cesta legal

- A questão da *jurisdição* é importante para a confiabilidade do e-comércio, em particular para a proteção do consumidor.
- A importância dos *direitos de propriedade intelectual* para o comércio eletrônico está vinculada ao aumento do volume de transações e-comerciais de produtos intangíveis.
- A *assinatura digital* facilita as transações *online* e resolve o problema da autenticação..
- Com o aumento da coleta e da reunião de informações pelo comércio eletrônico, a *proteção de dados* representa uma garantia essencial para a privacidade pessoal.

COMÉRCIO ELETRÔNICO

A escolha de uma definição para comércio eletrônico tem muitas implicações práticas e legais. Dependendo da classificação de uma determinada transação como e-comércio, regras específicas são aplicadas, como, por exemplo, as que regulamentam as práticas fiscais e alfandegárias.

Para o governo dos Estados Unidos, o elemento-chave a distinguir o comércio tradicional do e-comércio é o "o compromisso *online* de vender bens ou serviços". Isto significa que qualquer transação comercial fechada *online* deve ser considerada comércio eletrônico, mesmo que a realização do negócio envolva a entrega física do produto. Por exemplo, comprar um livro através da Amazom.com é considerado como operação e-comercial, apesar de o livro ser entregue via correio tradicional. A OMC define o comércio eletrônico mais precisamente: É "a produção, distribuição, marketing, venda ou entrega de bens e serviços por meios eletrônicos."

O comércio eletrônico toma muitas formas:

- empresas com consumidor (B2C) – o tipo mais conhecido de e-comércio (e.g. Amazom.com);
- empresas com empresas (B2B) – o mais intensivo economicamente. Em 2001, o volume de transações B2B nos Estados Unidos foi de 995 bilhões de dólares, o que representa 93,3% de todas as transações e-comerciais;
- empresas com governos (B2G) – muito importante na área dos mercados públicos;
- consumidor com consumidor (C2C) – por exemplo, leilões do tipo e-Bay.

Muitos países vêm desenvolvendo um ambiente regulador para o e-comércio. Leis têm sido adotadas nos campos da assinatura digital, da resolução de disputas, do cibercrime, da proteção ao consumidor e no campo fiscal. No âmbito internacional, um número crescente de iniciativas e regimes dizem respeito ao comércio eletrônico.

A OMC E O COMÉRCIO ELETRÔNICO

Ator político chave no comércio global contemporâneo, a Organização Mundial do Comércio (OMC) regulamenta muitas questões relevantes de e-comércio, inclusive a liberalização das telecomunicações, os direitos de propriedade intelectual e alguns aspectos do desenvolvimento das TICs. A OMC intervém diretamente no comércio eletrônico através das seguintes iniciativas:

- Uma moratória temporária dos direitos alfandegários impostos sobre transações eletrônicas, introduzida em 1998. Em escala global, a iniciativa isentou todas as transações e-comerciais de cobrança de impostos alfandegários.
- O estabelecimento do Programa de Trabalho sobre Comércio Eletrônico da OMC, que promove discussões sobre o comércio *online*.

Apesar de o comércio eletrônico ter estado em segundo plano na ordem do dia da diplomacia da OMC, várias iniciativas surgiram e algumas questões-chave foram identificadas. Duas delas serão mencionadas a seguir.

Devem as transações do comércio eletrônico ser classificadas como *serviço* (regulamentadas, portanto, pelo Acordo Geral sobre o Comércio de Serviços – GATS) ou como *bem* (regulamentadas pelo Acordo Geral sobre Tarifas e Comércio – GATT)?

Alterar-se-ia a classificação de música como bem ou serviço em função de o produto ser entregue em CD (bem tangível) ou via Internet (bem intangível)? Em última análise, a mesma canção pode ter diferentes *status* comerciais em função do meio como é entregue (podendo, portanto, ser objeto de diferentes direitos alfandegários e impostos). A questão da classificação tem implicações consideráveis por causa dos mecanismos reguladores diferentes existentes para bens e serviços.

Qual deve ser a ligação entre os Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio (ADPCI/TRIPS) e a proteção dos Direitos de Propriedade Intelectual (DPIs) na Internet?

Como o sistema ADCPI/TRIPS propicia um mecanismo de execução muito mais forte para os DPIs, os países desenvolvidos têm tentado estender a sua cobertura ao comércio eletrônico e à Internet mediante duas abordagens. Em primeiro, evocando o princípio da "neutralidade tecnológica", eles têm argumentado que os ADCPI, como outras regras da OMC, devem ser estendidos a todos os meios de telecomunicação, inclusive a Internet. Em segundo, alguns países desenvolvidos têm

reivindicado uma integração maior dos "tratados digitais" da Organização Mundial da Propriedade Intelectual (OMPI) no sistema ADCPI. Os ADCPIs provêm mecanismos de execução mais fortes do que as convenções da OMPI. Ambas as questões restam em aberto e se tornarão cada vez mais importantes no futuro das negociações da OMC.

Não é muito provável que o comércio eletrônico venha a receber, na fase em curso das negociações comerciais, uma atenção destacada na agenda da OMC. A ausência de arranjos e-comerciais será em parte coberta por algumas iniciativas específicas (atinentes, por exemplo, a contratos e assinaturas) e vários acordos regionais, principalmente nas regiões da União Européia e da Ásia-Pacífico.

OUTRAS INICIATIVAS INTERNACIONAIS EM MATÉRIA DE COMÉRCIO ELETRÔNICO

Uma das iniciativas internacionais mais bem-sucedidas e amplamente apoiadas no campo do e-comércio é a Lei Modelo sobre Comércio Eletrônico da UNCITRAL. O foco da Lei Modelo incide sobre os mecanismos de integração do comércio eletrônico no direito comercial tradicional (e.g. reconhecer a validade dos documentos eletrônicos). A Lei Modelo tem sido usada em muitos países como base peara a regulamentação do e-comércio.

Outra iniciativa projetada a desenvolver o e-comércio é a introdução do ebXML pelo Centro das Nações Unidas para a Facilitação do Comércio e dos Negócios Eletrônicos (UN/CEFAT). Na verdade, o ebXML pode rapidamente tornar-se o principal padrão de intercâmbio de documentos do comércio eletrônico, substituindo o atual – Intercâmbio Eletrônico de Dados (EDI).

As atividades da OCDE interferem em vários aspectos que dizem respeito ao comércio eletrônico, inclusive proteção ao consumidor e assinaturas digitais. A entidade enfatiza a promoção e a pesquisa referentes ao e-comércio através de recomendações e diretrizes. Outras organizações internacionais, como a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD) e a Força Tarefa da ONU sobre TIC, também implementam várias iniciativas de pesquisa e de construção de capacidades na área do comércio eletrônico.

No setor empresarial, as organizações mais ativas são a Câmara de Comércio Internacional, que produz uma ampla gama de recomendações e análises no campo do comércio eletrônico, e a Global Business Dialogue (Diálogo Comercial Global), que promove o comércio eletrônico tanto no contexto internacional como no nacional.

INICIATIVAS REGIONAIS

A União Européia desenvolveu uma estratégia de comércio eletrônico na assim chamada "Cúpula Ponto Com" dos líderes união-europeus em Lisboa, em março do ano 2000. Embora abrangesse uma abordagem privada e orientada para o mercado do comércio eletrônico, a UE também introduziu algumas medidas corretivas voltadas para a proteção dos interesses públicos e sociais (e.g. promoção de acesso universal, política de competição levando em consideração o interesse público, e restrições à distribuição de conteúdos nocivos). A União Européia adotou a Diretiva sobre Comércio Eletrônico, assim como um conjunto de outras diretivas relacionadas às questões de assinaturas eletrônicas, proteção de dados e transações financeiras eletrônicas.

A região da Ásia-Pacífico, o ponto central da cooperação e-comercial é a Cooperação Econômica Ásia-Pacífico (CEAP). A CEAP estabeleceu o Grupo Diretor sobre Comércio Eletrônico, que lida com várias questões do e-comércio, inclusive a proteção ao consumidor, aos dados, *spam* e cibersegurança. A última e mais destacada iniciativa da CEAP é o Plano de Ação Individual para o Comércio sem Papéis, que objetiva criar um comércio de bens inteiramente sem papéis na região até 2010.

PROTEÇÃO AO CONSUMIDOR

A confiança do consumidor é uma das principais pré-condições para o sucesso do comércio eletrônico. O e-comércio ainda é relativamente novo e os consumidores não têm tanta confiança nele quanto nas compras no "mundo real". A proteção ao consumidor é, portanto, um importante método legal para desenvolver a confiança no comércio eletrônico.

A regulamentação do e-comércio deve proteger os consumidores num certo número de áreas: o manuseio *online* das informações contidas em cartões de pagamento, propaganda enganosa, e entrega de produtos defeituosos. Uma nova idiossincrasia do e-comércio é a internacionalização da proteção ao consumidor, internacionalização esta que não é uma questão importante para o comércio ordinário.

No passado, os consumidores raramente tinham necessidade de proteção internacional. Com o e-comércio, um número crescente de transações ocorre através de fronteiras internacionais.

A jurisdição é uma questão importante para a proteção ao consumidor. Ela envolve duas abordagens principais. A primeira favorece o vendedor (principalmente o e-comércio) e corresponde a uma abordagem "país-de-origem/prescrita-pelo-vendedor". Neste cenário, as empresas de comércio eletrônico têm a vantagem de poder confiar num ambiente legal previsível e bem conhecido. A outra abordagem, que favorece o consumidor, é uma abordagem "país-destino". A principal desvantagem dessa abordagem para o comércio eletrônico é o seu potencial de produzir exposição a uma ampla variedade de jurisdições legais. Uma solução possível para este dilema seria intensificar a harmonia entre as regras existentes de proteção ao consumidor, tornando a questão das jurisdições menos relevante.

Como com outras questões relativas ao comércio eletrônico, a OCDE assumiu um papel de liderança ao adotar as Diretrizes para a Proteção do Consumidor no Contexto do Comércio Eletrônico (2000) e as Diretrizes para a Proteção do Consumidor contra Práticas Comerciais Transfronteiriças Fraudulentas e Enganosas (2003). A OCDE estabeleceu os princípios essenciais, agora adotados por algumas associações comerciais, inclusive a Câmara do Comércio e o Council of Better Business Bureaus (Conselho dos Birôs de Ética nos Negócios).

A União Européia oferece um alto nível de proteção ao consumidor do comércio eletrônico. Por exemplo, o problema das jurisdições foi resolvido através da Convenção de Bruxelas, que estipula que os consumidores terão sempre recurso a proteções legais locais.

No âmbito global, nenhum instrumento legal internacional adequado foi implantado. Um dos mais aptos entre eles, a Convenção da ONU sobre Contratos para a Venda Internacional de Bens, de 1980, não aborda contratos firmados diretamente com consumidores e tampouco a questão da proteção ao consumidor.

O desenvolvimento futuro do e-comércio exigirá ou bem a harmonização das leis nacionais ou então um novo regime internacional para a proteção ao consumidor do comércio eletrônico.

IMPOSTOS

O dilema da Governança da Internet quanto a saber se as questões ligadas ao ciberespaço devem ou não ser tratadas diferentemente das questões do "mundo real" tem se espelhado claramente no tópico dos impostos. Desde os primeiros dias, os Estados Unidos têm tentado fazer da Internet uma zona livre de impostos. Em 1998, o congresso estadunidense aprovou a Lei da Isenção Fiscal. A OCDE e a União Européia têm promovido a visão oposta, de que a Internet não deve ter um tratamento fiscal especial. Os Princípios de Ottawa da OCDE especificam que não existe nenhuma diferença entre o fisco tradicional e o fisco eletrônico, e que, portanto, nenhuma regulamentação especial é exigida. Nos Estados Unidos, muitos estados argumentam nesta mesma direção, exigindo a taxação das transações na Internet.

Outra questão fiscal do comércio eletrônico que permanece em aberto entre a UE e os EEUU é a da definição de onde deve incidir o imposto. Os princípios de Ottawa introduziram a noção de taxação "no destino" em vez de "na origem". Os Estados Unidos têm muito interesse em que as transações permaneçam taxadas na origem, considerando que a maioria das companhias de comércio eletrônico lá estão baseadas. Em contraste, o interesse da União Européia na "taxação no destino" inspira-se amplamente no fato de o comércio eletrônico união-europeu ter mais consumidores do que vendedores.

ALFÂNDEGA

O serviço alfandegário é diretamente afetado pelo e-comércio. A transação de bens digitais através de fronteiras internacionais não pode ser controlada da mesma maneira que as transações de bens materiais. É difícil, senão impossível, identificar pacotes de Internet que contenham produtos sobre os quais incidam taxas. Isto abre muitas questões sobre a aplicabilidade do conceito vigente de controle alfandegário, e aponta para a introdução de novos procedimentos.

No plano das políticas e diretrizes, a principal iniciativa é da OMC, a moratória das tarifas sobre transmissões do comércio eletrônico, de 1998. A última extensão explícita da moratória foi implementada em Doha em 2001. Devido ao fracasso das negociações da OMC em Cancun em 2003, a questão não foi discutida oficialmente, o que deixou muito espaço para diferentes interpretações sobre estar ou não ainda em vigência a moratória alfandegária global. Na prática, isto não faz muita diferença, pois dadas as dificuldades para inspecionar os bens e serviços entregues via Internet, a imposição de taxas alfandegárias é quase impossível.

PAGAMENTOS ELETRÔNICOS: BANCO ELETRÔNICO E DINHEIRO ELETRÔNICO

Pode-se definir a noção de pagamento eletrônico como a conclusão de transações financeiras nos marcos de um ambiente *online*, através do uso de vários instrumentos de pagamento *online*. A existência de um sistema de pagamentos eletrônico é uma pré-condição para o desenvolvimento bem-sucedido do comércio eletrônico. O campo dos pagamentos eletrônicos postula a necessidade de fazer uma distinção entre banco eletrônico e dinheiro eletrônico.

A noção de "banco eletrônico" envolve o uso de um computador e da Internet para a realização de operações bancárias tradicionais, como pagamentos de cartões ou transferências de valores. A novidade está apenas no meio, ao passo que o serviço bancário resta essencialmente o mesmo. O banco eletrônico oferece vantagens aos consumidores e reduz o custo das transações. Em termos de governança, a noção não coloca problemas além dos já mencionados, como a proteção do cliente no âmbito internacional, por exemplo.

A noção de "dinheiro eletrônico", por outro lado, introduz uma inovação considerável. O Federal Reserve Board, que é um equivalente aproximado do Banco Central no Brasil, define dinheiro eletrônico como "o dinheiro que circula eletronicamente". O dinheiro eletrônico é geralmente associado aos chamados "cartões inteligentes" emitidos por empresas como Mondex, Visa Cash e CyberCash. Todo dinheiro eletrônico reúne as seguintes características:

- É estocado eletronicamente, tipicamente num cartão com um microprocessador.
- É transferido eletronicamente. Na maioria dos casos, a transferência ocorre entre consumidores e comerciantes. Ocasionalmente, é possível realizar transferências entre particulares.
- As transações com dinheiro eletrônico envolvem um sistema complexo, abrangendo o emissor do valor do dinheiro eletrônico, os operadores de rede, e o compensador das transações com dinheiro eletrônico.

Até o momento, o dinheiro eletrônico ainda está em seus primeiros estágios de desenvolvimento. Ele ainda não é usado amplamente por causa das suas limitações em matéria de segurança e de privacidade. O uso do dinheiro eletrônico pode evoluir em duas direções diferentes:

A primeira seria uma perspectiva evolutiva abrangendo métodos mais sofisticados de transação eletrônica, inclusive o desenvolvimento de micropagamentos eficientes. Finalmente, todas as transações deste tipo seriam ancoradas nos sistemas bancário e monetário existentes.

A segunda seria um desenvolvimento de tipo revolucionário, tirando o dinheiro eletrônico do controle dos bancos centrais. O Banco Internacional de Compensações (BIS) já identificou a diminuição do controle do fluxo de capitais e da massa monetária como riscos associados ao dinheiro eletrônico. Conceitualmente, a emissão de dinheiro eletrônico seria semelhante a imprimir moeda sem controle de uma instituição bancária central. Tal abordagem autorizaria empresas privadas a emitirem dinheiro para o comércio eletrônico. Como disse um eminente banqueiro, seria um quadro em que "os sucessores de Bill Gates teriam levado os sucessores de Alan Greenspan à falência." Um tal desenvolvimento teria implicações consideráveis para o futuro do Estado e das relações internacionais; como observou o mesmo banqueiro: "As sociedades já se viraram sem bancos centrais no passado. Elas bem podem fazer o mesmo no futuro." Outras possibilidades de uso do dinheiro eletrônico restam especulativas.

QUESTÕES

1. A continuação do uso do banco eletrônico e do dinheiro eletrônico pode acarretar *mudanças no sistema bancário mundial*, criando possibilidades adicionais para os clientes e ao mesmo tempo reduzindo as tarifas bancárias. Os bancos físicos, de tijolo e cimento, serão seriamente ameaçados pelos bancos virtuais, que têm uma melhor razão de custo-efetividade.

2. Estudos sobre o comércio eletrônico listam a carência de métodos de pagamento (e.g. de cartões) como a terceira razão, depois da segurança e da privacidade, para a não utilização do e-comércio. Hoje em dia, é praticamente impossível realizar operações de e-comércio sem cartões de crédito. Este é um obstáculo significativo para aqueles países em desenvolvimento que não desenvolveram um mercado de cartões de crédito. Os governos desses países teriam de aprovar as mudanças legais necessárias para viabilizar a introdução mais rápida de cartões de pagamento.

3. Para fomentar o desenvolvimento do comércio eletrônico, os governos em todo o mundo precisarão estimular todas as *formas de pagamento sem dinheiro sonante*, inclusive cartões de crédito e dinheiro eletrônico. Para introduzir o dinheiro eletrônico mais rapidamente, os governos precisarão incrementar ações regularizadoras adicionais. Depois de Hong Kong, o primeiro país a introduzir uma legislação abrangente sobre dinheiro eletrônico, a União Européia adotou a Diretiva sobre Dinheiro Eletrônico, no ano 2000.

   Os governos estão relutantes em introduzir o dinheiro eletrônico por causa dos riscos potenciais implicados para as autoridades dos bancos centrais. Opiniões como as do economista David Saxton representam uma séria advertência neste sentido: "O dinheiro digital é uma ameaça séria para todos os governos deste planeta que desejam gerir a sua própria moeda." Os governos também se preocupam com o uso eventual do dinheiro eletrônico para lavagem de dinheiro.

4. Alguns analistas acreditam que a expansão real do comércio eletrônico está ligada à introdução de *serviços efetivos e confiáveis* para pequenas transações. Por exemplo, os usuários da Internet ainda relutam em usar seus cartões de crédito para pequenos pagamentos, de poucos euros/dólares/reais, já que em geral incide uma cobrança adicional para o acesso aos artigos e serviços na Internet. Um sistema baseado em micropagamentos em dinheiro eletrônico pode propiciar a solução necessária. O consórcio W3C, principal organismo internacional de padronização/normalização da Internet, está hoje envolvido na criação de padrões para sistemas de micropagamentos.

5. Devido à natureza da Internet, é provável que o dinheiro eletrônico venha a tornar-se global – o que justifica *lidar com esta questão no âmbito internacional*. Um ator potencial no campo dos bancos eletrônicos é o Grupo de Banco Eletrônico do Comitê da Basiléia. Este grupo já começou a tratar de temas como autorização, normas de prudência, transparência, privacidade, lavagem de dinheiro e supervisão transfronteiriça, questões-chave para a introdução do dinheiro eletrônico.

6. Várias formas de pagamento eletrônico têm sido desenvolvidas, principalmente no seio das economias avançadas. Pagamentos eletrônicos requerem um ambiente legal estável, seguro e funcional. Não obstante, *a maioria dos países avançados ainda são economias baseadas no dinheiro sonante*. Nos casos em que o uso de cartões é permitido, o sistema depende do uso de assinaturas. Esta imensa discrepância também afeta o desenvolvimento do comércio eletrônico e amplia a cisão digital existente entre o Norte rico e o Sul pobre. Ao contrário de medidas como a compra de equipamentos, a introdução de pagamentos eletrônicos exige a implementação gradual de muitos arranjos institucionais e técnicos. A confiança do consumidor é um elemento essencial tanto para o comércio como para os pagamentos eletrônicos em geral, e não pode ser adquirida rápida ou apressadamente.

7. A recente solicitação do procurador geral do estado de Nova Iorque à Paypal e ao Citibank para que não executem pagamentos a cassinos da Internet *vincula diretamente as noções de pagamento eletrônico e de execução da lei*. Aquilo que os poderes públicos encarregados da execução da lei não conseguiram executar através de mecanismos legais, eles obtiveram através de um controle de pagamentos eletrônicos.

SEÇÃO 5

A cesta do desenvolvimento

A CESTA DO DESENVOLVIMENTO

A tecnologia jamais é neutra. A história das sociedades humanas nos dá muitos exemplos da tecnologia conferindo poder a alguns indivíduos, grupos ou nações, ao mesmo tempo em que excluía outros. E a Internet não é diferente. Desde o âmbito individual até o global, uma mudança profunda ocorreu na distribuição de riqueza e de poder. O impacto das TICs na distribuição de poder e do desenvolvimento suscitou muitas perguntas:

- Como as mudanças aceleradas pelas TICs afetou a cisão já existente entre o Norte e o Sul? Irão as TICs reduzir ou aprofundar esta cisão?
- Como e quando as nações em desenvolvimento poderão alcançar os níveis de TICs dos países industrialmente desenvolvidos?

A resposta a estas e a outras perguntas exige uma análise da relevância do desenvolvimento dentro do contexto da Governança da Internet.

Quase todas as questões relativas à Governança da Internet têm um aspecto desenvolvimental. Por exemplo:

- a existência de uma infra-estrutura de telecomunicações, primeira pré-condição para superar a cisão digital;
- o modelo econômico corrente para o acesso à Internet, que impõe um fardo desproporcional aos países em desenvolvimento, que têm de financiar o acesso às espinhas dorsais situadas nos países desenvolvidos;
- *spam*, com impacto negativo comparativamente maior sobre os países em desenvolvimento, devido à sua largura de banda limitada e à sua carência de capacidades para remediar o problema;
- a regulamentação global dos DPIs, que afeta diretamente o desenvolvimento, em função da oportunidade reduzida dos países em desenvolvimento de ter acesso a conhecimentos e informações *online*.

O aspecto desenvolvimental da Cúpula Mundial sobre a Sociedade de Informação (CMSI) foi freqüentemente reiterado, a começar pela própria Resolução da Assembléia Geral das Nações Unidas sobre a CMSI, a qual salientou que a Cúpula devia "promover o desenvolvimento, particularmente no que diz respeito ao acesso e à transferência de tecnologia." A Declaração de Genebra da CMSI e seu Plano de Ação destacam o desenvolvimento como prioridade e o vinculam à promoção, pela Resolução do Milênio, do "acesso de todos os países à informação, ao conhecimento e à comunicação de tecnologias para o desenvolvimento."

Estabelecido deste modo o vínculo com os Objetivos do Milênio, a CMSI assume uma posição forte no contexto do desenvolvimento.

Este capítulo só tratará das questões centrais do desenvolvimento, como a cisão digital e o acesso universal, freqüentemente levantadas no debate. Esta explanação será seguida por uma análise dos principais fatores a influenciar a Internet e o desenvolvimento: infra-estrutura, assistência financeira, questões relativas a políticas e diretrizes, e aspectos socioculturais.

Como as TICs afetam o desenvolvimento da sociedade?

Os dilemas essenciais sobre TICs e desenvolvimento foram resumidos num artigo recente no *The Economist* ("Falling through the Net?" [Dando em nada com a Rede?], de 21 de setembro de 2000). O artigo propõe argumentos pró e contra a tese de que as TICs dão um impulso específico ao desenvolvimento.

As TICs *não facilitam* o desenvolvimento	**As TICs *facilitam* o desenvolvimento**
• "Fatores externos à Rede" ajudam os primeiros a chegar a estabelecer uma posição dominante. Isto favorece as gigantes americanas, fazendo com que as empresas locais das economias emergentes se vejam de fato excluídas do comércio eletrônico. • A transferência de poder do vendedor ao comprador (a Internet dá origem inevitavelmente a um cenário "um fornecedor alternativo nunca está a mais de um *clic* de distância") prejudicará os países mais pobres. Ela prejudicará os produtores de matérias-primas, essencialmente dos países em desenvolvimento. • Os juros maiores dos títulos de alta tecnologia nas economias ricas reduzirá o interesse dos investidores pelos países em desenvolvimento.	• As TICs baixam o custo da mão-de-obra; é mais barato investir nos países em desenvolvimento. • Comparada com tecnologias anteriores, a difusão das TICs através das fronteiras nacionais é muito rápida. As tecnologias anteriores (ferrovia e eletricidade) levaram décadas para disseminarem-se nos países em desenvolvimento, mas o avanço das TICs se dá aos saltos. • A oportunidade de saltar etapas de tecnologias anteriores, evitando estágios intermediários, como fios de cobre e telefones analógicos, estimula o desenvolvimento. • A tendência inerente às TICs de reduzir o tamanho ótimo da empresa na maioria das indústrias condiz muito mais com as necessidades dos países desenvolvidos.

A CISÃO DIGITAL

A cisão digital pode ser definida como o fosso existente entre aqueles que, por razões técnicas, políticas, sociais ou econômicas, têm acesso e capacidades para utilizar as TICs e aqueles que não os têm. Várias opiniões têm sido avançadas sobre a dimensão e a relevância da cisão digital.

As cisões digitais existem em diferentes níveis: no interior de países e entre países, entre populações rurais e urbanas, entre velhos e jovens, assim como entre homens e mulheres. Cisões digitais não são fenômenos independentes. Elas refletem desigualdades socioeconômicas mais amplas em termos de educação, assistência médica, capital, moradia, emprego, água potável e alimentação. Isto foi claramente assinalado pela Força-Tarefa da Oportunidade Digital do G8: "Não há nenhuma dicotomia entre a cisão digital e as cisões sociais e econômicas mais amplas que o processo de desenvolvimento deve tratar; a cisão digital deve ser compreendida e tratada no contexto dessas cisões mais amplas."

A cisão digital está aumentando?

Os progressos das TICs deixam o mundo em desenvolvimento para trás numa velocidade muito maior do que os avanços em outros campos (e.g. técnicas agrícolas ou médicas) e, como o mundo desenvolvido dispõe das ferramentas necessárias para usar com sucesso o avanço tecnológico, a cisão digital parece estar em contínuo e rápido aprofundamento. Esta é a opinião freqüentemente expressa em vários documentos de grande autoridade, como o Relatório sobre o Desenvolvimento Humano da PNUD e os Relatórios Mundiais de Emprego da OIT.

Algumas opiniões opostas argumentam que as estatísticas sobre a cisão digital estão freqüentemente equivocadas, e que, na verdade, a cisão digital absolutamente não está aumentando. Segundo esta opinião, o enfoque tradicional sobre o número de computadores, o número de sites na Internet ou a largura de banda disponível deve ser substituído por um foco sobre o impacto mais amplo das TICs sobre as sociedades dos países em desenvolvimento. Os sucessos digitais da Índia e da China são exemplos freqüentemente citados por esta vertente.

ACESSO UNIVERSAL

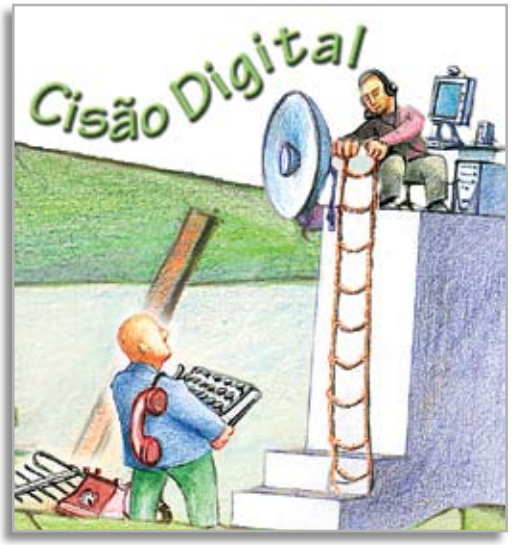
Além da cisão digital, outra noção freqüentemente mencionada no debate sobre o desenvolvimento é o conceito de acesso universal, isto é, de acesso para todos. Embora devesse ser a pedra fundamental de toda e qualquer política de desenvolvimento das TICs, restam percepções e concepções diferentes da natureza e do alcance dessa política de acesso universal. A referência freqüente ao acesso universal nos preâmbulos das declarações internacionais sem indicação das necessárias medidas de apoio político e financeiro o transformam num princípio vago de pouca relevância prática. O problema do acesso universal no âmbito global resta em grande parte uma questão política, dependente em última análise da disposição dos países desenvolvidos de investir na concretização dessa meta.

À diferença do acesso universal no âmbito global, em alguns países o acesso universal é um conceito econômico e legal bem desenvolvido. Prover acesso às telecomunicações a todos os cidadãos tem sido a base da política de telecomunicações dos Estados Unidos. O resultado foi um sistema bem desenvolvido de mecanismos políticos e financeiros cuja proposta é subsidiar custos de acesso em áreas remotas e outras regiões com altos custos de conexão. O subsídio é financiado por regiões em que os custos de conexão são baixos, principalmente as grandes cidades. A União Européia também tomou uma série de medidas concretas a fim de alcançar a meta do acesso universal.

ESTRATÉGIAS PARA SUPERAR A CISÃO DIGITAL

A teoria do desenvolvimento centrado na tecnologia, que tem dominado os círculos políticos e acadêmicos nos últimos 50 anos, argumenta que o desenvolvimento depende da disponibilidade de tecnologias. Quanto mais tecnologia, mais desenvolvimento. Contudo, esta abordagem fracassou em muitos países (principalmente ex-socialistas), onde tornou-se óbvio que o desenvolvimento da sociedade é um processo muito mais complexo. A tecnologia é uma pré-condição necessária mas não

suficiente para o desenvolvimento. Entre outros elementos, estão um quadro regulador, apoio financeiro, disponibilidade de recursos humanos e outras condições socioculturais. Mesmo que todos esses ingredientes estejam presentes, o desafio essencial continua a ser como e quando eles devem ser usados, combinados e colocados em interação.



DESENVOLVER TELECOMUNICAÇÕES E INFRA-ESTRUTURAS DE INTERNET

A possibilidade de implantar conectividade é uma pré-condição para trazer indivíduos e instituições para a Internet e, em última análise, superar a cisão digital. Várias possibilidades de prover ou melhorar a conectividade estão à disposição.

O rápido crescimento da comunicação sem fio dá a muitos países em desenvolvimento uma nova chance. Patrick Gelsinger, da Intel, aconselhou os países em desenvolvimento a dizerem "não" às infra-estruturas à base de fios de cobre e usarem comunicação sem fio como solução para os seus *loops* locais e fibra ótica para as suas espinhas dorsais nacionais. A comunicação sem fio pode ser a solução para os problemas suscitados pelo desenvolvimento de uma infra-estrutura terrestre tradicional de comunicações (deitar cabos sobre distâncias muito longas em numerosos países africanos e asiáticos). Viabiliza-se, deste modo, uma solução para o problema das redes de distribuição ou *loops* locais, um dos obstáculos-chave para o desenvolvimento mais rápido da Internet. Tradicionalmente, o foco central de atenção da União Internacional de Telecomunicações (UIT) tem sido o aspecto infra-estrutural da cisão digital.

APOIO FINANCEIRO

Os países em desenvolvimento recebem apoio financeiro através de vários canais, incluindo agências bilaterais ou multilaterais de desenvolvimento, como o PNUD ou o Banco Mundial, assim como de iniciativas regionais e de bancos de desenvolvimento. Com a liberalização crescente do mercado das telecomunicações, a tendência de desenvolver infra-estruturas de telecomunicações através de investimento estrangeiro direto ganhou força. Muitos países em desenvolvimento lutam continuamente para atrair investimentos privados.

Atualmente, a maior parte das companhias de telecomunicação ocidentais estão em fase de consolidação, depois de terem acumulado imensas dívidas por sobreinvestimento na década de 1990. Embora ainda relutem em investir, espera-se amplamente que a médio prazo elas venham a investir nos países em desenvolvimento, já que o mercado do mundo desenvolvido está supersaturado com as imensas capacidades construídas no final de década de 1990.

A importância do aspecto financeiro foi claramente reconhecida durante a fase de Genebra da CMSI. Uma idéia ali proposta foi o estabelecimento de um Fundo de Solidariedade Digital gerido pela ONU, para ajudar os países em desvantagem tecnológica a construírem infra-estruturas de telecomunicações. O fundo seria mantido por contribuições voluntárias. Alguns propuseram o estabelecimento de um sistema de doação, como por exemplo de um dólar à compra de cada computador pessoal, pacote de programas ou componentes de equipamento de rede. Não obstante, a proposta de instituir um Fundo de Solidariedade não granjeou um apoio amplo dos países desenvolvidos, que preferem o investimento direto ao estabelecimento de um fundo de desenvolvimento centralizado. Em vista de explorar as possibilidades de esquemas de financiamento mais flexíveis e apropriados, acordou-se o estabelecimento de um Grupo de Trabalho sobre Financiamento de Tecnologia de Informação e Comunicações para o Desenvolvimento (ICT4D), o qual prestou contas na CMSI 2005, na Tunísia.

ASPECTOS SOCIOCULTURAIS

O aspecto sociocultural das cisões digitais abrange uma variedade de questões, inclusive alfabetização, qualificação em TICs, treinamento, educação e proteção da língua.

Para os países em desenvolvimento, uma das principais questões tem sido a "fuga de cérebros", descrita como o movimento da mão-de-obra altamente qualificada dos países em desenvolvimento para os países desenvolvidos. Através da fuga de cérebros, os países em desenvolvimento perdem de uma infinidade de maneiras. A principal perda é a da própria mão-de-obra qualificada. Mas os países em desenvolvimento também perdem o investimento que fizeram na formação dessa mão-de-obra. É provável que a fuga de cérebros continue, considerando os vários regimes de emprego e de imigração que foram introduzidos nos Estados Unidos, na Alemanha e em outros países desenvolvidos para atrair mão-de-obra qualificada, principalmente na área das tecnologias de informação e telecomunicação.

Um desenvolvimento que pode parar ou, em alguns casos, até inverter a fuga de cérebros é o aumento da terceirização de tarefas das TICs para os países em desenvolvimento. Os exemplos mais bem-sucedidos foram os centros industriais de *software* desenvolvidos na Índia, como Bangalore.

No âmbito global, a ONU criou a Rede Digital da Diáspora para promover o desenvolvimento da África através da mobilização dos conhecimentos especializados e recursos tecnológicos, empresariais e profissionais das diásporas africanas no campo das TICs.

As iniciativas da UNESCO são particularmente relevantes para o aspecto social da cisão digital. A UNESCO adotou uma convenção sobre a proteção da diversidade cultural e lançou um certo número de projetos voltados para a promoção da diversidade lingüística e cultural na Internet.

POLÍTICA E REGULAMENTAÇÃO DAS TELECOMUNICAÇÕES

O desenvolvimento de políticas de telecomunicações está estreitamente ligado, em muitos aspectos, à superação da cisão digital. Em primeiro lugar, tanto os investidores privados quanto (e cada vez mais) os doadores públicos não se mostram prontos a investir em países que não tenham um ambiente institucional e legal adequado ao desenvolvimento da Internet. Em segundo, o desenvolvimento de setores nacionais na área das TICs depende da criação dos marcos reguladores necessários. Em terceiro, a existência de monopólios nacionais de telecomunicações é geralmente indicada como uma das razões para custos mais elevados de acesso à Internet.

A criação de um ambiente capacitador é uma tarefa exigente, implicando a desmonopolização gradual do mercado de telecomunicações, a introdução de leis relacionadas à Internet (cobrindo direitos autorais, privacidade, comércio eletrônico, etc.) e a garantia de acesso a todos, sem restrições políticas, religiosas ou outras.

O debate acerca do impacto da liberalização do mercado das telecomunicações sobre o desenvolvimento gira em torno de dois pontos de vista dominantes. O primeiro é que a liberalização não beneficiou os países em desenvolvimento. Com a perda dos monopólios de telecomunicação, governos do mundo em desenvolvimento teriam perdido uma fonte importante de arrecadação de receitas. A entrada de menos receitas teria afetado todos os demais setores da vida social e econômica. Segundo esta opinião, os perdedores são os governos dos países em desenvolvimento e os ganhadores são as companhias de telecomunicações do mundo desenvolvido. O segundo ponto de vista mencionado é que a abertura dos mercados de telecomunicações teria gerado mais competição, levando a uma elevação da qualidade dos serviços e a custos mais baixos. Em última análise, uma pré-condição para o desenvolvimento da sociedade como um todo.

SEÇÃO 6

A cesta sociocultural

A CESTA SOCIOCULTURAL

Redes conectando computadores já existiam antes da Internet. O que torna a Internet diferente é a facilitação que ela propicia a várias formas de comunicação e de criatividade humanas. As inovações mais importantes são associadas às maneiras como a Internet foi usada para novos modos de comunicação (*e-mail*, a Rede mundial, multimídia). Neste contexto, alguns autores argumentam que a Internet seja mais um fenômeno social do que tecnológico. Ela suplementa as comunicações tradicionais assim como fornece novas formas de comunicação que lhe são próprias (e.g. as cibercomunidades). Tais desenvolvimentos engendraram a dimensão sociocultural da Internet. A cesta sociocultural inclui algumas das questões mais controversas em todo o campo da Governança da Internet, como políticas de conteúdo e multilingüismo. Estas questões refletem de modo muito particular as diferenças nacionais, religiosas e culturais hoje prevalecentes.

POLÍTICAS DE CONTEÚDO

Uma das principais questões socioculturais são as políticas de conteúdo, freqüentemente abordadas a partir do ponto de vista dos direitos humanos (liberdade de expressão e direito de comunicar), de governo (controle de conteúdos) e da tecnologia (ferramentas para controle de conteúdos), para mencionar apenas alguns.

A discussão em geral concentra-se em três grupos de conteúdos. O *primeiro grupo* consiste nos conteúdos sobre os quais há um consenso global sobre o seu controle. Nele estão incluídas a pornografia infantil e vários outros tópicos, como a justificação de genocídios e o incitamento ou organização de atos terroristas, práticas proibidas pelo direito internacional (*ius cogens*). Embora tenha se estabelecido um consenso sobre a remoção desses conteúdos da Internet, restam interpretação diferentes. Por exemplo, o que exatamente constitui um ato terrorista?

O *segundo grupo* consiste nos conteúdos que podem ser sensíveis para países, regiões ou grupos étnicos específicos, em função dos seus valores religiosos e culturais particulares. A comunicação globalizada e mais intensiva põe em questão os valores culturais e religiosos locais. A maioria dos processos judiciais concernentes à Internet diz respeito a este grupo de conteúdos. No caso Yahoo!, um tribunal francês solicitou que a Yahoo.com (EEUU) proibisse o acesso de cidadãos franceses a partes de um site que vendia materiais e *memorabilia* nazistas. A Alemanha tem uma jurisprudência muito desenvolvida, com muitos processos contra proprietários de sites que hospedam materiais nazistas. A maior parte dos controles de conteúdos exercidos no Oriente Médio e nos países asiáticos é oficialmente justificada como proteção de valores culturais específicos. Em geral, a proteção em questão envolve bloquear acesso a sites pornográficos ou de apostas.

O *terceiro grupo* consiste nos conteúdos que são política e ideologicamente sensíveis. Em essência, trata-se de exercer censura na Internet. A Transparência Internacional tem relatado um certo número de práticas dessa natureza na China, no Myanma (ex-Birmânia) e na Arábia Saudita.

COMO SÃO CONDUZIDAS AS POLÍTICAS DE CONTEÚDO?

Um cardápio *à la carte* das políticas de conteúdo dispõe das seguintes opções legais e técnicas, usadas em diferentes combinações.

Filtragem pública (governamental) de conteúdos

A filtragem governamental se dá comumente através de um "Índice de Internet" de sites bloqueados para acesso dos cidadãos. Se um site estiver no Índice de Internet, o acesso não será permitido. Tecnicamente falando, a filtragem usa tipicamente o bloqueio de um IP a partir de um roteador, servidores proxy e redirecionamento DNS. A filtragem de conteúdos é praticada em muitos países. Além dos países geralmente associados a essas práticas (China, Arábia Saudita e Cingapura), outros países a praticam cada vez mais. Por exemplo, a Áustria tem um sistema específico para páginas nacionais. Na Alemanha, o estado da Renânia do Norte-Vestfália solicitou aos ISPs a filtragem do acesso principalmente a sites neonazistas, embora não apenas a eles.

Sistemas privados de classificação e filtragem

Face ao risco potencial de desintegração da Internet por causa do desenvolvimento de várias barreiras nacionais (sistemas de filtragem), o W3C e outras instituições com idéias afins sugeriram a implementação de sistemas de classificação e filtragem controlados pelos usuários. Tecnicamente falando, mecanismos de filtragem são parte integrante dos programas de navegação na Internet. A acessibilidade de um conteúdo específico é indicada através de um rótulo que corresponde a um site particular. O uso deste tipo de filtragem foi especialmente aprovado como sistema de acesso exclusivo a site "favoráveis à criança".

Programas de geolocalização

Outra solução técnica relacionada à questão dos conteúdos são os *programas de geolocalização*, que filtram o acesso a conteúdos específicos da Rede segundo a origem geográfica/nacional dos usuários. O caso Yahoo! foi importante quanto a isto, pois o grupo de especialistas envolvidos, incluindo Vint Cerf, indicou que em 90 por cento dos casos o Yahoo! seria capaz de determinar se algum setor dos seus sites hospedados de *memorabilia* nazista estava sendo acessado a partir da França. Esta avaliação tecnológica ajudou o tribunal a chegar à sua decisão final. As empresas fabricantes de programas de geolocalização afirmam que são capazes de identificar o país de origem sem margem de erro, e a cidade em cerca 85 por cento dos casos, especialmente se for uma grande cidade. Os programas de geolocalização podem ajudar os provedores de conteúdo da Internet a filtrar o acesso segundo a localização do usuário e, deste modo, evitar processos em tribunais estrangeiros.

Controle de conteúdos através de motores de busca

Há uma diferença significativa entre disponibilidade e acessibilidade de materiais na Internet. O fato de uma página (ou conteúdo) particular estar disponível na Rede não significa que poderá ser acessada por todos os usuários que quiserem. Por exemplo, se um site específico não puder ser encontrado através do Google, a sua relevância se vê seriamente diminuída. A ponte entre o usuário final e o conteúdo da Rede é geralmente o motor de busca. Divulgou-se amplamente que um dos primeiros exemplos de controle de conteúdo através de motores de busca foi implementado pelas autoridades chinesas em relação ao Google. Se os usuários digitavam uma palavra proibida na pesquisa do Google, o seu IP perdia a conectividade por alguns instantes. O serviço de informação chinês afirmou: "É totalmente normal, com alguns sites da Internet, que às vezes seja possível acessá-lo e às vezes não. O ministério não recebeu nenhuma informação sobre bloqueios no Google."

Para ajustar-se às leis locais, o Google resolveu restringir alguns materiais nos seus sites nacionais. Por exemplo, nas versões alemã e francesa do Google é impossível buscar e encontrar sites com materiais nazistas. Isto indica um certo nível de autocensura da parte do Google, a fim de evitar possíveis processos judiciais.

A necessidade de um quadro legal apropriado

O vácuo legal no campo das políticas de conteúdo, que caracterizou o uso inicial da Internet, permitiu aos governos altos níveis de poder discricionário em termos de controle de conteúdos. Considerando que a política de conteúdos é uma questão sensível para todas as sociedades, impõe-se a necessidade de adotar instrumentos legais. Uma regulamentação nacional no campo das políticas de conteúdo pode facultar melhor proteção aos direitos humanos e dirimir os papéis e responsabilidades às vezes ambíguos dos ISPs, agências de execução legal e outros atores. Nos anos recentes, muitos países introduziram legislações de controle de conteúdos.

Iniciativas internacionais

No âmbito internacional, as principais iniciativas estão vinculadas aos países europeus, que contam com uma legislação forte no campo dos discursos de ódio, inclusive o racismo e o anti-semitismo. As instituições regionais européias têm tentado impor suas regras ao ciberespaço. O instrumento legal mais importante no tratamento da questão dos conteúdos é o Protocolo Adicional à Convenção do Conselho da Europa sobre o Cibercrime. Este protocolo especifica vários tipos de discurso de ódio que deveriam ser proibidos na Internet, incluindo propaganda de caráter racista ou xenófoba, justificação de genocídios e de crimes contra a humanidade.

A Organização para a Segurança e Cooperação na Europa (OSCE) é particularmente ativa neste campo. Em junho de 2003, o Encontro sobre a Liberdade dos Meios de Comunicação e da Internet adotou as Recomendações de Amsterdã sobre Liberdade dos Meios de Comunicação e da Internet. As recomendações promovem a liberdade de expressão e buscam reduzir a censura na Internet. Em junho de 2004, a OSCE organizou a Conferência sobre a Relação entre Propaganda Racista, Xenófoba e Anti-Semita na Internet e Crimes de Ódio (Paris, 16-17 de junho de 2004). A temática central do evento foram os maus usos e abusos potenciais da Internet e da liberdade de expressão. Essas manifestações da OSCE possibilitaram o acesso a um amplo espectro de pontos de vista acadêmicos e políticos sobre esses dois aspectos do controle de conteúdos.

A União Européia tem implementado várias iniciativas no contexto do controle de conteúdos, adotando a Recomendação da Comissão Européia contra o Racismo e a Intolerância na Internet. Num nível mais prático, a União Européia introduziu o Plano de Ação por uma Internet Mais Segura, que contempla os seguintes pontos principais:

- estabelecer uma rede de linhas diretas na Europa para relatar a presença de conteúdos ilegais;
- estimular a auto-regulamentação;
- desenvolver práticas de classificação e filtragem de conteúdos, e testes de desempenho de filtragem;
- desenvolver programas e serviços específicos;
- estimular a consciência de uso seguro da Internet.

QUESTÕES

Controle de conteúdos *versus* liberdade de expressão

Quando falamos de controle de conteúdos, o outro lado da moeda é muito freqüentemente a restrição à liberdade de expressão. Isto é especialmente importante nos Estados Unidos, onde a Primeira Emenda garante ampla liberdade de expressão, até mesmo o direito de publicar materiais nazistas ou outros semelhantes. Alcançar o equilíbrio adequado entre controle de conteúdos e liberdade de expressão constitui um desafio considerável. O objetivo essencial do debate recente sobre a Governança da Internet, em processos judiciais e na atividade legislativa inclusive, tem sido encontrar este equilíbrio.

O congresso dos Estados Unidos tende a um controle mais estreito dos conteúdos, ao passo que a Suprema Corte busca proteger a Primeira Emenda da Constituição estadunidense (sobre a Liberdade de Expressão). O exemplo mais notável desta tensão foi a Lei da Decência nas Comunicações, aprovada no Congresso dos Estados Unidos em 1996, mas declarada inconstitucional pela Suprema Corte, com base em que violava a Primeira Emenda.

A questão da liberdade de expressão determina em grande parte a posição dos Estados Unidos no debate internacional sobre a Governança da Internet. Por exemplo, embora os Estados Unidos tenham assinado a Convenção sobre o Cibercrime, não podem assinar o Protocolo Adicional a esta convenção, que lida com discurso de ódio e controle de conteúdos. A questão da liberdade de

expressão também foi trazida à baila no contexto do caso Yahoo!. Esta é uma fronteira que os Estados Unidos se negam a cruzar nas negociações internacionais.

"Ilegal *offline* – ilegal *online*"

Esta noção traz a discussão sobre conteúdo ao dilema entre mundo "real" e mundo "ciber". As regras existentes sobre conteúdo podem ser implementadas na Internet. Isto é freqüentemente salientado no contexto europeu. A Decisão-Quadro do Conselho da Europa sobre Combate ao Racismo e à Xenofobia indica explicitamente "o que é ilegal *offline* é ilegal *online*". Um dos argumentos da abordagem "ciber" da regulamentação da Internet é que a quantidade (volume de comunicação, número de mensagens) engendra uma diferença qualitativa. Segundo este ponto de vista, o problema dos discursos de ódio não é que nenhuma legislação tenha sido promulgada sobre eles, mas sim que seu volume e disseminação na Internet os tornam um tipo diferente de problema legal. Mais indivíduos são expostos e é difícil impor a observância das leis existentes. Conseqüentemente, a diferença que a Internet suscita relaciona-se principalmente aos problemas de execução legal, não às regras ou leis elas mesmas.

A eficácia do controle de conteúdos

Em discussões sobre políticas e diretrizes para a Internet, um dos argumentos-chave é que a natureza descentralizada da Internet permite contornar a censura. A Internet dispõe de muitas técnicas e tecnologias capazes de propiciar um controle eficaz; tecnicamente falando, porém, os mecanismos de controle podem ser contornados. Em países com controle de conteúdo dirigido pelo governo, usuários tecnicamente talentosos têm encontrado maneiras de contornar os controles. Não obstante, o controle de conteúdos não visa esse pequeno grupo de usuários tecnicamente talentosos; ele visa a população mais ampla. Lessing enuncia este problema de maneira clara: *"A regulamentação não precisa ser absolutamente eficaz para ser suficientemente eficaz."*

Quem deve ser responsável pelas políticas de conteúdo?

Os principais atores na área de políticas de conteúdo são os governos. Os governos prescrevem o que deve e como deve ser controlado. Alguns grupos de usuários individuais, como pais, por exemplo, demonstram grande interesse em introduzir políticas de conteúdo mais eficazes para proteger seus filhos. Várias iniciativas de classificação visam ajudar os pais a filtrar conteúdos favoráveis à criança. Políticas de conteúdo também são desempenhadas por empresas privadas e universidades para restringir o acesso a alguns materiais. Em alguns casos, conteúdos são controlados por pacotes de programas; por exemplo, o movimento da Cientologia distribuiu um pacote de programas entre os seus seguidores, o Scienositter, que limita o acesso a sites na Internet críticos à Cientologia.

Uma iniciativa inovadora é a Internet Watch Foundation (Fundação Observatório da Internet), no Reino Unido, cuja meta é combater o abuso contra crianças na Internet. A fundação é uma iniciativa multipartite implementada pelo governo, por provedores de serviço da Internet e representantes de usuários.

DIREITOS HUMANOS

A Internet introduziu novas formas de comunicação e interação na sociedade e em última instância influenciou os conceitos tradicionais de direitos humanos. O conjunto básico de direitos humanos relacionados à Internet inclui privacidade, liberdade de expressão, o direito de receber informações, vários direitos protetores da diversidade cultural, lingüística e das minorias, e o direito à educação. Durante a fase da CMSI, muitos grupos da sociedade civil propuseram a introdução do direito de comunicar, que vai além dos direitos relacionados à Internet existentes.

Os direitos humanos existentes que não foram cobertos em outras partes desta brochura serão brevemente examinados aqui.

A liberdade de expressão e o direito de procurar, receber e transmitir informações

Este é um dos direitos humanos fundamentais, que geralmente aparece no centro das discussões sobre políticas de conteúdo e censura. Na Declaração dos Direitos Humanos da ONU, a liberdade de expressão é contrabalançada pelo direito do Estado de limitar a liberdade de expressão em nome da moralidade, da ordem pública e do bem-estar geral (Artigo 29).

Assim, tanto a discussão como a implementação do Artigo 19, que garante a liberdade de opinião e de expressão, devem ser postas no contexto do estabelecimento de um equilíbrio adequado entre as duas necessidades. Este regime ambíguo abre muitas possibilidades de interpretações diferentes das normas e, em última análise, de diferentes implementações.

O direito à privacidade

O direito à privacidade é discutido na Cesta Legal (p. 73).

Direitos de Propriedade Intelectual

Os direitos de propriedade intelectual habilitam toda pessoa a desfrutar da proteção dos interesses morais e materiais resultantes de sua produção científica, literária ou artística. Este direito é contrabalançado pelo direito de todos de participar livremente na vida cultural e de compartilhar os avanços científicos. Estabelecer um equilíbrio entre essas duas reivindicações é um dos maiores desafios da Governança da Internet.

MULTILINGÜISMO E DIVERSIDADE CULTURAL

Desde os seus primeiros dias, a Internet tem sido um meio predominantemente anglófono. Segundo algumas estatísticas, aproximadamente 80 por cento do conteúdo da Internet está em inglês. Esta situação incitou muitos países a tomar iniciativas em concerto de promoção do multilingüismo e de proteção à diversidade cultural. A promoção do multilingüismo não é apenas uma questão cultural, pois está diretamente ligada à necessidade de desenvolvimentos suplementares da Internet. Para que a Internet seja acessível a setores mais amplos da sociedade e não apenas às elites nacionais, seus conteúdos têm de ser acessíveis a mais línguas.

QUESTÕES

Em primeiro lugar, a promoção do multilingüismo exige a implantação de padrões técnicos que facilitem o uso de alfabetos não românicos. Uma das primeiras iniciativas relacionadas ao uso multilíngüe de computadores foi o Unicode. O Consórcio Unicode é uma instituição sem fins lucrativos que desenvolve padrões para facilitar o uso de conjuntos de caracteres para diferentes línguas. Recentemente, a ICANN e a IETF deram um passo importante ao promover nomes de domínio internacionais escritos em chinês, árabe e outros alfabetos não latinos.

Em segundo lugar, muitos esforços foram envidados para desenvolver a tradução de máquina. Dada a sua política de traduzir todas as atividades oficiais nas línguas de todos os Estados membros, a União Européia tem apoiado várias iniciativas de desenvolvimento no campo da tradução de máquina. Apesar de avanços importantes terem sido alcançados, restam limitações.

Em terceiro, a promoção do multilingüismo exige marcos de governança apropriados. O primeiro elemento dos regimes de governança tem sido provido por organizações como a UNESCO. A UNESCO instigou muitas iniciativas centradas na questão do multilingüismo, inclusive a adoção de importantes documentos, como a Declaração Universal sobre a Diversidade Cultural. Outra promotora-chave do multilingüismo é a União Européia, já que ela incorpora o multilingüismo como um dos seus princípios políticos e operacionais fundamentais.

BEM PÚBLICO GLOBAL

O conceito de Bem Público Global pode ser vinculado a muitos aspectos da Governança da Internet. Os vínculos mais diretos encontram-se nas áreas do acesso à infra-estrutura da Internet, da proteção ao conhecimento desenvolvido através da interação na Internet, da proteção às normas ou padrões técnicos, e do acesso à educação *online*.

A infra-estrutura da Internet é predominantemente gerida por empresas privadas. Um dos desafios atuais é a harmonização da propriedade privada da Internet com a sua condição de bem público global. Leis nacionais prevêem a possibilidade de restrições à propriedade privada por certas exigências públicas, inclusive prover direitos iguais a todos os usuários potenciais e não interferir nos conteúdos transportados.

Uma das características essenciais da Internet é que novos conhecimentos e informações são produzidos através da interação mundial dos usuários. Conhecimentos consideráveis foram gerados através de intercâmbios em listas de correio, grupos de discussão e *blogs*. Em muitos casos, nenhum mecanismo internacional está disponível para proteger esses conhecimentos. Deixado num vácuo legal, o conhecimento pode ser transformado em mercadoria e comercializado por particulares. Este viveiro de conhecimentos comuns, uma base importante de criatividade, corre assim o risco de ser esvaziado. Quanto mais a Internet for comercializada, menos espontâneos se tornarão seus intercâmbios. Isto pode levar a uma redução da interatividade criativa. O conceito de bem público global pode prover soluções que também protegeriam o conhecimento comum da Internet para as gerações futuras.

Com relação à normalização ou padronização, esforços quase permanentes têm sido feitos para substituir os padrões públicos por padrões privados e proprietários. Este foi o caso com a Microsoft (através de navegadores e de ASP) e com a Sun Microsystems (através do Java). Os padrões da Internet (principalmente o TCP/IP) são considerados abertos e públicos. O regime da Governança da Internet deve assegurar a proteção dos principais padrões da Internet como bens públicos globais.

Proteger a Internet como bem público global

Algumas soluções baseadas no conceito da Internet como bem público global podem ser desenvolvidas a partir dos conceitos econômicos e legais existentes. Assim, por exemplo, a teoria econômica propõe o apurado conceito de "bem público", que foi estendido ao âmbito internacional como "bem público global". O bem público tem duas propriedades que são cruciais: consumo não concorrencial e caráter não exclusivo. A primeira supõe que o consumo por um indivíduo não se dê em detrimento do consumo por outro; a segunda, que seja difícil, senão impossível, excluir um indivíduo do desfrute do bem. No âmbito global, o Programa das Nações Unidas para o Desenvolvimento (PNUD) introduziu o conceito de bens públicos globais. No direito internacional, uma solução potencial é o conceito de *res communis omnium* (patrimônio comum da humanidade, a ser regulamentado e guardado por todas as nações).

Será importante avaliar qual desses conceitos deve ser aplicado à Internet e com que conseqüências. Muitos concordam que o modelo para o desenvolvimento futuro da Internet vai depender do estabelecimento de um equilíbrio apropriado entre os interesses privados e o interesse público.

EDUCAÇÃO

A Internet abriu novas possibilidades para a educação. Várias iniciativas de "e-educação", "educação *online*" ou "educação à distância" foram introduzidas; sua meta principal é usar a Internet como meio para ministrar cursos. Embora não possa substituir o ensino tradicional, a educação *online* abre novas possibilidades de aprendizado, especialmente quando limitações de tempo e espaço impedem a freqüentação em sala de aulas. Há estimativas que prevêem que o mercado da educação à distância irá crescer até cerca de 10 bilhões de dólares até 2010.

A aprendizagem eletrônica também levou a uma educação transfronteiriça mais intensiva, com estudantes tomando parte em cursos *online* em outros países. Isto introduziu uma dimensão de governança internacional para o setor da educação.

Tradicionalmente, a educação tem sido governada por instituições nacionais. O credenciamento de instituições educacionais, o reconhecimento das qualificações e a controle de qualidade são governados no âmbito nacional. Não obstante, a educação transfronteiriça postula o desenvolvimento de novos regimes de governança. Muitas iniciativas internacionais visam preencher este vazio de governança, especialmente nas áreas de controle de qualidade e de reconhecimento de diplomas acadêmicos.

OMC e educação

Uma questão polêmica nas negociações da OMC é a interpretação dos Artigos 1 (3) (b) e (c) do Acordo Geral sobre Comércio de Serviços, que especifica exceções ao regime de livre comércio para serviços prestados pelo Estado. Segundo uma perspectiva, esposada principalmente pelos Estados Unidos e o Reino Unido, essas exceções devem ser tratadas com certa restrição, permitindo *de facto* o livre comércio na educação superior. Esta opinião é presidida principalmente pelos interesses dos setores educacionais privados dos Estados Unidos e do Reino Unido, que visam a conquista do mercado global de educação, e recebeu oposição de muitos países.

O principal argumento contra este ponto de vista é que, em todos os países, as universidades provêm bens públicos e desempenham uma importante função social e cultural, além da simples transferência de

conhecimentos e de informações. Segundo esta opinião, o mercado livre global na área da educação pode colocar em perigo as universidades dos países pequenos e em desenvolvimento, e levar a um predomínio educacional de instituições estadunidenses e britânicas. Isto reduziria consideravelmente a diversidade cultural e privaria muitas sociedades do papel da universidade como catalisadora do desenvolvimento da cultura nacional. Outra crítica à proposta de livre comércio na educação diz respeito à sua incompatibilidade com a implementação do direito universal à educação.

O debate futuro, que provavelmente terá lugar no contexto da OMC e de outras organizações internacionais, irá centrar-se no dilema da educação como mercadoria ou como bem público. Se a educação for considerada mercadoria, as regras de livre comércio da OMC serão implementadas também neste campo. A abordagem da educação como bem público, por outro lado, preserva o modelo atual de educação, no qual as universidades públicas têm um *status* especial como instituições de importância para as culturas nacionais. O resultado deste debate terá um impacto considerável no desenvolvimento da educação *online*.

Controle de qualidade

A disponibilidade de sistemas de aprendizado online e a facilidade de ingresso neste mercado abriu a questão do controle de qualidade. O foco excessivo sobre o fornecimento online pode sobrepujar a importância da qualidade dos materiais e da didática. Uma variedade de dificuldades possíveis pode ameaçar a qualidade da educação. Uma delas é o ingresso fácil de novas instituições educacionais, orientadas principalmente para o lucro, as quais freqüentemente possuem poucas das capacidades acadêmicas e didáticas necessárias. Outro problema de controle de qualidade é que a mera transferência de suportes com base em papel para o meio online não tira vantagem do potencial didático específico do novo meio.

As discussões sobre a educação transfronteiriça em geral e o aprendizado online em particular já começaram no âmbito internacional. Uma das primeiras tentativas abrangentes de dar garantia de qualidade aos programas educacionais transnacionais ganhou corpo da UNESCO e no Conselho da Europa em seu "Código de Boa Prática no Fornecimento de Educação Transnacional".

O reconhecimento de diplomas acadêmicos e a transferência de créditos

O reconhecimento de diplomas tornou-se particularmente relevante dentro do ambiente do aprendizado *online*, o seu principal desafio sendo o reconhecimento de diplomas além do contexto regional, principalmente no âmbito global.

A tendência geral rumo à mobilidade do estudante nos graus mais elevados da educação torna possível estudar num sem número de universidades. A União Européia, em particular, realizou avanços significativos neste campo, através de várias iniciativas, como o programa Sócrates, de promoção da cooperação européia ao longo de todas as fases do processo educativo. A mobilidade do estudante postula a necessidade de transferências de créditos entre universidades de diferentes países. O marcos reguladores necessários começaram a ser desenvolvidos nos níveis regionais. Com o Sistema Europeu de Transferência de Créditos (ECTS), a União Européia começou a desenvolver um quadro regulador. A região Ásia-Pacífico seguiu na esteira da Europa, introduzindo o seu próprio modelo regional para o intercâmbio de estudantes e um sistema correlato de transferência de créditos (UCTS).

A padronização da aprendizagem *online*

A fase inicial do desenvolvimento da aprendizagem online foi caracterizada por um crescimento rápido e uma grande diversidade de materiais, isto é, de suportes, de conteúdos e de preceitos didáticos. Não obstante, coloca-se a necessidade de desenvolver padrões comuns em vista de facultar o intercâmbio mais fácil entre cursos online e introduzir um certo padrão de qualidade.

O primeiro padrão, o AICC (Comitê de Treinamento Baseado em Computador da Indústria de Aviação), foi desenvolvido pela indústria da aviação com o objetivo principal de prover interoperabilidade nos pacotes de aprendizagem online. O desenvolvimento essencial subseqüente foi a introdução do IMS (Sistema de Gestão Instrucional), que introduziu um certo número de padrões para a aprendizagem online, inclusive especificação de metadados que podem ser compartilhados por cursos online (descrição de conteúdos, título de cursos, custos, sistemática da aprendizagem, etc.). O IMS é baseado em XML (eXtended Markup Lamguage). Além disso, o Comitê de Padrões de Tecnologia de Aprendizagem (LTSC) do Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE) implementou diversas iniciativas neste campo.

Em 1997, o Departamento de Defesa dos Estados Unidos (DoD) lançou o desenvolvimento mais recente. Confrontado às limitações dos padrões existentes, o DoD criou a iniciativa Aprendizagem Avançada Distribuída (ADL), resultando num novo padrão chamado SCORM, o acrônimo do inglês para Modelo de Referência de Objetos de Conteúdo Compartilháveis. O SCORM é o padrão mais elaborado e mais amplamente utilizado para cursos online. Uma das razões para o sucesso do SCORM é que ele se tornou obrigatório para os cursos dispensados pelo DoD (um mercado de 700 milhões de dólares por ano) e outros órgãos do governo estadunidense. O SCORM também está ganhando visibilidade internacional, sendo cada vez mais amplamente utilizado.

A maior parte das iniciativas de padronização é desenvolvida nos Estados Unidos por instituições privadas e profissionais. Outras iniciativas, inclusive internacionais, são de muito menor escala.

SEÇÃO 7

A estrutura brasileira de governança da Internet

A estrutura brasileira de governança da Internet

Carlos Afonso[1]

O Comitê Gestor da Internet no Brasil (CGI.br) foi criado pela Portaria Interministerial nº 147, de 31 de maio de 1995 e alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003, para coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Também é responsável por assegurar a justa e livre competição entre os provedores e garantir a manutenção de adequados padrões de conduta de usuários e provedores.

Composto por membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica, o CGI.br representa um modelo de governança na Internet pioneiro no que diz respeito à efetivação da participação da sociedade nas decisões envolvendo a implantação, administração e uso da rede. Com base nos princípios de multilateralidade, transparência e democracia, desde julho de 2004 o CGI.br elege democraticamente seus representantes da sociedade civil para participar das deliberações e debater prioridades para a internet, junto com o governo.

– descrição na página Web do CGI.br (*http://www.cgi.br*)

A missão

O Brasil foi pioneiro na formulação e realização de uma abordagem particular para a governança da Internet, por conta de um intenso *lobby* realizado pela comunidade acadêmica e por organizações da sociedade civil[2] em 1994-1995. Esse processo resultou, em maio de 1995, na formação do Comitê Gestor da Internet no Brasil (CGI.br). O comitê era originalmente composto nove voluntários, escolhidos pelo governo federal, incluindo representantes do governo federal, operadoras de telecomunicações,

1 Carlos A. Afonso é diretor de planejamento da Rits - Rede de Informações para o Terceiro Setor (www.rits.org.br) e membro do Comitê Gestor da Internet no Brasil, eleito como um dos representantes da sociedade civil no CFI-Br no período de 2004 a 2007.

2 Entre as organizações ativamente envolvidas nesse processo na época, destacaram-se o Ibase (Instituto Brasileiro de Análises Sociais e Econômicas – *http://www.ibase.br*) e a RNP (Rede Nacional de Ensino e Pesquisa – *http://www.rnp.br*).

provedores de acesso, comunidade acadêmica e representante dos usuários. Coube aos ministérios da Ciência e Tecnologia e das Comunicações a formalização do comitê.

A missão do CGI.br, desde então, tem sido exercer as funções de coordenação e governança da infra-estrutura lógica da Internet no país, incluindo a administração dos nomes de domínio ".br" e a distribuição dos endereços IP no Brasil.

Desde a sua formação, o CGI.br formulou uma política de governança que define o ccTLD (*country code top level domain*)[3] ".br" como um bem da comunidade e como a identidade do Brasil na Internet. Assim, a função central de gestão de domínios e números IP é um serviço sem fins lucrativos no qual a cessão anual dos nomes de domínio custa a mesma coisa (atualmente R$30 por ano) qualquer que seja o domínio. Essa anuidade é necessária para cobrir os custos anuais de operação e desenvolvimento do sistema de governança. O ".br" é restrito a pessoas físicas e jurídicas brasileiras ou com residência permanente no país. Assim, uma pessoa ou entidade que deseja registrar um domínio sob o ".br" deve ter nacionalidade brasileira ou apresentar comprovante de status legal no país (identificado por seu número de registro na Receita Federal – CPF ou CNPJ – e comprovante de endereço físico no país).

As funções do sistema brasileiro de governança encabeçado pelo CGI.br são:

- estabelecer diretivas estratégicas relacionadas com o uso e o desenvolvimento da Internet no Brasil;
- estabelecer diretivas para a organização do relacionamento entre o governo e a sociedade na administração do registro de nomes de domínio, distribuição de números IP e administração do ccTLD .br em prol dos interesses do desenvolvimento da Internet no país;
- propor programas de pesquisa e desenvolvimento relativos à Internet em conformidade com elevados padrões e inovações técnicas, bem como estimular a disseminação da Internet por todo o Brasil, buscando oportunidades para agregar valor aos bens e serviços relativos à rede;

3 Para informação detalhada sobre os ccTLDs no mundo, ver, por exemplo, *http://en.wikipedia.org/wiki/Cctld*.

- promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais relativos à segurança adequada para redes e serviços;
- coordenar ações ligadas à formulação de normas e procedimentos para a regulação de atividades relacionadas com a Internet;
- participar de fóruns técnicos de âmbito nacional e internacional relativos à Internet;
- adotar os procedimentos administrativos e operacionais necessários para que a governança da Internet no Brasil seja realizada conforme padrões internacionais aceitos pelos organismos de governança globais, para os quais pode assinar convênios, contratos e instrumentos semelhantes.

O processo de consolidação

Até 2005, as funções administrativas relacionadas à operação do sistema de nomes de domínio (*DNS*) brasileiro e à arrecadação das anuidades de nomes de domínio (o CGI.br não cobra pela distribuição de números IP) estava a cargo de um projeto junto à Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) em acordo com o governo federal, já que o Comitê Gestor não tinha uma estrutura institucional que permitisse executar essas funções. Em 2004 o CGI.br definiu que fosse formalizada, sob sua supervisão, uma sociedade civil sem fins de lucro, o Núcleo de Informação e Coordenação do .BR, conhecido pela sigla NIC.br, especialmente criada para assumir funções administrativas, inclusive registro, distribuição de números IP, operação de uma rede nacional de pontos de troca de tráfego e manutenção de um projeto nacional de segurança de redes. Uma resolução do CGI.br formalizada em dezembro de 2005 transferiu as funções administrativas do projeto FAPESP para o NIC.br, o que consolidou a autonomia do comitê para realizar plenamente o conjunto de funções acima descritas.

Desde dezembro de 2005 o NIC.br implementa as decisões e projetos do CGI.br, incluindo as seguintes atribuições:

- o registro e manutenção dos nomes de domínios que usam o ".br", e a distribuição de endereços IPs, através do serviço conhecido como Registro.br;
- o tratamento e resposta a incidentes de segurança em computadores envolvendo redes conectadas à Internet brasileira, através do projeto CERT.br (iniciado em 1997);

- a promoção da infra-estrutura para a interconexão direta entre as redes que compõem a Internet no Brasil, através do projeto PTT.br;
- a divulgação de indicadores, estatísticas e informações estratégicas sobre o desenvolvimento da Internet brasileira, através do projeto CETIC.br;
- o suporte técnico e operacional ao LACNIC (Registro de Endereços da Internet para a América Latina e Caribe), que coordena regionalmente a distribuição de números IP.

Assim, todas as operações relacionadas à governança da Internet no país passaram a ser exercidas pelo NIC.br no início de 2006. No entanto, os recursos excedentes arrecadados desde o início da cobrança pela administração de nomes em 1997 e até o início de 2006, e que hoje somam mais de R$140 milhões, estão ainda sob a guarda da FAPESP. O CGI.br, legítimo detentor e responsável por estes recursos, tem examinado junto à FAPESP a forma que será usada para seu repasse ágil em benefício da Internet no país.

A dependência histórica da FAPESP ainda causou outra situação de desconforto quando, em 2002, o maior Ponto de Troca de Tráfego (PTT) da Internet no Brasil na época (interligando as principais espinhas dorsais do país), operado pela FAPESP, foi vendido para a empresa norte-americana Terremark – que passou a explorá-lo comercialmente, com o nome de Network Access Point (NAP) do Brasil, após mudá-lo fisicamente para as instalações da Hewlett-Packard, em São Paulo. Assim, um serviço público sem fins de lucro passava a ser um empreendimento comercial, e o principal ponto nacional de troca de tráfego de dados à época passava a ser controlado por uma empresa dos EUA.

Em 2004 O CGI.br respondeu a essa situação com a implantação do projeto PTT Metropolitano (PTT-Metro) que visa promover como serviço público a criação de infra-estrutura necessária para manter diversos pontos de troca de tráfego nas grandes cidades brasileiras, visando a interconexão direta entre as redes que compõem a Internet no país, em uma operação sem finalidade de lucro – afinal, os PTTs devem contribuir para a maior eficácia do tráfego de dados e uma consequente redução de custos, e não adicionar custos a esse tráfego. Já estão em operação PTTs do projeto nas cidades de Belo Horizonte, Brasília, Curitiba, Florianópolis, Porto Alegre, Rio de Janeiro e São Paulo.

A representatividade no CGI.br já foi uma questão bastante debatida – desde a sua criação os conselheiros eram indicados exclusivamente pelo governo federal. Depois da mudança de governo no final de 2002, iniciou-se uma processo de transição a partir de sugestões apresentadas ao novo governo em fevereiro de 2003 pela comunidade acadêmica e entidades civis. Essencialmente a proposta buscava, por um lado, que a representação tivesse uma maioria de membros não governamentais, e por outro, que todos os conselheiros não governamentais fossem eleitos por seus respectivos grupos de interesse.

Entre 2003 e 2004, ocorreu, como resultado, um desdobramento significativo: o governo federal determinou que o número de membros do conselho subisse para 21, onze dos quais oriundos de organizações ou associações não governamentais eleitos para mandatos de três anos por suas próprias bases. Nessa nova estrutura de representação, já estabelecida desde a primeira eleição *online* de conselheiros em 2004, a distribuição de membros do comitê é a seguinte:

- o governo federal escolhe oito conselheiros;
- as secretarias estaduais de Ciência e Tecnologia escolhem um conselheiro;
- entidades civis não empresariais (o chamado "terceiro setor") escolhem quatro conselheiros;
- associações empresarias (provedores de acesso e conteúdo da Internet; provedores de infra-estrutura de telecomunicações; indústria de bens de informática, de bens de telecomunicações e de software; setor empresarial usuário) escolhem quatro conselheiros;
- as associações acadêmicas escolhem três conselheiros;
- por fim, um conselheiro considerado de notório saber no campo das tecnologias de informação e comunicação é escolhido por consenso.

Os conselheiros não governamentais têm mandato de três anos.

As conquistas

O registro do Brasil vem angariando uma reputação internacional como iniciativa muito bem administrada e tecnicamente sofisticada. Além de sediar todos os serviços técnicos do registro regional de números IP (LACNIC), mantém servidores espelho para outros países e exporta sua tecnologia de administração de DNS (baseada em software livre e de

código aberto) para vários outros países (especialmente da África), para os quais também provê treinamento.

Atualmente o registro de domínios ".br" está entre os maiores em números de domínios de países, com mais de 1,1 milhão de domínios registrados.[4]

O NIC.br mantém em suas instalações em São Paulo um "espelho" (duplicata) de um dos 13 servidores-raiz[5] da rede mundial – o servidor-raiz "F". Isso significa que a consulta aos servidores-raiz globais a partir de qualquer computador no Brasil não precisa ir aos Estados Unidos, Suécia, Inglaterra, Holanda ou Japão para obter um endereço Internet não brasileiro (ou seja, que não seja do domínio ".br").

O NIC.br mantém em suas instalações em São Paulo um "espelho" (duplicata) de um dos 13 servidores-raiz da rede mundial -- o servidor-raiz "F". Isso significa que a consulta aos servidores-raiz globais a partir de qualquer computador no Brasil não precisa ir aos Estados Unidos, Suécia, Inglaterra, Holanda ou Japão para obter um endereço Internet não brasileiro (ou seja, que não seja do domínio ".br").

Outras cópias de servidores-raiz (o "K" e o "I") serão instaladas no país aumentando ainda mais a independência da rede brasileira em relação ao acesso à raíz do DNS Internet.

O servidor-raiz DNS do ".br" está sediado em São Paulo, com secundários no Rio de Janeiro (Embratel), Brasília (RNP), San Francisco (ISC) e Frankfurt (DENIC). O NIC.br opera servidores secundários para diversos países como Alemanha (".de"), o Panamá (".pa"), Paraguai (".py"), El Salvador (".sv"), Uruguai (".uy") e Iêmen (".ye"). Em todos estes locais o NIC.br mantém equipamentos e uma rede autônoma (*ASN*) próprios.

O software de gerência de domínios desenvolvido pelo NIC.br (livre e de código aberto) é atualmente utilizado pelo Quênia, e já foram treinadas para uso do software equipes de Angola, Moçambique, Uruguai e Tanzânia, sendo que Moçambique e Tanzânia já estão em fase de ativação do sistema. O software também foi repassado ao Uruguai.

Através do projeto CERT.br, em convênio com a Carnegie Mellon, o NIC.br iniciou cursos de treinamento avançado em segurança da rede em abril de 2004. Desde então foram treinados mais de 200 profissionais de

4 Ver a tabela completa, atualizada regularmente, em *http://registro.br/estatisticas.html*.

5 Sobre os servidores-raiz, ver, por exemplo, *http://en.wikipedia.org/wiki/Root_nameserver*.

várias áreas de atuação (alguns em mais de um curso) em tópicos como: criação e gestão de um centro de resposta a incidentes de segurança; segurança da informação para equipes técnicas; fundamentos do manejo de incidentes de segurança; manejo avançado de incidentes de segurança para equipes técnicas. As principais funções do CERT.br incluem:

- atuar como ponto de contato nacional para notificação de incidentes de segurança;
- prover o apoio necessário no processo de resposta a incidentes;
- trabalhar em colaboração com outras entidades, como os operadores da justiça;
- colaborar nas questões de segurança de rede com os provedores de acesso e serviços, bem como as operadoras de espinhas dorsais (*backbones*);
- auxiliar novos grupos de segurança de redes a estabelecerem e desenvolverem suas atividades.

O CGI.br mantém ainda, através do projeto CETIC.br, acordos com o IBGE e entidades privadas de pesquisa de amostragem para a elaboração regular de estatísticas sobre o uso e disseminação das TICs (tecnologias de informação e comunicação) e em especial da Internet no Brasil.

Por fim, o Brasil é um dos primeiros países a iniciar a implantação de um sistema de nomes de domínio seguro, conhecido pela sigla DNSsec, que consiste basicamente em uma metodologia de validação de nomes de domínio protegida por autenticação criptografada. Isso na prática impede que nomes de domínio sejam forjados, conduzindo o usuário a um sítio Web falso, por exemplo.

Desafios

Como visto, a abordagem brasileira para a governança da Internet é uma conquista inovadora em gestão pluralista de bens da comunidade. O CGI.br não cobre todos os temas da governança da Internet, atualmente objeto de discussão mundial através do Fórum de Governança da Internet da ONU (IGF). No entanto, através de Comissões de Trabalho voluntárias, busca acompanhar esses temas (conteúdo, acesso, inclusão digital, privacidade, regulação, uso indevido, entre outros). É importante destacar que o CGI.br participa em forma destacada dos principais fóruns, conferências, organismos e eventos internacionais relacionados ao desenvolvimento e governança da Internet, entre os quais as reuniões da ICANN e do IGF.

O CGI.br aprovou em 2007 uma política geral de apoio a projetos estruturantes relacionados aos temas da governança e à alavancagem das TICs para o desenvolvimento humano no Brasil. Parte da receita excedente será utilizada no apoio a projetos que serão captados através de editais a partir de 2008. Para isso é necessário resolver um problema crucial – o repasse dos recursos já mencionados, ainda retidos pela FAPESP.

Resta ainda assegurar que a legislação que criou e regulamenta o CGI.br seja aperfeiçoada e perpetuada para tornar essa conquista da sociedade brasileira imune a flutuações políticas.

Referências na Internet

http://www.cgi.br – Comitê Gestor da Internet no Brasil (CGI.br)

http://www.fapesp.br – Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP)

http://www.icann.org – Internet Corporation for Assigned Names and Numbers (ICANN)

http://www.intgovforum.org – Internet Governance Forum (IGF)

http://www.lacnic.net/pt/index.html – Registro de Endereços Internet para a América Latina e o Caribe (LACNIC)

SEÇÃO 8

Anexos

ANEXO I

"OS HOMENS CEGOS E O ELEFANTE"

Havia seis homens no Industão
A aprender muito inclinados.
Eles foram ver o elefante
(Embora da visão todos fossem privados)
Para que cada qual, por observação,
Pudesse satisfazer a sua razão

O Primeiro aproximou-se do elefante
E, tropeçando, deu
Contra o seu grande e robusto flanco,
Passando imediatamente a apregoar:
"Deus me abençoe!, mas o Elefante
parece certamente uma parede!"

O Segundo, apalpando uma das presas,
Gritou, "Oh!, o que temos aqui
Tão arredondado, liso e pontiagudo?
Para mim, nada há de mais claro
O prodigioso Elefante
parece certamente uma lança!"

O Terceiro aproximou-se do animal,
E tendo-lhe pego
A tromba serpeante entre as mãos,
Valentemente a levantou e disse:
"Vejo, pois, que o Elefante
parece certamente uma serpente!"

O Quarto estendeu uma mão ansiosa,
E o apalpou na altura do joelho.
"Ao que mais o animal extraordinário
se assemelha,
Não há mistério", repetiu ele;
"Está bem claro, o Elefante
parece certamente uma árvore!"

O Quinto, que por acaso tocou-lhe
a orelha,
Disse: "Mesmo o mais cego dos homens
Pode dizer com que isto mais parece;
Que o negue quem puder
Esta maravilha de Elefante
parece certamente um abano!"

O Sexto logo em seguida começou
A apalpar a besta,
Então, agarrou a cauda balangante
Que lhe caiu no alcance,
"Sim", disse ele, "o Elefante
parece certamente uma corda!"

E então esses homens do Industão
Discutiram alto e longamente,
Cada qual com sua própria opinião
A avultar-se inflexível e forte.
Embora cada um tivesse parcialmente razão,
E todos estivessem errados!

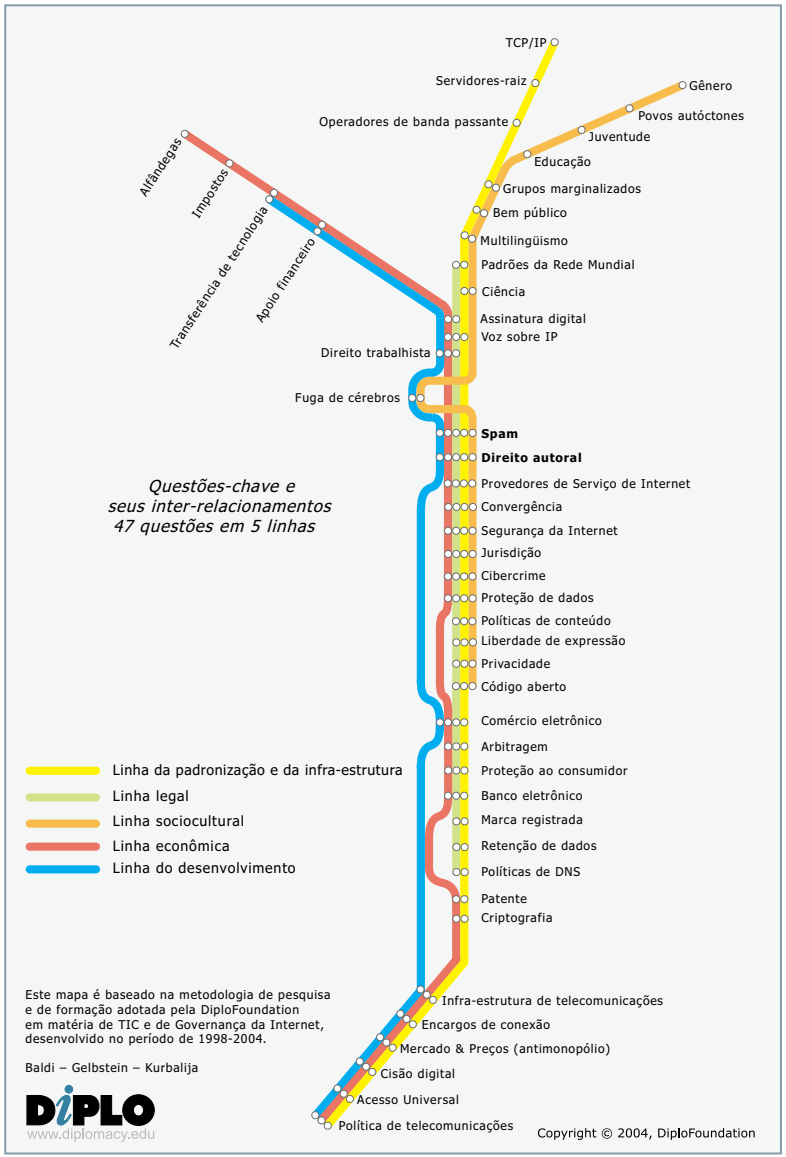
Moral: Muito amiúde nas guerras teológicas,
As partes em conflito, eu suponho,
Ralham na mais total ignorância
Do que o outro lhe quer dizer,
E tagarelam sobre um Elefante
Que nenhuma viu!

Poeta norte-americano John Godfrey Saxe (1816 – 1887)

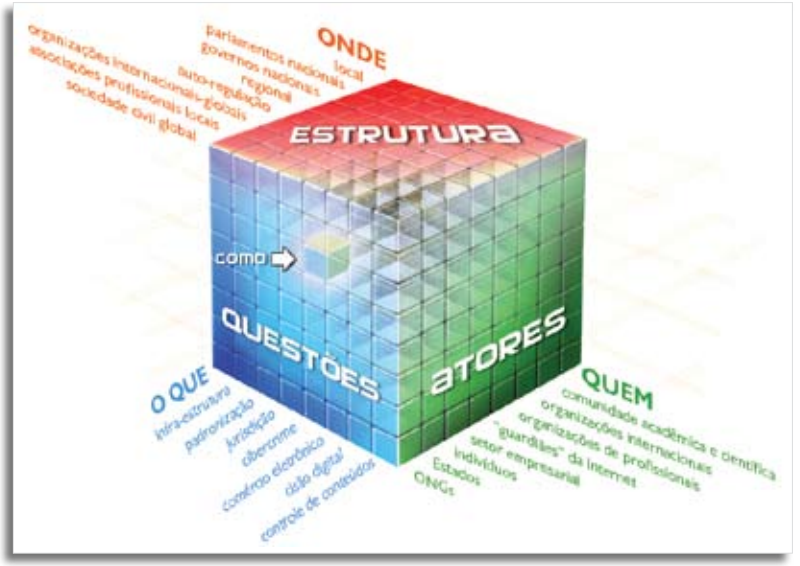
ANEXO II – UMA SÍNTESE DA EVOLUÇÃO DA GOVERNANÇA DA INTERNET

Ator / Período	Estados Unidos	"Guardiões" da Internet	Organizações Internacionais	Setor privado	Países	Sociedade Civil
	O Departamento de Defesa (DoD) gere o DNS.					
1986	Fundação Nacional de Ciências (NSF) pega o bastão do DoD.					
1994				A NSI assina contrato com a NSF para gerir DNS de 1994-1998.		
O COMEÇO DA "GUERRA DO DNS" Depois de a NSF terceirizar a gestão do DNS à NSI (uma empresa privada), a comunidade da Internet (principalmente a Internet Society - ISOC) tenta por vários anos devolver a gestão do DNS ao domínio público. Após 4 anos, ela consegue. Eis a seguir um panorama desse processo, que envolveu muitas técnicas diplomáticas, como negociação, formação de coalizões, uso de pressões, construção de consensos, etc.						
Junho de 1996		IANA/ISOC – Planejam pegar o bastão da NSI após o término do seu contrato; a introdução de domínios adicionais; forte oposição do setor de marcas registradas contra novos domínios de primeiro nível; oposição forte também da UIT.				
Primavera de 1997		Proposta de criação de um Comitê Ad Hoc internacional – IAHC. Composição do IAHC: 2 representantes dos grupos de interesse das marcas registradas, OMPI, UIT e NSF; e 5 representantes da IETF. Conclusão do Memorando de Acordo sobre os gTLDs especificando: DNS como "recurso público"; 7 novos domínios; forte proteção a marcas registradas. Criação do CORE (Conselho de Registradores – cerimônia de assinatura em março de 1997 na UIT, em Genebra; o CORE entrou imediatamente em colapso. Forte oposição do governo EEUU, da NSI e da UE.				
1997	Governo dos EEUU transfere a gestão do DNS para o Departamento de Comércio (DoC).					
Junho de 1998	Um documento estratégico do DoC convida os principais atores a propor soluções próprias.	São recebidas propostas do IFDT (International Forum on White Paper), ORSC (Open Root Server Confederation) e BWG (Boston Working Group).				
		Em vez de esboçar um novo documento, a ISOC se concentrou em: - Construir uma grande coalizão envolvendo organizações internacionais (a partir da iniciativa do IAHC), do setor privado (IBM) e dos países-chave (UE, Japão, Austrália). - Criar uma nova organização.				
Segunda metade de 1998		Setembro de 1998 – Minuta de Acordo Conjunto ISOC-NSI. Outubro de 1998 – ISOC abandona acordos e cria a ICANN.				
15 de novembro de 1998	DoC transfere autoridade para ICANN.	ICANN adquire duas novas funções cruciais: - Autoridade para credenciar registradores para o gTLD. - Gestão do papel de supervisão (a dimensão política permanece com o DoC).				
Abril de 1999		Assinatura de um acordo DoC – ICANN – NSI e introdução de um "Sistema de Registro Compartilhado"; NSI perde o monopólio mas obtém um arranjo de transição favorável (gestão de 4 domínios, etc.). A ESTRUTURA E O FUNCIONAMENTO DA ICANN.				
Junho de 1998		Formação da PSO (Protocol Suporting Organization) reagrupando a IETF, o W3C e outros pioneiros da Internet.	Início do processo de Nomes de Domínio da Internet da OMPI.	- Criação da ASO (Address Support Organization) – para representar a associação de registros de Internet (ARN, RIPE, NCC). - Criação da DNSO (Domain Name Supporting Organization) – para proteger marcas registradas e interesses comerciais.	- 30 países fundam o GAC em vista de conquistar mais influência na gestão de domínios nacionais. - ICANN reage fundando o subcomitê DNSO 0 ccTLDs.	
O FIM DA "GUERRA DO DNS" A "guerra" terminou graças a um compromisso. A ISOC obteve mais controle público do DNS, ainda que os interesses comerciais tenham permanecido muito poderosos. Assim, os interesses comerciais privados e aqueles das comunidades de "guardiões" da Internet foram adequadamente protegidos. Este não foi o caso dos interesses dos Estados-nação e da comunidade da Internet em geral. Estes são os dois aspectos mais frágeis da governança da ICANN.						
2000-2003			Emergência de uma maior atenção à Internet da parte de UIT, OMPI, UNESCO, OCDE, Conselho da Europa e do Banco Mundial .	Fortes pressões da parte do setor privado em prol de regulamentar a Internet (leis de direito autoral; comércio eletrônico, etc.).	Desenvolvimento da legislação sobre a Internet, processos judiciais, etc.	Envolvimento das ONGs nas questões de cisão digital, direitos humanos e gênero na Internet.
			Iniciativas multi-setoriais e globais centradas no desenvolvimento da Internet, governança, etc.: G8 Ponto Força, Fórum Econômico Mundial (FEM), Força Tarefa da ONU sobre TIC, Cúpula Mundial sobre Sociedade da Informação (CMSI), Global Knowledge Partnership (GKP).			

ANEXO III – UM MAPA PARA UMA JORNADA PELA GOVERNANÇA DA INTERNET



ANEXO IV – O CUBO DIPLO DA GOVERNANÇA DA INTERNET



O eixo QUE diz respeito às QUESTÕES da Governança da Internet (e.g. infra-estrutura, direitos autorais, privacidade). Ele traduz a dimensão multidisciplinar desta abordagem. O eixo QUEM do cubo enfoca os principais ATORES (Estados, organizações internacionais, o setor privado). Trata-se do lado multipartite ou multi-acionário da abordagem. O eixo ONDE do cubo lida com o QUADRO no qual as questões da Internet devem ser tratadas (auto-regulamentação, local, nacional, regional e global). Trata-se da abordagem por camadas da Governança da Internet.	Ao movermos as peças em nosso cubo, nós obtemos as interseções – COMO. Esta é a parte do cubo que pode nos ajudar a ver como questões específicas devem ser regulamentadas, tanto em termos de técnicas cognitivo-legais (e.g. analogias) quanto em termos de instrumentos (e.g. direito brando, tratados e declarações). Por exemplo, uma interseção específica pode nos ajudar a ver COMO questões de privacidade (que) devem ser tratadas pela sociedade civil (quem) no âmbito nacional (onde). E à parte do cubo da Internet há um quinto componente – QUANDO.

SOBRE OS AUTORES

Jovan Kurbalija

Jovan Kurbalija é diretor fundador da DiploFoundation. Ele é um ex-diplomata com experiência profissional e acadêmica em direito internacional, diplomacia e tecnologia da informação. Desde o final dos anos 1980, ele conduz pesquisas nos domínios da TIC e do direito. Em 1992, ele foi encarregado de criar a primeira Unidade sobre Tecnologias da Informação e Diplomacia na Academia Mediterrânea de Estudos Diplomáticos, em Malta. Após mais de dez anos de esforços bem-sucedidos nos campos da formação, pesquisa e edição, em 2003 a Unidade se desdobrou na DiploFoundation.

Jovan Kurbalija dirige cursos *online* de teleformação em TIC e diplomacia e dá conferências em instituições acadêmicas e de treinamento na Suíça, Estados Unidos, Áustria, Reino Unido, Holanda e Malta. Ele também foi membro do Grupo de Trabalho sobre Governança da Internet da ONU.

Entre os seus principais interesses de pesquisa estão: a diplomacia e o desenvolvimento de um regime internacional para a Internet, a utilização do hipertexto na diplomacia, as negociações *online*, e o direito diplomático.

jovank@diplomacy.edu

Ed Gelbstein

Eduardo Gelbstein é membro honorário do Instituto das Nações Unidas para Formação e Pesquisa (UNITAR) e colaborador da Força Tarefa das Nações Unidas sobre Tecnologias da Informação e Comunicação, tendo participado dos trabalhos preparatórios para a Cúpula Mundial sobre a Sociedade da Informação. Ele é ex-diretor do Centro Internacional de Informática das Nações Unidas.

Além da sua colaboração com as Nações Unidas, as suas atividades como conferencista e palestrante universitário refletem a sua experiência de 40 anos em gestão de teconologias da informação.

Ele trabalhou na Argentina, Holanda, Reino Unido, Austrália e, depois de entrar para a ONU, em Genebra (Suíça) e em Nova Iorque (Estados Unidos). Foi graduado em engenharia eletrônica na Universidade de Buenos Aires, Argentina, em 1963, tendo feito mestrado na Holanda e doutorado no Reino Unido.

gelbstein@diplomacy.edu

www.diplomacy.edu

A Diplo é uma organização sem fins lucrativos cujo objetivo é ajudar todos os países, particularmente os que dispõem de poucos recursos, a participar significativamente nas relações internacionais. A Diplo promove uma abordagem mutipartite ou multi-acionária, envolvendo a participação de organizações internacionais, da sociedade civil e de outros atores nos assuntos internacionais. Entre as atividades da Diplo figuram programas de educação e de formação profissional, pesquisas e o desenvolvimento de tecnologias de informação e comunicações para os meios diplomáticos.

www.globalknowledge.org

A Global Knowledge Partnership (GKP) é uma rede mundial cujo compromisso é tirar proveito do potencial das tecnologias de informação e comunicações (TICs) em prol do desenvolvimento sustentável e eqüitativo. A visão da GKP é a de um mundo de oportunidades iguais em que todas as pessoas possam ter acesso e usar conhecimentos e informações para melhorar as suas vidas. A rede viabiliza o compartilhamento de informações, experiências e recursos em vista de ajudar a reduzir a pobreza e a fortalecer a autonomia dos povos.

www.sdc.admin.ch

A Agência Suíça para o Desenvolvimento e a Cooperação (SDC) é o órgão encarregado da cooperação internacional e da ajuda humanitária no seio do Ministério das Relações Exteriores da Suíça. Sua atividade inclui programas de apoio abrangente a países, apoio a organizações multilaterais e financiamento de trabalhos conduzidos por organizações suíças e internacionais de relevo.

www.idrc.ca

O Centro Internacional de Pesquisas sobre Desenvolvimento (IDRC) é uma entidade criada pelo Parlamento do Canadá em 1970 para apoiar países em desenvolvimento a utilizarem a ciência e a tecnologia para encontrar soluções de longo prazo para os problemas sociais, econômicos e ambientais que enfrentam. O apoio do IDRC é direcionado a construir uma comunidade de pesquisa cujo trabalho presente e futuro irá construir sociedades mais saudáveis, mais equitativas e mais prósperas.

www.rits.org.br

www.nupef.org.br

A RITS - Rede de Informações para o Terceiro Setor, através de seu Núcleo de Pesquisas, Estudos e Formação (NUPEF) organiza e promove a pesquisa, os estudos, a disseminação de conhecimento e a formação e qualificação de pessoas atuantes no universo da sociedade civil organizada, frente aos novos desafios enfrentados nas sociedades da informação e da comunicação.

Este trabalho foi desenvolvido com o apoio financeiro do Centro Internacional de Pesquisas sobre o Desenvolvimento, Ottawa, Canada.