CADERNOS CGI.br Referências

3

Uma introdução à Governança da Internet

Jovan Kurbalija

Esta obra foi publicada nos termos da licença
Atribuição-Não Comercial-Sem Derivações 4.0 Internacional
<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.pt>

Núcleo de Informação
e Coordenação do Ponto BR

CADERNOS CGI.br **Referências**

Uma introdução à Governança da Internet

Jovan Kurbalija

Comitê Gestor da Internet no Brasil
2016

Núcleo de Informação e Coordenação do Ponto BR

Diretor Presidente
Demi Getschko

Diretor de Assessoria às Atividades do CGI.br
Hartmut Richard Glaser

Diretor Administrativo
Ricardo Narchi

Diretor de Serviços e Tecnologia
Frederico Neves

Diretor de Projetos Especiais e de Desenvolvimento
Milton Kaoru Kashiwakura

Produção dos Cadernos CGI.br
Diretoria de Assessoria às Atividades do CGI.br

Assessoria Administrativa
Paula Liebert, Salete Matias

Assessoria Técnica às Atividades do CGI.br
Carlos Francisco Cecconi, Diego Rafael Canabarro, Jamila Venturini, Jean Carlos Ferreira dos Santos, Juliano Cappi, Marcelo Oliveira, Nathalia Sautchuk Patrício, Vinicius Wagner Oliveira Santos

Coordenação Executiva e Editorial
Carlos Francisco Cecconi e Juliano Cappi

Produção Editorial
Caroline D'Avo (Comunicação NIC.br) e Everton Rodrigues (Comunicação NIC.br)

Projeto Gráfico
Pilar Velloso

Produção desta publicação
Revisão Técnica
Jamila Venturini, Jean Carlos Ferreira dos Santos e Juliana Nolasco

Tradução
Carolina Carvalho

Revisão da Tradução
Neuza Paranhos e André Linn

Diagramação
Ana Beatriz Pádua

Ilustrações
Zoran Marcetic – Marča & Vladimir Veljašević e Pilar Velloso (livro em português)

Fotos
Getty Images (imagem de fundo da capa) e iStockphoto

Traduzido do Original
Kurbalija, Jovan. An Introduction to Internet Governance. 6ª ed. Malta, Switzerland: DiploFoundation, 2014. 204 p. ISBN: 978-99932-53-28-0.

Esta publicação está disponível também em formato digital em <http://www.cgi.br>

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Kurbalija, Jovan
Uma introdução à governança da internet [livro eletrônico] / Jovan Kurbalija ; [Zoran Marcetic -Marca & Vladimir Veljasevic ; tradução Carolina Carvalho]. -- São Paulo : Comitê Gestor da Internet no Brasil, 2016.
6,95 Mb ; PDF
Título original: An introduction to internet governance.
ISBN 978-85-5559-023-8
1. Internet - Administração 2. Internet - Aspectos econômicos 3. Internet - Leis e legislação 4. Redes de computadores 5. Redes de computadores - Leis e legislação I. Zoran Marcetic - Marca & Vladimir Veljasevic. II. Título.
16-05386 CDD-004.678

Índices para catálogo sistemático:
1. Governança da Internet : Ciência da computação
004.678
2. Internet : Governança : Ciência da computação
004.678

Comitê Gestor da Internet no Brasil (CGI.br)

Composição em Dezembro de 2016

Integrantes

Representantes do Setor Governamental
Carlos Roberto Fortner
Francilene Procópio Garcia
Franselmo Araújo Costa
Igor Vilas Boas de Freitas
Luiz Carlos de Azevedo
Luiz Fernando Martins Castro
Marcelo Daniel Pagotti
Marcos Vinícius de Souza
Maximiliano Salvadori Martinhão

Representantes do Setor Empresarial
Eduardo Fumes Parajo
Eduardo Levy Cardoso Moreira
Henrique Faulhaber
Nivaldo Cleto

Representantes do Terceiro Setor
Carlos Alberto Afonso
Flávia Lefèvre Guimarães
Percival Henriques de Souza Neto
Thiago Tavares Nunes de Oliveira

Representantes da Comunidade Científica e Tecnológica
Flávio Rech Wagner
Lisandro Zambenedetti Granville
Marcos Dantas Loureiro

Representante de notório saber em assuntos de Internet
Demi Getschko

Coordenador
Maximiliano Salvadori Martinhão

Secretário Executivo
Hartmut Richard Glaser

Prefácio

Em 2004, quando disse a meus amigos o que fazia como membro do GTGI – o Grupo de Trabalho Sobre Governança da Internet – eles costumavam me telefonar para consertar suas impressoras ou instalar um software novo. Pelo que entendiam, eu trabalhava com algo relacionado a computadores. Lembro-me de fazer uma rápida consulta com os meus colegas de GTGI, perguntando-lhes como eles explicavam a seus amigos, namoradas, esposas e filhos o que faziam. Assim como eu, também estavam tendo dificuldades. Este é um dos motivos pelos quais comecei a planejar e elaborar os primeiros textos e desenhos da Diplo relacionados à governança da Internet.

Hoje, apenas dez anos depois, as mesmas pessoas que me pediam para instalar suas impressoras vêm a mim para perguntar de que maneira podem manter a propriedade de seus dados no Facebook ou de que maneira podem garantir que seus filhos usem a Internet de forma segura. Cada vez mais, eles se preocupam com uma possível guerra cibernética e os riscos online para o abastecimento de água, as usinas elétricas e outras infraestruturas cruciais em suas cidades e países. Avançamos muito!

A governança da Internet ganha cada vez mais espaço junto à opinião pública. Quanto mais a sociedade moderna depende da Internet, mais relevante é a sua governança. Longe de pertencer à esfera de alguns poucos escolhidos, a governança da Internet é de interesse de todos nós, em menor ou maior grau, quer sejamos um dos 2,9 bilhões de usuários da Internet ou um não usuário que depende das facilidades que ela oferece.

A governança da Internet é obviamente mais relevante para aqueles que estão profundamente integrados com o meio eletrônico, quer seja fazendo negócios pelo meio eletrônico ou fazendo networking pelo Facebook. No entanto, o seu alcance é amplo. Autoridades governamentais, militares, advogados, diplomatas, e outras pessoas comprometidas com o fornecimento de bens públicos ou com a preservação da estabilidade pública também estão envolvidas no meio. A governança da Internet, e mais especificamente a proteção da privacidade e de outros direitos humanos, é um ponto central para os ativistas da sociedade civil e as organizações não governamentais.

Para as universidades e os inovadores mundo afora, a governança da Internet deve garantir que a Internet permaneça aberta, visando o desenvolvimento e a inovação. Os inventores criativos de futuros Googles, Skypes, Facebooks e Twitters estão por aí, em algum lugar, navegando na Internet.

A criatividade e inovação dessas pessoas não devem ser reprimidas; em vez disso, devem ser incentivadas, desenvolvendo novas formas mais criativas de usar a Internet.

Espero que este livro seja uma introdução clara e acessível à governança da Internet. Para alguns de vocês, será o primeiro contato com o assunto. Para outros, poderá servir como lembrete de que o que já estão fazendo em sua área de especialização – seja saúde, comércio ou governança e outros assuntos por meios eletrônicos – faz parte de uma família mais ampla relacionada às questões de governança da Internet.

O objetivo subjacente de uma abordagem tão ampla é contribuir modestamente para a preservação da Internet como um meio integrado e facilitador para bilhões de pessoas ao redor do mundo. Pelo menos, espero despertar a curiosidade e incentivar as pessoas a se aprofundarem nesse tema extraordinário e fluente. Atualize-se. Acompanhe os acontecimentos em <http://diplomacy.edu/capacty/IG>

Jovan Kurbalija
Diretor da DiploFoundation
Chefe da Geneva Internet Plataform

Prefácio à edição brasileira

Segundo dados de empresas especializadas em software corporativo, menos de 5% do conteúdo total Web é acessível publicamente. Mais de 95% pertencem a redes corporativas e/ou encontram-se disponíveis em servidores protegidos por senhas e outros mecanismos de segurança, que em seu conjunto constituem a "Web profunda." Nos emaranhados da "Web profunda" coexiste a "Web escura", espaço de atividades supostamente sigilosas ou ilegais.

Nessa "deep Web" estão cerca de oito zettabytes de dados (oito trilhões de gigabytes), que crescem vertiginosamente. É o espaço restrito das grandes corporações multinacionais, das redes financeiras, dos sistemas governamentais e militares.[1]

Na "dark Web" ou "DarkNet", segundo o Trend Micro Deep Web Analyzer, pode-se conseguir um passaporte falso dos EUA por US$5.900, ou 100 contas roubadas do PayPal ou eBay por US$100, ou ainda pode-se contratar o assassinato de uma celebridade ou político por US$180 mil.[2]

Tanto a Web pública como a profunda coexistem em uma rede de redes planetária, usando canais exclusivos ou compartilhando os mesmos canais, utilizando a mesma tecnologia e o mesmo universo de endereços IP, bem como os mnemônicos conhecidos como nomes de domínio, associados a endereços IP pelo sistema de nomes de domínio (DNS) coordenado pela ICANN (Corporação da Internet para Designação de Nomes e Números), ou em sistemas de DNS paralelos (como o utilizado pela rede Tor). Mesmo usando domínios DNS alternativos, seguem de algum modo interconectadas. Essa complexa e gigantesca rede de redes é o que chamamos de Internet.

A governança da Internet pode ser vista como o conjunto de atividades desenvolvidas por uma complexa teia de agentes (privados e públicos, na-

1 Ver <http://www.legaltechnology.com/wp-content/uploads/2013/07/OpenText-EIM Summary.pdf>

2 Ver <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploring-the-deep-web>

cionais e internacionais) de gerência e coordenação de recursos, processos, conteúdos, aplicativos e sistemas relacionados. Como conceito formal, a governança da Internet surgiu dos debates da Cúpula Mundial da Sociedade da Informação (WSIS/CMSI). A expressão busca abranger toda a Internet, e não só o relativamente diminuto pedaço público da rede. De fato, por exemplo, é impraticável separar a Web profunda da pública nas políticas de endereçamento, ou nos protocolos de comunicação.

Internacionalmente, o esforço em espaços multilaterais e multissetoriais é buscar o consenso para critérios comuns de governança, que permitam garantir, como expressa a declaração do Encontro NETmundial,[3] que a Internet continue a ser "uma rede de redes globalmente coerente, interconectada, estável, não fragmentada, escalável e acessível, baseada em um conjunto comum de identificadores únicos e que permita que datagramas e informação fluam livremente de ponta a ponta independentemente de seu conteúdo legal."

No âmbito do direito à comunicação, no dia 1 de julho de 2016 o Conselho de Direitos Humanos da ONU aprovou a resolução "A promoção, proteção e desfrute dos direitos humanos na Internet,"[4] que reforça os princípios em defesa de direitos da declaração do NETmundial, afirmando que a liberdade de expressão é um direito universal não limitado por fronteiras ou os meios utilizados para expressar-se, e tem que ser característica integrante de uma Internet aberta e livre.

Garantir os direitos universais é componente fundamental da governança da Internet. Mas hoje vai além, tendo que considerar praticamente todos os setores de atividade das sociedades humanas. No momento em que termino de escrever este prefácio, quase meia-noite, o Internet Live Stats[5] informa que a Internet contabiliza 3,4 bilhões de usuários; consumiu apenas hoje 3,2 mil gigawats-hora de energia elétrica; e emitiu 2,8 milhões de toneladas de CO2, lembrando-nos que, da infraestrutura física e lógica à defesa dos direitos fundamentais e ao desenvolvimento humano sustentável, passando pela inclusão digital (e por que não dizer social) dos 3,6 bilhões restantes da população do planeta, uma significativa lista diversificada de temas precisa ser considerada na governança da Internet.

Em especial, em setembro de 2015 a Assembléia Geral da ONU aprovou 17 Objetivos de Desenvolvimento Sustentável, com 169 metas específicas a serem cumpridas pelos Estados-membros até 2030.[6] É crucial relacionar a realização dessas metas com as iniciativas de governança da Internet.

---

3 Ver <http://netmundial.br>
4 Ver <https://www.article19.org/data/files/Internet_Statement_Adopted.pdf>
5 Ver <http://www.internetlivestats.com>
6 Ver <http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E>

Este compêndio, organizado cuidadosamente (e periodicamente atualizado) pela DiploFoundation, sistematiza e problematiza tais temas. Para além de uma introdução ao assunto, serve como um guia permanente sobre a agenda técnica, socioeconômica, política e cultural que compõe o verdadeiro mosaico formado pela Internet e sua governança.

Carlos A. Afonso
Conselheiro do CGI.br
dezembro de 2016

Sumário

Embora a governança da Internet lide com a parte central do mundo digital, governança não pode ser tratada por uma lógica digital-binária de verdadeiro/falso e bom/mau . Em vez disso, a governança da Internet exige diferentes sutilezas e matizes de significado e percepção; Exige, portanto, uma abordagem análoga, que possa dar conta de um continuum de opções e compromissos. Assim, este livro não tenta oferecer declarações definitivas sobre questões de governança da Internet. Pelo contrário, o seu objetivo é propor um quadro prático para análise , discussão e resolução de problemas, que seja significativo para o campo.

Introdução

A controvérsia que envolve a governança da Internet começa pela sua definição. Não se trata apenas de pedantismo linguístico. A forma como a Internet é definida reflete diferentes perspectivas, abordagens e interesses de políticas.

Tradicionalmente, os especialistas da telecomunicação veem a governança da Internet sob a ótica do desenvolvimento de determinada infraestrutura técnica. Os especialistas da computação se concentram no desenvolvimento de diferentes padrões e aplicações, como XML (*eXtensible Markup Language*) ou Java. Os especialistas da comunicação enfatizam a facilidade da comunicação. Os ativistas dos direitos humanos enxergam a governança da Internet do ponto de vista da liberdade de expressão, da privacidade e de outros direitos humanos básicos. Os advogados se concentram na jurisdição e resolução de controvérsias. Os políticos ao redor do mundo geralmente priorizam questões que ressoam junto ao seu eleitorado, como o tecno-otimismo (mais computadores = mais educação) e ameaças (segurança da Internet, proteção à criança). Os diplomatas se preocupam principalmente com o desenvolvimento dos interesses nacionais e sua proteção. A lista de abordagens profissionais potencialmente conflitantes acerca da governança da Internet não tem fim.

O que significa governança da Internet?

A Cúpula Mundial sobre a Sociedade da Informação (CMSI)[1] apresentou a seguinte definição prática sobre governança da Internet:

> Governança da Internet é o desenvolvimento e a aplicação pelos Governos, pelo setor privado e pela sociedade civil, em seus respectivos papéis, de princípios, normas, regras, procedimentos de tomadas de decisão e programas em comum que definem a evolução e o uso da Internet[2].

Esta definição prática, um tanto ampla, não responde à questão das diferentes interpretações de dois termos-chave: 'Internet' e 'governança'.

'i'NTERNET OU 'I'NTERNET E A SINALIZAÇÃO DIPLOMÁTICA

Em 2003, a revista The Economist começou a escrever Internet com "i" minúsculo. Esta mudança na política editorial foi inspirada pelo fato de que a Internet havia se tornado um elemento corriqueiro, deixando de ser algo único e especial o bastante para assegurar a letra maiúscula inicial. A palavra 'internet' seguia o destino linguístico de (t)elégrafo, (t)elefone, (r)ádio, (t)elevisão e outras invenções do tipo.

A questão de escrever Internet/internet com "i" maiúsculo ou minúsculo ressurgiu na Conferência da União Internacional de Telecomunicações (UIT) em Antália (novembro de 2006), na qual a dimensão política foi introduzida quando o termo 'Internet' apareceu na deliberação da UIT sobre governança da Internet com 'i' minúsculo em vez do habitual "I" maiúsculo. David Gross, o embaixador dos Estados Unidos responsável

1 A Resolução 56/183 (21de dezembro de 2001) da Assembleia Geral da ONU aprovou a realização da Cúpula Mundial sobre a Sociedade da Informação (CMSI) em duas fases. A primeira fase aconteceu em Genebra de 10 a 12 de dezembro de 2003 e a segunda fase aconteceu em Túnis, de 16 a 18 de novembro de 2005. O objetivo da primeira fase era desenvolver e fomentar uma declaração clara de vontade política e de tomar medidas concretas para estabelecer as bases para uma sociedade da informação para todos, refletindo todos os diferentes interesses em jogo. Mais de 19 000 participantes de 174 países participaram do encontro e de eventos relacionados. Fonte: <http://www.itu.int/wsis/basic/about.html> [acessado em 21 de janeiro 2014].

2 A definição GTGI segue o padrão de definições utilizadas frequentemente na teoria de regimes. O fundador da teoria de regimes, Stephen D. Krasner, observa que: os regimes podem ser definidos como um conjunto de princípios implícitos ou explícitos, normas, regras e procedimentos de tomada de decisão em torno do qual as expectativas dos atores convergem em uma determinada área das relações internacionais. Princípios são crenças de fato, nexo de causalidade e retidão. Normas são padrões de comportamento definidos em termos de direitos e obrigações. Regras são prescrições ou proscrições de ação específicas. Procedimentos de tomada de decisão são as práticas em vigor para fazer e implementar a escolha coletiva. Krasner S (1983) Introduction, em International Regimes. Krasner SD (ed.), Cornell University Press: Ithaca, NY, EUA.

pela governança da Internet, manifestou sua preocupação de que a grafia minúscula proposta pela UIT poderia sinalizar a intenção de tratar a Internet como outros sistemas de telecomunicação internacionalmente regulados pela UIT. Outros interpretaram a questão como uma sinalização diplomática da intenção da UIT de desempenhar um papel mais proeminente na governança da Internet.[3]

Internet

O termo 'Internet' não abrange todos os aspectos existentes dos desenvolvimentos digitais globais. Outros dois termos – sociedade da informação e tecnologia da informação e da comunicação (TIC) – são geralmente apresentados como mais abrangentes. Estes incluem áreas fora do domínio da Internet, como a telefonia móvel. O argumento para o uso do termo 'Internet', no entanto, é reforçado pela rápida transição da comunicação global em direção ao uso do Protocolo da Internet (IP) como principal padrão técnico de comunicação. A já onipresente Internet continua expandindo-se a uma velocidade rápida, não somente em termos de número de usuários, mas também em termos dos serviços que oferece, notavelmente o protocolo de voz através da Internet (VoIP), que poderá tomar o lugar da telefonia convencional.

Governança

No debate sobre governança da Internet, especialmente na fase inicial da CMSI 2003, surgiu uma controvérsia com relação ao termo 'governança' e suas inúmeras interpretações. De acordo com uma das interpretações, governança é sinônimo de governo. Muitas delegações nacionais tinham este entendimento inicial, levando à interpretação de que a governança da Internet deveria ser assunto de governos e consequentemente abordada no nível intergovernamental com a participação limitada de outros atores, principalmente não relacionados ao Estado.[4] Esta interpretação colidiu com o significado mais amplo do termo 'governança', que inclui a governança dos assuntos

3 Shannon V (2006) What's in an 'i'? International Herald Tribune, 3 de dezembro de 2006. Acessível em: <http://www.nytimes.com/2006/12/03/technology/03iht-btitu.3755510.html> [acessado em 21 de janeiro de 2014].

4 A confusão tecnológica foi destacada pela forma como o termo "governança" foi usado por algumas organizações internacionais. Por exemplo, o termo "boa governança" tem sido utilizado pelo Banco Mundial para promover a reforma dos Estados ao introduzir maior transparência, reduzir a corrupção e aumentar a eficiência da administração. Neste contexto, o termo "governança" está diretamente relacionado às funções centrais do governo.

de qualquer instituição, incluindo instituições não governamentais. Este foi o significado aceito pelas comunidades da Internet, uma vez que descreve a forma como a Internet tem sido governada desde o seu início. A confusão terminológica se complicou ainda mais com a tradução do termo governance para outros idiomas. Em espanhol, o termo se refere basicamente a atividades públicas ou ao governo (gestión pública, gestión del sector público, e función de gobierno). A referência a atividades públicas ou ao governo também aparece no francês (gestion des affaires publiques, efficacité de l'administration, qualité de l'administration, e mode de gouvernement).

O português segue um padrão similar ao se referir ao setor público e ao governo (gestão pública e administração pública).

A evolução da governança da Internet

Início da governança da Internet (1970–1994)

A Internet teve início como um projeto de governo. No final da década de 60, o governo dos Estados Unidos financiou o desenvolvimento do Defense Advanced Research Project Agency Network (DARPA Net), recurso de comunicação eficiente. Por volta do meio da década de 70, com a invenção do TCP/IP (Transmission Control Protocol/Internet Protocol), esta rede evoluiu para o que hoje é conhecida como Internet. Um dos princípios fundamentais da Internet é sua natureza distribuída: pacotes de dados podem seguir caminhos diferentes através da rede, evitando barreiras tradicionais e mecanismos de controle. Este princípio tecnológico foi acompanhado de uma abordagem similar de regulação da Internet em suas fases iniciais: a Internet Engineering Task Force (IETF), estabelecida em 1986, conduziu o avanço do desenvolvimento da Internet por meio de um processo de tomada de decisão baseado na cooperação e no consenso, envolvendo uma extensa variedade de pessoas. Não havia governo central, nem planejamento central, e nenhum projeto grandioso.

Isso fez com que muitas pessoas pensassem que a Internet era, de alguma forma, única, e que poderia oferecer uma alternativa às políticas do mundo moderno. Na sua famosa Declaração da Independência do Ciberespaço, John Perry Barlow afirmou:

> [a Internet] é intrinsecamente extranacional, intrinsecamente antisoberana e a soberania [dos países] não é aplicável a nós. Temos que descobrir as coisas por conta própria.[5]

5 Barlow JP (1996) A declaration of the independence of cyberspace. Acessível em:<https://projects.eff.org/~barlow/Declaration-Final.html> [acessado em 21 de janeiro de 2014].

A guerra do DNS (1994–1998)

A abordagem descentralizada à governança da Internet logo começou a mudar quando os governos e o setor empresarial perceberam a importância da rede mundial. Em 1994, a US National Science Foundation, que administrou a estrutura-chave da Internet, decidiu terceirizar a administração do sistema de nomes de domínio (DNS) a uma empresa privada norte-americana denominada Network Solutions Inc. (NSI). Isso não repercutiu bem junto à comunidade da Internet, levando à chamada guerra do DNS.

Esta guerra introduziu novos atores no cenário: organizações internacionais e Estados nacionais. Ela terminou em 1998 com a criação de uma nova organização, a Corporação da Internet para Atribuição de Nomes e Números (ICANN - Internet Corporation for Assigned Names and Numbers), que se tornou o tema central da maioria dos debates sobre governança da Internet na atualidade.

Cúpula Mundial sobre a Sociedade da Informação (CMSI) (2003–2005)

A CMSI, realizada em Genebra (2003) e em Túnis (2005), colocou oficialmente a questão da governança da Internet na agenda diplomática. A prioridade da etapa de Genebra da cúpula, precedida por uma séria de Comitês Preparatórios (PrepComs) e reuniões regionais era bastante ampla, com uma gama de temas relacionados à informação e comunicação apresentados pelos participantes. Na verdade, durante as primeiras reuniões preparatórias e regionais, o termo 'Internet' não era usado, muito menos 'governança da Internet'.[6] A expressão governança da Internet foi introduzida ao processo da CMSI durante a reunião regional da Ásia Ocidental em fevereiro de 2003, após a cúpula de Genebra se tornar o assunto principal das negociações da CMSI.

Após longas negociações e acordos de última hora, a primeira cúpula CMSI em Genebra (dezembro de 2003) concordou com a criação do Grupo de Trabalho sobre Governança da Internet. O GTGI preparou um relatório que foi usado como base para as negociações na segunda cúpula CMSI realizada em Túnis (novembro de 2005). A Agenda da CMSI de Túnis para a Sociedade da Informação

6 Para a evolução do uso da palavra 'Internet' na preparação da CMSI: DiploFoundation (2003) The Emerging Language of ICT Diplomacy – Key Words. Acessível em <http://archive1.diplomacy.edu/IS/Language/html/words.htm> [acessado em 3 de agosto de 2014].

elaborou sobre a questão da governança da Internet, inclusive adotando uma definição, enumerando questões sobre governança da Internet e criando o Fórum de Governança da Internet (IGF), órgão multissetorial convocado pelo Secretário-Geral das Nações Unidas.

Acontecimentos de 2006

Após a cúpula de Túnis, três importantes acontecimentos e eventos marcaram o debate sobre governança da Internet em 2006. O primeiro foi a expiração do Memorando de Entendimento (MoU) existente e a elaboração de um novo memorando entre a ICANN e o Departamento de Comércio dos Estados Unidos. Alguns participantes esperavam que esse evento mudasse a relação entre a ICANN e o governo dos Estados Unidos e que o primeiro se tornasse um novo tipo de organização internacional. No entanto, enquanto o Memorando estreitava os laços entre a ICANN e o governo dos Estados Unidos, ao mesmo tempo mantinha a possibilidade de uma possível internacionalização do status da ICANN.

O segundo evento de 2006 foi o Fórum de Governança da Internet (IGF) em Atenas. Foi o primeiro Fórum do tipo e, em muitos aspectos, um experimento para a diplomacia multissetorial.

O IGF foi verdadeiramente um evento multissetorial, com a participação de países, empresas e a sociedade civil. Também contava com uma estrutura organizacional interessante para seus principais eventos e oficinas. Os jornalistas moderavam as discussões, fazendo com que o IGF se diferenciasse do formato comum de reunião da ONU. No entanto, alguns críticos alegaram que o IGF era apenas um talk show que não apresentava quaisquer resultados tangíveis por meio de um documento final ou de um plano de ação.

O terceiro principal acontecimento de 2006 foi a Conferência Plenipotenciária da UIT realizada em Antália, Turquia, em novembro. O novo Secretário-Geral da UIT, Dr. Hamadoun Touré, foi eleito. Ele anunciou prioridade maior à segurança cibernética e assistência ao desenvolvimento. Também era esperado que ele introduzisse novas modalidades à abordagem da UIT à governança da Internet.

Acontecimentos de 2007

Em 2007, a discussão da ICANN priorizou os domínios .xxx (para materiais adultos), reabrindo debates sobre inúmeros pontos de governança, inclusive se a ICANN deveria abordar somente problemas

técnicos ou também questões de relevância para políticas públicas.[7] Intervenções por parte dos Estados Unidos e de outros governos relativos a domínios .xxx levantaram ainda a questão de como os governos nacionais deveriam se envolver com as resoluções da ICANN. No segundo IGF, realizado em novembro, no Rio de Janeiro, o principal acontecimento foi a inclusão de recursos críticos de Internet (nomes e números) à agenda do IGF.

Acontecimentos de 2008

O maior acontecimento de 2008, que continuou influenciando a governança da Internet, bem como outras esferas políticas, foi a eleição de Barak Obama para Presidente dos Estados Unidos. Durante sua campanha eleitoral para presidente, o Presidente Obama usou a Internet e as ferramentas da Web 2.0 de forma intensa. Algumas pessoas até argumentam que esta era uma das razões de seu sucesso. Entre seus assessores estão muitas pessoas do setor da Internet, entre os quais o Presidente Executivo do Google. Além de sua consciência tecnológica, o Presidente Obama apoia o multissetorialismo que provavelmente influenciará as discussões sobre a internacionalização da ICANN e o desenvolvimento do regime de governança da Internet.

Em 2008, a neutralidade[8] da rede surgiu como uma das principais questões relacionadas à governança da Internet. O tema foi discutido principalmente nos Estados Unidos, entre dois principais blocos divergentes, tendo até se tornado assunto da campanha presidencial dos Estados Unidos, com o apoio do Presidente Obama. A neutralidade da rede é apoiada principalmente pela chamada indústria da Internet, incluindo empresas como Google, Yahoo! e Facebook.

A mudança na arquitetura da Internet, desencadeada por uma brecha na neutralidade da rede, pode colocar os negócios dessas empresas em perigo. Do outro lado estão as empresas de telecomunicações, como a Verizon e a AT&T, provedoras de serviços de Internet (ISP) e o setor multimídia. Por razões diversas, esses setores teriam interesse em algum tipo de diferenciação nos pacotes de navegação da Internet.

VER A SEÇÃO 2 PARA UMA DISCUSSÃO MAIS APROFUNDADA SOBRE A NEUTRALIDADE DA REDE

Outro grande acontecimento foi o rápido crescimento do Facebook e das redes sociais. Quando se trata de governança da Internet, o uso crescente das ferramentas 2.0 fizeram surgir questões sobre privacidade e proteção de dados no Facebook e em serviços similares.

7 Em junho de 2010, a ICANN aprovou o nome de domínio de topo .xxx para material adulto.

8 Para mais informações sobre neutralidade da rede, ver nosso vídeo explicativo em <https://www.youtube.com/watch?v=R-uMbZFfJVU> [acessado em 12 de fevereiro de 2014].

Acontecimentos de 2009

A primeira parte de 2009 viu o Cinturão de Washington tentando compreender as implicações e futuras direções das políticas relacionadas à Internet do Presidente Obama. Os seus compromissos com relação a questões fundamentais referentes à Internet não apresentaram nenhuma grande surpresa. O apoio do Presidente Obama a uma Internet aberta foi endossado e sua equipe também trabalhou pela implementação da neutralidade da rede em linha com as promessas feitas durante a campanha eleitoral.

O destaque de 2009 foi a conclusão da Afirmação de Compromissos entre a ICANN e o Departamento de Comércio dos Estados Unidos, cuja intenção era tornar a ICANN uma organização mais independente. Apesar de o compromisso ter resolvido alguns problemas de governança da Internet – a supervisão dos Estados Unidos sobre a ICANN – ele levantou diversas novas questões, como a posição internacional da ICANN e a supervisão de suas atividades. A Afirmação de Compromissos apresentou diretrizes, mas deixou muitas questões a serem resolvidas nos anos futuros.

Em novembro de 2009, o quarto IGF foi realizado em Sharm el Sheikh, Egito. O tema principal foi o futuro do IGF diante da revisão de seu mandato que seria feita em 2010. Em suas propostas, os participantes apresentaram diferentes pontos de vista sobre o futuro do IGF. Apesar de a maioria deles ter apoiado sua continuação, havia diferenças de opinião significativas sobre como o futuro do IGF deveria ser organizado. A China e muitos países em desenvolvimento defenderam uma maior base do IGF no sistema das Nações Unidas, o que implicaria em um papel mais proeminente por parte dos governos. Os Estados Unidos, a maior parte dos países em desenvolvimento, o setor empresarial e a sociedade civil defenderam a preservação do atual modelo do IGF.

Acontecimentos de 2010

O principal acontecimento de 2010 foi o impacto da mídia social em rápida expansão no debate sobre governança da Internet, inclusive a proteção da privacidade de usuários das plataformas de mídia social como o Facebook. Em 2010, o principal desenvolvimento na geopolítica da Internet foi o discurso da Secretária de Estado dos Estados Unidos, Hillary Clinton, sobre liberdade de expressão na Internet, mais espe-

cificamente com relação à China.[9] Os Estados Unidos e as autoridades chinesas discordaram sobre o acesso restrito às buscas no Google na China, levando ao encerramento das operações de busca do Google neste país.

Houve dois importantes acontecimentos no âmbito da ICANN. Primeiramente, houve a introdução de nomes de domínio com caracteres não ASCII para o árabe e o chinês. Ao resolver o problema do domínio de nomes em outros idiomas, a ICANN reduziu o risco de desintegração do DNS da Internet. Em segundo lugar, houve a aprovação da ICANN do domínio .xxx (materiais adultos). Com essa decisão a ICANN inevitavelmente firmou um compromisso nesse sentido ao adotar oficialmente uma decisão de alta relevância para políticas públicas na Internet. Anteriormente, a ICANN havia tentado permanecer, pelo menos formalmente, dentro do campo da tomada de decisões técnicas.

O processo de revisão do IGF começou em 2010 com a Comissão da ONU de Ciência e Tecnologia para o Desenvolvimento, que adotou a resolução a favor da continuação do Fórum, sugerindo sua continuação para os próximos cinco anos, somente com pequenas mudanças em sua organização e estrutura. Em julho de 2010, o Conselho Econômico e Social das Nações Unidas (ECOSOC) endossou esta resolução. A Assembleia Geral das Nações Unidas decidiu no período de setembro-novembro de 2010 por continuar com o IGF pelos próximos cinco anos (2011-2015).

Acontecimentos de 2011

Em 2011, o desenvolvimento geral mais importante foi a maior relevância da governança da Internet nas agendas políticas globais. A relevância da governança da Internet se aproximou das questões diplomáticas, como mudança climática, migração e segurança alimentar. Outra consequência da crescente relevância política da Internet é a mudança gradual da cobertura nacional de questões relacionadas à governança da Internet, dos ministérios de tecnologia (TI, telecomunicações) para ministérios da esfera política (diplomacia, gabinetes de primeiros-ministros). Além disso, a mídia global de maior destaque (por exemplo, The Economist, IHT, Al Jazeera, a BBC) passou a acompanhar os progressos da governança da Internet com mais interesse do que nunca.

A governança da Internet foi afetada pela Primavera Árabe. Apesar dos

9 Clinton H (2010) Comentários sobre a liberdade na Internet. Acessível em <http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm> [acessado em 21 de janeiro de 2014].

diversos pontos de vistas sobre o impacto da Internet no fenômeno da Primavera Árabe (desde impacto mínimo até essencial), uma consequência é certa: a mídia social agora é vista como uma ferramenta decisiva da vida política moderna. Sob diversas formas, a Internet– e sua governança – fez-se presente nos radares políticos de todo o mundo nesse ano.

Em 27 de janeiro, as autoridades egípcias cortaram o acesso à Internet na vã esperança de parar os protestos políticos. Este foi o primeiro apagão total sofrido pela Internet em um país inteiro ordenado pelo governo. Anteriormente, mesmo no caso de conflitos militares (ex-Iugoslávia, Iraque), a comunicação via Internet nunca havia sido completamente cortada.

A iniciativa de Hillary Clinton com relação à liberdade de expressão na Internet, iniciada com o seu discurso de fevereiro de 2010, avançou em 2011. Houve duas importantes conferências sobre o assunto: a Conferência de Viena sobre Direitos Humanos e a Internet e a Conferência de Haia sobre Internet e Liberdade.

Em 2011, a ICANN continuou fazendo sua autocrítica por meio das seguintes ações:

- Implementação de uma reforma administrativa.
- Preparativos políticos finais para a introdução de domínios genéricos de topo (gTLDs).
- A demissão de seu Diretor-Presidente e a procura por um substituto.

O ano de 2011 também foi marcado por uma abundância de princípios de governança da Internet propostos pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE), o Conselho da Europa, a União Europeia, o Brasil e outros atores. As inúmeras convergências destes princípios poderiam ser o ponto de partida para um futuro preâmbulo da declaração global da Internet ou documento similar que poderia servir de estrutura para o desenvolvimento da governança da Internet.

Acontecimentos de 2012

Dois grandes eventos marcaram a agenda de 2012 devido com importantes consequências para os anos seguintes: a mudança na liderança da ICANN e a revisão das Regulações Internacionais de Telecomunicação (ITRs).

A ICANN passou por avanços significativos em 2012 com a introdução dos novos Domínios genéricos de Topo (gTLDs). Apesar de alguns pro-

blemas com o processo de registro (falhas no software, controvérsias sobre processos normativos), mais de 1900 pedidos para novos gTLDs foram recebidos e avaliados. Além disso, o novo Diretor-Presidente, Fadi Chehadé, contribuiu com uma nova abordagem à direção dos processos normativos multissetoriais. Em seu discurso à sociedade civil na ICANN 45, ele traçou algumas melhorias promissoras, inclusive o desenvolvimento da multissetorialismo responsável, o franco reconhecimento de problemas, a escuta ativa, a orientação empática, a busca por compromisso, etc.

A Conferência Mundial de Telecomunicações Internacionais WCIT ocorreu em Dubai, em dezembro de 2012, para alterar as ITRs pela primeira vez desde 1988. Ela provocou o debate sobre o impacto da nova regulação sobre o futuro da Internet. Ao final de uma conferência cansativa de duas semanas, as negociações terminaram em um impasse: os participantes não conseguiram chegar a um consenso sobre o texto alterado, deixando o debate em aberto para futuras reuniões. O principal ponto de discórdia foi uma resolução não vinculativa sobre o incentivo ao papel da UIT na governança da Internet, polarizando os países participantes em dois blocos: os países ocidentais eram a favor do atual modelo multissetorial, ao passo que os defensores da resolução, entre os quais países como a China, a Rússia e os países árabes, pendiam para o modelo intergovernamental.

Outros acontecimentos de destaque ocorreram na área de diretos de propriedade intelectual, nos quais a mobilização e os protestos de usuários da Internet conseguiram travar regulamentos nacionais (SOPA - Stop Online Piracy Act, nos Estados Unidos) e internacionais (ACTA - Anti- Counterfeiting Trade Agreement) que teriam afetado os direitos legítimos dos usuários com sua implementação.

Acontecimentos em 2013

O principal acontecimento nas políticas digitais globais foram as revelações de Edward Snowden sobre diversos programas de vigilância executados pela Agência de Segurança Nacional dos Estados Unidos (NSA) e outras agências. As revelações de Snowden fizeram com que o público global se interessasse em saber de que forma a Internet é governada. A questão central era a proteção de dados e os direitos de privacidade.

A questão da proteção da privacidade foi abordada por muitos líderes durante a Assembleia Geral das Nações Unidas. A resolução da AGNU deu início a um novo processo normativo sobre privacidade online. A

questão será aprofundada em 2014 no Conselho de Direitos Humanos das Nações Unidas.

Em outubro de 2013, a presidente do Brasil, Dilma Rousseff, e o presidente da ICANN, Fadi Chehadi, iniciaram o processo NETmundial. A governança da Internet foi debatida com destaque em inúmeras conferências acadêmicas e atividades de pesquisa em think-tanks ao redor do mundo.

PREFIXOS: e- / VIRTUAL / CIBER / DIGITAL/NET

Os prefixos e- / virtual / ciber / digital / net são usados para descrever os diversos desenvolvimentos referentes à TIC/Internet. São usados de forma intercambiável. Cada prefixo descreve o fenômeno da Internet.

Mesmo assim, costumamos usar e- para comércio, ciber para crime e segurança, digital para níveis desiguais de desenvolvimento e virtual para moedas, como o Bitcoin. Padrões de uso começaram a surgir. Enquanto na linguagem do dia a dia a escolha pelos prefixos e- / virtual/ ciber / digital / net é algo casual, na política da Internet o uso de prefixos começou a agregar mais significado e relevância.

Vamos dar uma rápida olhada na etimologia destes termos e a maneira como são usados nas políticas para Internet.

A etimologia de "ciber" remonta à Grécia Antiga e significa "governar". Este termo foi introduzido na nossa época no livro Cibernética de Norbert Weiner, que abordava o tema da governança baseada em informações. Em 1984, William Gibson cunhou o termo ciberespaço no romance de ficção científica Neuromancer. O aumento do uso do prefixo "ciber" acompanhou a expansão da Internet. No final dos anos 90, praticamente qualquer coisa relacionada à internet era "ciber": cibercomunidade, ciberdireito, cibersexo, cibercrime, cibercultura, ciber.... era só nomear algo na Internet e o termo "ciber" vinha junto.

No início dos anos 2000, esse termo começou a desaparecer gradualmente do uso mais amplo e sua utilização foi preservada apenas em terminologias relacionadas à segurança.

O termo ciber foi usado para designar a Convenção sobre o Cibercrime do Conselho da Europa de 2001, que continua sendo o único tratado internacional no campo da segurança da Internet. Hoje, existe a Estratégia para o Ciberespaço dos Estados Unidos, a Agenda Global de Cibersegurança da UIT, a política de ciberdefesa da OTAN, O Centro de Excelência em Ciberdefesa da Estônia.

O autor ciberpunk e colunista da Wired, Bruce Sterling, declarou:

Acho que sei por que os militares usam o termo "ciber". É porque a metáfora de defender um "campo de batalha" que consiste de espaço "ciberespaço" facilita para determinados fornecedores a obtenção de subsídios do Pentágono. Se você usa o termo "ciberespaço" sob a perspectiva alternativa de "redes, fios, tubos e cabos", nesse caso a NSA já se torna proprietária dele por 50 anos e as forças armadas não podem

Prefixos: e- / virtual / ciber / digital. [10]

"E" é a abreviação de "eletrônico". O seu primeiro e principal uso se deu na esfera do comércio eletrônico, como uma descrição da incipiente comercialização via Internet. Na Agenda de Lisboa da União Europeia (2000), e- foi o prefixo mais usado. E- também foi o prefixo mais usado nas declarações da CMSI (Genebra 2003; Túnis 2005). A implementação de acompanhamento da CMSI priorizou linhas de ação que incluíam e-governo, e-negócios, e-ensino, e-saúde, e-emprego, e-agricultura e e-ciência. Mesmo assim, o prefixo e- não é mais tão presente quanto antes. Até mesmo a UE abandonou seu uso recentemente, provavelmente na tentativa de se distanciar do fracasso da sua Agenda de Lisboa.

Hoje, a EU possui uma Agenda Digital para a Europa. [11] Digital se refere a "1" e "0" – dois dígitos que são a base de toda a Internet. No fim, todo software e programa começa com esses dígitos. No passado, o termo digital era principalmente usado em círculos de desenvolvimento para representar a exclusão digital. Nos últimos anos, ele começou a ganhar espaço na terminologia linguística da Internet. Provavelmente continuará sendo o principal prefixo usado para a Internet. J-C Juncker, presidente eleito da Comissão Europeia usou o termo 'digital' 10 vezes em seu discurso no Parlamento Europeu, apresentando seu plano de políticas para os próximos cinco anos. Além da UE, a Grã Bretanha adotou a diplomacia digital.

Virtual está relacionado à natureza intangível da Internet, introduzindo a ambiguidade em ser tanto intangível quanto, potencialmente, não existente. A realidade virtual pode ser tanto uma realidade intangível (algo que não se pode tocar) quanto uma realidade que não existe (uma realidade falsa). Acadêmicos e pioneiros da Internet usavam o termo virtual para enfatizar a novidade que era a Internet, bem como o surgimento de um "admirável mundo novo". O termo virtual, devido a sua ambiguidade, raramente aparece na linguagem de políticas e documentos internacionais. Hoje, existe uma trégua na guerra pela dominância do prefixo.

Cada prefixo conquista seu próprio espaço, sem a denominação abrangente que, por exemplo, o termo ciber tinha no final dos anos 90. Hoje, ciber preserva sua dominância em assuntos relacionados à segurança. E- ainda é usado para negócios. O uso do termo digital evoluiu de questões de desenvolvimento para um uso mais abrangente pelo setor da administração pública. Virtual foi praticamente abandonado.

10 Newitz A (2013) The bizarre evolution of the word 'cyber'. Acessível em <http://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487> [acessado em 3 de agosto de 2014].

11 Comissão Europeia (sem data) Uma Agenda Digital para a Europa. Acessível em <http://ec.europa.eu/digital-agenda/> [acessado em 3 de agosto de 2014]

Ferramentas Cognitivas de Governança da Internet

Verdades profundas são reconhecidas pelo fato de que seu inverso também é uma verdade profunda, em oposição às trivialidades, cujos inversos são obviamente um absurdo.
Niels Bohr, Físico Nuclear (1885–1962)

As Ferramentas Cognitivas de Governança da Internet é um conjunto de instrumentos que servem para o desenvolvimento e a compreensão da argumentação política. O ponto central deste conjunto de ferramentas consiste em um quadro de referência que inclui percepções das relações de causa e efeito, formas de raciocínio, valores, terminologia e jargão. Este quadro de referência é bastante relevante na vida política, definindo de que forma questões específicas são apresentadas e quais são as medidas tomadas.

Em muitos casos, o quadro de referência comum é influenciado pela cultura profissional específica (os padrões de conhecimento e cultura compartilhados por membros da mesma profissão). A existência de tal quadro geralmente ajuda a facilitar uma melhor comunicação e entendimento. Também pode ser usado para proteger determinado campo profissional e prevenir influências externas. Em citação ao linguista norte-americano Jeffrey Mirel: "Todas as linguagens profissionais são uma língua específica". [12]

O regime de governança da Internet é complexo, uma vez que envolve muitas questões, atores, mecanismos, procedimentos e instrumentos. A figura 1, inspirada pelo artista holandês MC Escher, mostra alguns pontos de vista paradoxais associados à governança da Internet.

A caixa de ferramentas reflete a natureza da governança da Internet, sob a forma de uma área normativa conhecida como perversa, caracterizada pela dificuldade encontrada na atribuição de causalidade para o desenvolvimento de políticas para um raciocínio específico. Em muitos casos, os problemas são sintoma de outro problema, às vezes criando círculos viciosos. Certas abordagens cognitivas, como a abordagem linear, monocausal e ambos/ou o pensamento têm uma utilidade muito limitada no campo da governança da Internet, que é muito complexa para ficar presa a

12 Citado em Helfand D (2001) Edpseak is in a class by itself. Los Angeles Times, 16 de agosto. Acessível em <http://articles.latimes.com/2001/aug/16/news/mn-34814> [acessado em 13 de fevereiro de 2014].

um molde rígido de coerência, não contradição e consistência. A flexibilidade, bem como estar aberto e preparado para o inesperado, talvez sejam a melhor parte da Internet.[13]

Assim como o processo de governança, a caixa de ferramentas também é um fluxo. Abordagens, padrões e analogias surgem e desaparecem dependendo de sua relevância conjuntural no processo normativo. Sustentam narrativas normativas específicas no debate sobre a governança da Internet.

Figura 1

Abordagens e padrões

Inúmeras abordagens e padrões apareceram gradualmente, representando pontos onde as diferenças sobre posições de negociação, bem como sobre culturas profissionais e nacionais podem ser identificadas. A identificação de abordagens e padrões comuns podem reduzir a complexidade das negociações e ajudar a criar um quadro de referência comum.

13 Esta seção não teria sido concretizada sem a discussão com Aldo Matteucci, membro sênior da Diplo, cujas visões "contestadoras" sobre questões da governança moderna são uma permanente constatação da realidade referente às atividades de ensino e pesquisa da Diplo.ção não teria sido concretizada sem a discussão com Aldo Matteucci, membro sênior da Diplo, cujas visões "contestadoras" sobre questões da governança moderna são uma permanente constatação da realidade referente às atividades de ensino e pesquisa da Diplo.

Abordagem limitada x ampla

A abordagem limitada prioriza a infraestrutura da Internet (DNS, IP, números e servidores-raiz) e o posicionamento da ICANN como um ator importante neste campo. De acordo com a abordagem ampla, as negociações referentes à governança da Internet devem ir além das questões de infraestrutura e abordar outras questões jurídicas, econômicas, de desenvolvimento e socioculturais. Esta última abordagem é adotada no relatório conclusivo da WGIG, sendo também usada como princípio estruturante da arquitetura do IGF.

Coerência técnica e de políticas

Um desafio significativo do processo de governança da Internet tem sido a integração dos aspectos técnico e normativo, uma vez que é difícil fazer uma distinção clara entre os dois. As soluções técnicas não são neutras. No fim, cada solução/opção técnica promove determinados interesses, fortalece determinados grupos e, até certo ponto, afeta a vida social, política e econômica. No caso da Internet, por um bom tempo, tanto o aspecto técnico quanto o aspecto normativo eram regulados por apenas um grupo social – a incipiente comunidade da Internet.

Com o crescimento da Internet e o surgimento de novos atores de governança da Internet – principalmente o setor empresarial e governos – tornou-se difícil para a comunidade da Internet manter a cobertura integrada de questões técnica e normativas sob apenas um teto. As reformas subsequentes, entre as quais a criação da ICANN, tentaram reestabelecer a coerência entre os aspectos técnico e normativo. Esta questão permanece aberta e, conforme esperado, tem se revelado um dos tópicos polêmicos do debate sobre o futuro da governança da Internet.

Abordagem antigo "real" x novo "ciber"

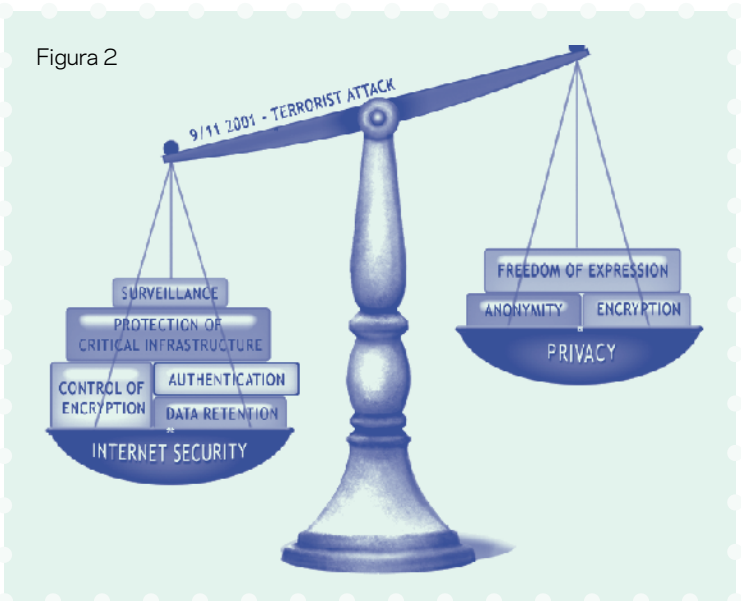
Existem duas abordagens para praticamente qualquer questão de governança da Internet (Figura 2). A abordagem antigo "real" argumenta que a Internet não contribuiu com nada de novo no campo da governança. É somente mais um dispositivo novo, do ponto de vista da governança, sem nenhuma diferença com relação a seus precursores: o telégrafo, o telefone e o rádio.

Por exemplo, em discussões jurídicas, esta nova abordagem argumenta que as leis existentes podem ser aplicadas à Internet com alterações mínimas apenas. Na esfera econômica, essa abordagem argumenta

que não há diferença entre o comércio comum e o comércio eletrônico. Consequentemente, não existe necessidade de tratamento jurídico específico para o comércio eletrônico.

A abordagem novo "ciber" argumenta que a Internet é um sistema de comunicação essencialmente diferente dos anteriores. A principal premissa da abordagem ciber é que a Internet conseguiu desconectar a nossa realidade social e política do mundo dos Estados soberanos (separados geograficamente). O ciberespaço é diferente do espaço real e requer uma forma de governança diferente. No campo jurídico, a escola cibernética de pensamento argumenta que as leis existentes de jurisdição, crime cibernético e contratos não podem ser aplicadas à Internet e que é necessário criar novas leis. Cada vez mais, a abordagem velho-real está se tornando proeminente tanto no campo regulatório quanto no campo normativo.

Figura 2



Estrutura descentralizada x centralizada de governança da Internet

De acordo com a visão descentralizada, a estrutura de governança da Internet deveria refletir a própria natureza da Internet: a rede das redes. Este ponto de vista salienta que a Internet é tão complexa que não pode ser colocada sob uma única governança, como por exemplo

uma organização internacional, e que a governança descentralizada é um dos principais fatores que possibilitam o crescimento da Internet. Esse ponto de vista é basicamente apoiado pela comunidade técnica da Internet e por países desenvolvidos.

A abordagem centralizada, por outro lado, baseia-se parcialmente na dificuldade prática de países com recursos humanos e financeiros limitados para o acompanhamento das discussões sobre a governança da Internet em um cenário altamente descentralizado e pluri institucional. Tais países têm dificuldade em comparecer às reuniões nos principais centros diplomáticos (Genebra, Nova York), sem mencionar o acompanhamento das atividades de outras instituições, como a ICANN, o W3C (World Wide Web Consortium) e a IETF. Esses países, em sua maioria em desenvolvimento, defendem um único ponto de cobertura (one-stop-shop), preferencialmente dentro da estrutura de uma organização internacional.

Proteção dos interesses públicos na Internet

VER A SEÇÃO 2 PARA UMA DISCUSSÃO MAIS APROFUNDADA SOBRE A NEUTRALIDADE DA REDE

Uma das principais qualidades da Internet é sua natureza pública, que possibilitou sua rápida expansão e que incentiva criatividade e inclusão. A forma de proteger a natureza pública da Internet continuará sendo um dos temas centrais do debate sobre governança da Internet. Este problema é especialmente complicado porque uma parte significativa da infraestrutura básica da Internet – desde plataformas transcontinentais até redes de área local – é privada. A possibilidade ou não de proprietários particulares serem requisitados para administrar esta propriedade junto ao interesse público e quais partes da Internet podem ser consideradas globais são algumas das difíceis questões que precisam ser abordadas. A questão da natureza pública da Internet foi reaberta com o debate sobre a neutralidade da rede.

Geografia e Internet

Uma das primeiras premissas a respeito da Internet era que ela ultrapassava fronteiras nacionais e minava o princípio da soberania. Com a comunicação via Internet facilmente transcendendo fronteiras nacionais e o anonimato do usuário incorporado à própria concepção da Internet, pareceu para muitos, para citar a famosa *Declaração da Independência do Ciberespaço,*[5] que os governos "não tinham direito moral de nos governar (os usuários) nem "quaisquer métodos de coerção a que tenhamos reais motivos para temer". Os avanços tecnológicos do passado recente entre os quais softwares mais sofisti-

cados de geolocalização, desafiam cada vez mais a perspectiva do fim da geografia na era da Internet.

Hoje, ainda é difícil identificar exatamente quem está por trás da tela, mas é razoavelmente simples identificar sua localização geográfica. Quanto mais a Internet se baseia na geografia, menos singular é sua governança. Por exemplo, com a possibilidade de localizar geograficamente usuários da Internet e transações via Internet, a complexa questão acerca da jurisdição na Internet pode ser resolvida pelas leis existentes.

Incerteza política

A tecnologia da Internet se desenvolve muito rapidamente. Novos serviços são introduzidos quase que diariamente, criando dificuldades adicionais na organização do debate sobre governança da Internet. Por exemplo, em novembro de 2005, quando a o atual acordo de governança da Internet foi negociado na CMSI na Tunísia,[14] o Twitter não existia. Hoje, o Twitter é responsável por levantar algumas das principais questões acerca da governança da Internet, como proteção da privacidade, liberdade de expressão e proteção da propriedade intelectual.

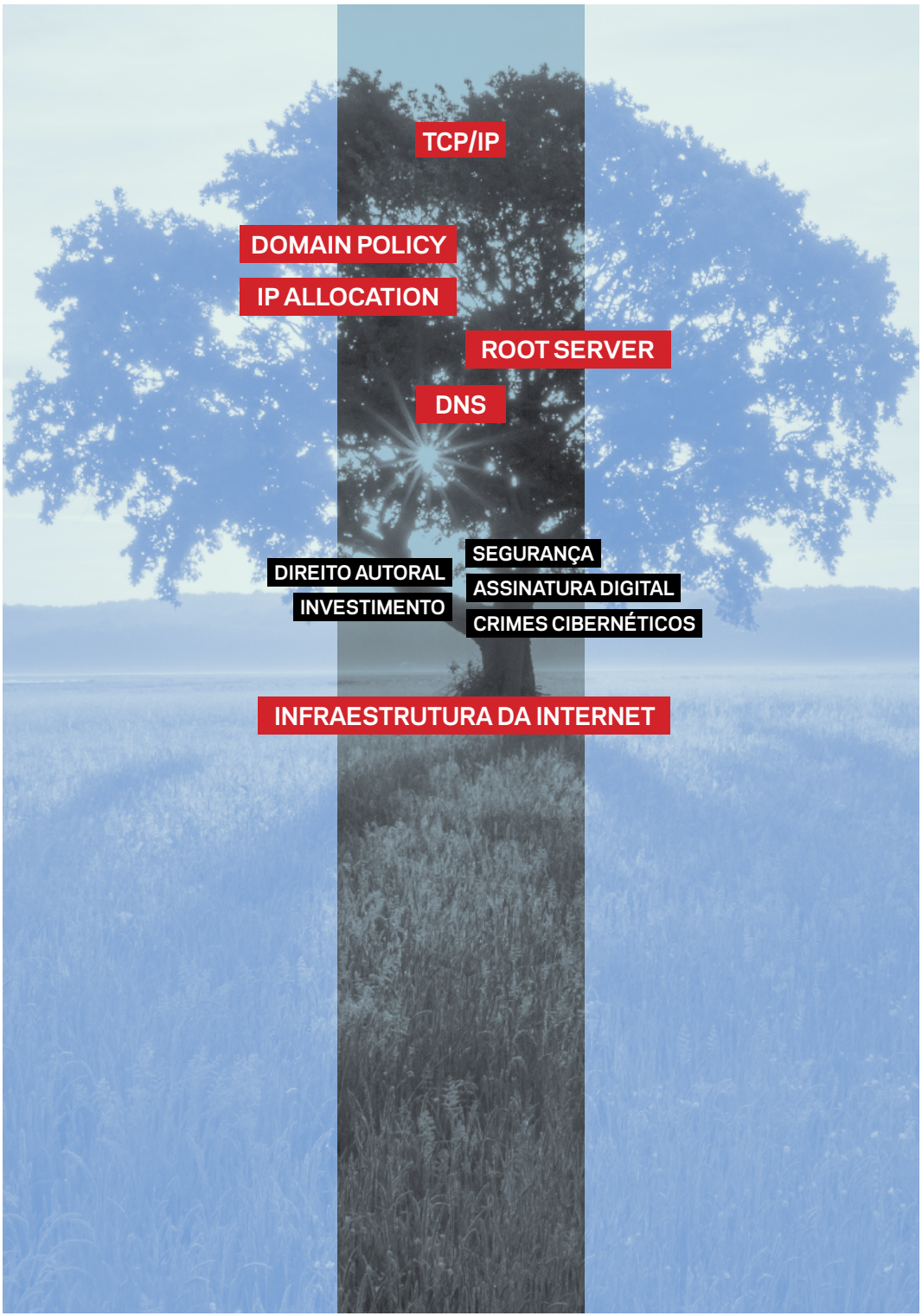
Outro exemplo das rápidas mudanças da tecnologia é a relevância do spam. Em 2005, ele era um dos principais problemas sobre governança. Hoje, graças à tecnologia de filtragem altamente sofisticada, o spam é um problema de menor importância de governança da Internet.

O equilíbrio político

O equilíbrio talvez seja o panorama mais adequado para os debates sobre governança e políticas da Internet. Em muitas questões sobre governança da Internet, é necessário estabelecer um equilíbrio entre vários interesses e abordagens. A definição deste equilíbrio é com frequência a base para o consenso. As áreas onde é possível encontrar tal equilíbrio entre as políticas incluem:

> **Liberdade de expressão x proteção da ordem pública:** o conhecido debate entre o Artigo 19 (liberdade de expressão) e o Artigo 27 (proteção da ordem pública) da Declaração Universal dos Direitos Humanos foi estendido à Internet; e é frequentemente discutido dentro do contexto do controle de conteúdo e censura na Internet.

14 O processo da CMSI teve início com a primeira reunião preparatória realizada em julho de 2002 em Genebra. A primeira cúpula aconteceu Genebra (dezembro de 2003) e a segunda cúpula aconteceu em Túnis (novembro de 2005).


TCP/IP
DOMAIN POLICY
IP ALLOCATION
ROOT SERVER
DNS
SEGURANÇA
DIREITO AUTORAL
ASSINATURA DIGITAL
INVESTIMENTO
CRIMES CIBERNÉTICOS
INFRAESTRUTURA DA INTERNET

VER A SEÇÃO 2
PARA UMA DISCUSSÃO MAIS APROFUNDADA SOBRE A CIBERSEGURANÇA

Cibersegurança x privacidade: assim como a segurança na vida real, a cibersegurança pode colocar em perigo alguns direitos humanos, como o direito à privacidade. O equilíbrio entre cibersegurança e privacidade está sempre mudando, dependendo da situação política global. Após o 11 de setembro, com a securitização da agenda global, o equilíbrio passou a pender para o lado da cibersegurança.

VER A SEÇÃO 3
PARA UMA DISCUSSÃO MAIS APROFUNDADA SOBRE A PROPRIEDADE INTELECTUAL

Propriedade intelectual – proteção dos direitos do autor x uso justo de materiais: outro dilema jurídico "real" da lei que assumiu uma nova perspectiva no mundo online.

Muitos criticam estes "pares contrabalanceadores", considerando-os falsos dilemas. Por exemplo, existem fortes argumentos de que cibersegurança não necessariamente significa menos privacidade. Existem abordagens em busca do aprimoramento tanto da cibersegurança quanto da privacidade. Embora esses pontos de vista sejam defendidos com fortes justificativas, a realidade da política de governança da Internet é de que ela é definida pelas opções de políticas "binárias" anteriormente citadas.

Não é preciso reinventar a roda

Qualquer iniciativa no campo da governança da Internet deveria começar a partir das regras existentes, que podem ser divididas em três grupos abrangentes:

- regras inventadas para a Internet (ex., ICANN);
- regras que precisam de alterações relevantes para tratar das questões relacionadas à Internet (ex., proteção de marcas registradas, tributação); e
- regras que podem ser aplicadas à Internet sem alterações significativas (ex., proteção da liberdade de expressão).

O uso das regras existentes elevaria de forma significativa a estabilidade jurídica e reduziria a complexidade do desenvolvimento do regime de governança da Internet.

Se não quebrou, não conserte

A governança da Internet deve manter a funcionalidade e solidez atual da Internet e ao mesmo tempo permanecer flexível o suficiente para adotar mudanças em busca de maior funcionalidade e maior legitimidade. O consenso geral reconhece que a estabilidade e funcionalidade da Internet deveriam constituir-se em um dos princípios orientadores de sua governança.

A estabilidade da Internet deveria ser preservada por meio da abordagem inicial da Internet do "código de execução", que envolve a introdução gradual de mudanças extensivamente testadas na infraestrutura técnica. No entanto, alguns atores se preocupam com o fato de que o uso do lema "se não quebrou, não conserte" levaria à proteção geral contra quaisquer mudanças na atual governança da Internet, inclusive mudanças não necessariamente relacionadas à infraestrutura técnica. Uma solução é usar este princípio como critério para a avaliação de decisões específicas relacionadas à governança da Internet (ex., a introdução de novos protocolos e mudanças nos mecanismos de tomada de decisão).

Incentivo a uma abordagem holística e à priorização

Uma abordagem holística deveria facilitar a abordagem tanto do aspecto técnico quanto dos aspectos jurídico, social, econômico e evolutivo do desenvolvimento da Internet.

Esta abordagem também deveria levar em consideração a crescente convergência da tecnologia digital, inclusive a migração de serviços de telecomunicação para ISPs.

Ao mesmo tempo em que mantêm uma abordagem holística das negociações acerca da governança da Internet, os atores participantes deveriam identificar questões prioritárias de acordo com seus interesses particulares. Os países em desenvolvimento e os países desenvolvidos não constituem grupos homogêneos.

Entre os países em desenvolvimento existem diferenças consideráveis de prioridades, nível de desenvolvimento e disponibilidade de TI (ex., entre países com TIC avançadas, como Índia, China e Brasil e alguns dos países menos desenvolvidos da África Subsaariana.

A abordagem holística e a priorização da agenda de governança da Internet deveriam ajudar os atores participantes de países desenvolvidos e em desenvolvimento a priorizar um conjunto específico de questões. Isso deveria levar a negociações mais significativas e possivelmente menos politizadas. Os atores participantes se reuniriam ao redor de questões em vez de divisões políticas tradicionais (ex., países desenvolvidos – países em desenvolvimento, governos – sociedade civil).

O princípio da neutralidade tecnológica

De acordo com o princípio da neutralidade tecnológica, as políticas não deveriam ser elaboradas para dispositivos tecnológicos e técni-

cos específicos. Por exemplo, as regras de proteção da privacidade deveriam especificar o que deve ser protegido (ex., dados pessoais, documentos médicos) e não como deveria ser protegido. O uso do princípio da neutralidade tecnológica faz com que alguns instrumentos de privacidade e proteção de dados, como as diretrizes da OCDE desde 1980, sejam tão relevantes hoje quanto eram antigamente.

VER A SEÇÃO 2 PARA UMA DISCUSSÃO MAIS APROFUNDADA SOBRE A NEUTRALIDADE DA REDE

A neutralidade tecnológica oferece muitas vantagens de governança. Garante a continuidade da governança independentemente de futuros avanços tecnológicos e possível convergência das principais tecnologias (telecomunicação, mídia, a Internet, etc). A neutralidade tecnológica é diferente da neutralidade da rede: a primeira indica que uma política específica é independente da tecnologia que regula; a segunda prioriza principalmente a neutralidade do tráfego na rede.

Faça com que as soluções tecnológicas implícitas tornem explícitos os princípios de políticas

Um ponto de vista geralmente defendido na comunidade da Internet é que determinados valores sociais, como a comunicação livre, são facilitados pela forma como a Internet é tecnologicamente abordada. Por exemplo, o princípio da neutralidade da rede, de acordo com o qual a rede deveria simplesmente transmitir dados entre dois pontos terminais em vez de introduzir intermediários é frequentemente reconhecido como uma garantia de liberdade de expressão na Internet. Este ponto de vista poderia levar à conclusão errônea de que soluções tecnológicas são suficientes para promover e proteger valores sociais. Os avanços mais recentes na Internet, como o uso de tecnologias firewall para a restrição do fluxo de informações comprovam que a tecnologia pode ser usada de muitas maneiras aparentemente contraditórias. Sempre que possível, os princípios como a livre comunicação deveriam ser claramente afirmados em nível de políticas e não implicitamente supostos no nível técnico. As soluções tecnológicas deveriam fortalecer os princípios de políticas, mas não deveriam ser a única maneira de promovê-los.

Evite o risco de fazer a sociedade funcionar por meio de códigos de programadores

Um elemento essencial da relação entre tecnologia e políticas foi identificado por Lawrence Lessig, que observou que, com a crescente dependência na Internet, a sociedade moderna pode acabar sendo regulada por códigos de software em vez de normas legais. Por fim,

algumas funções legislativas do parlamento e do governo podem de fato ser assumidas por empresas de informática e desenvolvedores de software. Por meio da combinação de software e soluções técnicas, elas seriam capazes de influenciar a vida em sociedades cada vez mais baseadas na Internet. Se o funcionamento da sociedade por meio de códigos em vez leis um dia se tornasse realidade, desafiaria significativamente a própria base da organização política e jurídica da sociedade moderna.

Analogias

Apesar de a analogia ser frequentemente enganadora, é a coisa menos enganadora que temos.
Samuel Butler, Poeta Britânico (1835–1902)

A analogia nos ajuda a entender novos progressos ao se referir ao que já é conhecido. Desenhar paralelos entre exemplos passados e atuais, apesar dos riscos, é um dos principais processos cognitivos no direito e na política. A maioria das ações judiciais referentes à Internet é resolvida por meio de analogias, principalmente no sistema jurídico anglo-saxão baseado em precedentes. O uso de analogias na governança da Internet tem algumas limitações importantes.

Primeiramente, "Internet" é um termo amplo, que engloba uma variedade de serviços, entre os quais e-mail (análogo ao telefone), serviços web (análogos aos serviços de radiodifusão – televisão) e bancos de dados (análogos às bibliotecas). A analogia a qualquer aspecto específico da Internet talvez simplifique em excesso o entendimento da Internet.

Em segundo lugar, com a crescente convergência de diferentes serviços de telecomunicação e mídia, as tradicionais diferenças entre os vários serviços estão difusas. Por exemplo, com a introdução do VoIP, está cada vez mais difícil traçar uma distinção clara entre Internet e telefonia. Apesar destes fatores limitantes, a analogia ainda é um elemento poderoso; ainda é a principal ferramenta cognitiva para resolver ações judiciais e desenvolver um regime de governança da Internet.

Internet – telefonia

Semelhanças: quando a Internet estava em seu início, a analogia era influenciada pelo fato de que o telefone era usado para acesso

discado à Internet. Além disso, uma analogia funcional é válida entre o telefone e a Internet (correio eletrônico e bate papo), ambos sendo meios para a comunicação direta e pessoal.

Diferenças: a Internet usa pacotes em vez de circuitos (o telefone). Diferentemente do telefone, a Internet não consegue garantir serviços; ela só consegue garantir "melhores esforços". A analogia enfatiza apenas um aspecto da Internet: comunicação via correio eletrônico ou bate papo. Outros importantes aplicativos da Internet, como a World Wide Web, serviços interativos etc, não possuem elementos em comum com a telefonia.

Usado por: esta analogia é usada por aqueles que são contra a regulação do conteúdo da Internet (principalmente nos Estados Unidos). Se a Internet for análoga ao telefone, o conteúdo da comunicação via Internet não pode ser controlado legalmente ao contrário de – por exemplo – a radiodifusão. Também é usada por aqueles que defendem que a Internet deveria ser regulada como quaisquer outros sistemas de comunicação (ex., telefonia, correio) por autoridades nacionais, desempenhando o papel de coordenação das organizações internacionais, como a UIT. De acordo com essa analogia, o DNS da Internet deveria ser organizado e gerenciado da mesma forma que o sistema de numeração telefônica.[15]

Uma nova virada nesta complexa analogia foi criada via VoIP (ex., Skype) que desempenha a função do telefone ao mesmo tempo em que usa protocolos de Internet. Esta dicotomia fez surgir uma controvérsia na Conferência Mundial de Telecomunicações Internacionais (CMTI) de 2012, em Dubai. A atual visão de que o VoIP é um serviço de Internet é contestado por aqueles que argumentam que ela deveria ser regulamentada da mesma forma que foi o serviço de telefonia, tanto em nível nacional quanto internacional, o que inclui um papel mais proeminente para a UIT.

Internet – mensagem/correio

Semelhanças: Esta é uma analogia funcional, a saber, o envio de mensagens. O nome em si, e-mail, enfatiza esta semelhança.

15 Volker Kitz defende a analogia entre os nomes e números da administração dos sistemas de telefonia e da Internet. Kitz V (2004) ICANN may be the only game in town, but Marina del Rey isn't the only town on Earth: Some thoughts on the so-called uniqueness of the Internet. Acessível em <http://studentorgs.law.smu.edu/Science-and-Technology-Law-Review/Articles/Fall-2005/Kitz.aspx> [acessado em 21 de janeiro de 2014].

Diferenças: esta analogia abrange apenas um serviço da Internet: o e-mail. Além disso, o serviço postal tem uma estrutura intermediária muito mais elaborada entre o remetente e o destinatário que o sistema de e-mail, no qual a função intermediária ativa é desempenhada pelos ISPs ou por um provedor de serviço de e-mail como o Yahoo! ou o Hotmail.

Usada por: a Convenção Postal Universal traça esta analogia entre o correio e o e-mail - "O correio eletrônico é um serviço postal que usa as telecomunicações para transmissão". Esta analogia pode gerar consequências relacionadas ao envio de documentos oficiais. Por exemplo, receber uma decisão judicial via e-mail seria considerado um envio oficial.

As famílias dos soldados norte-americanos que morreram no Iraque também tentaram fazer uso dessa analogia entre correio (cartas) e o e-mail para obter acesso aos e-mails e blogs privados de seus entes queridos, argumentando que elas deveriam ter direto de herdar seus e-mails e blogs como se fossem cartas e diários. Os ISPs têm tido dificuldade em lidar com essa carga emocional. Em vez de acompanhar a analogia entre cartas e e-mails, a maior parte dos ISPs negaram o acesso pedido, com base no acordo de privacidade que assinaram com seus usuários.

O SISTEMA POSTAL E A ICANN

Paul Twomy, ex-Diretor-Presidente da ICANN, usou a seguinte analogia entre o sistema postal e a função da ICANN: "Se você pensar na Internet como o correio ou o sistema postal, o nome de domínio e o endereço IP basicamente garantem que os endereços na frente do envelope funcionem. Não têm a ver com o que você coloca dentro do envelope, quem envia o envelope, quem tem permissão para ler o envelope, quanto tempo demora para o envelope chegar ao seu destino, qual o preço do envelope. Nenhuma destas questões são importantes para as funções da ICANN. A função tem como papel central garantir que o endereço funcione".[16]

Internet – televisão

Semelhanças: a analogia inicial estava relacionada à semelhança física entre as telas do computador e da televisão. Uma analogia mais

16 Trechos do discurso do Secretário-Geral na reunião da ICANN no Cairo (6 de novembro de 2008). Acessível em <http://archive.icann.org/en/meetings/cairo2008/files/meetings cairo2008/toure-speech-06nov08.txt > [acessado em 21 de janeiro de 2014].

sofisticada traça um paralelo do uso de ambas as mídias – web e TV – para a radiodifusão.

Diferenças: a Internet é um meio mais amplo que a televisão. Além da semelhança entre a tela do computador e da TV, existem diferenças estruturais significativas entre os dois. A televisão é um meio de um para vários, com o objetivo de transmitir a radiodifusão aos telespectadores, ao passo que a Internet facilita diferentes tipos de comunicação (de um para um, de um para vários, de vários para vários).

Usada por: esta analogia é utilizada por aqueles que querem adotar um controle de conteúdo mais rígido para a Internet. Do ponto de vista deles, devido a seu poder como uma ferramenta de mídia de massa similar à televisão, a Internet deveria ser estritamente controlada. O governo dos Estados Unidos tentou usar essa analogia no caso de referência Reno vs ACLU. Este caso foi influenciado pela Lei de Decência nas Comunicações aprovada no Congresso dos Estados Unidos, que estipula o controle de conteúdo mais rígido para evitar que crianças sejam expostas a materiais pornográficos via Internet. A justiça dos Estados Unidos não reconheceu a analogia com a televisão.

Internet – biblioteca

Semelhanças: a Internet às vezes é vista como um vasto repositório de informações e o termo "biblioteca" costuma ser usado para descrevê-la. Por exemplo, "vasta biblioteca digital", "ciberbiblioteca", "Biblioteca de Alexandria do século XXI", etc.

Diferenças: o armazenamento de informações e dados é apenas um dos aspectos da Internet. Existem diferenças consideráveis entre bibliotecas e a Internet:

- As bibliotecas tradicionais têm por objetivo atender pessoas que vivem em determinado lugar (cidade, país etc.), ao passo que a Internet é global.
- Livros, artigos e periódicos são publicados por meio de procedimentos que garantem sua qualidade (editores). A Internet nem sempre tem editores .
- As bibliotecas são organizadas de acordo com métodos de classificação específicos, possibilitando aos usuários localizar livros em seu acervo. Não existe tal método de classificação para as informações na Internet .
- Além das descrições das palavras-chave, os conteúdos de uma biblioteca (texto em livros e artigos) não são acessíveis até que

um usuário pegue emprestado um livro ou artigo específico. O conteúdo da Internet pode ser acessado de imediato por meio de motores de busca.

Usada por: esta analogia é usada em diversos projetos cujo objetivo é a criação de um sistema abrangente de informação e conhecimento sobre questões específicas (portais, bancos de dado, etc). A analogia com a biblioteca tem sido usada no contexto do projeto Google Livros com o objetivo de digitalizar todos os livros impressos.

Internet – videocassete, fotocopiadora

Semelhanças: esta analogia prioriza a reprodução e a difusão de conteúdo (ex., textos e livros). O computador tem reprodução simplificada por meio do processo "copiar e colar". Isto, por sua vez, torna a difusão de informações via Internet muito mais simples.

Diferenças: o computador tem uma função muito mais ampla que a cópia de materiais, apesar de a cópia em si ser muito mais simples via Internet do que via VCR ou via copiadora.

***Usado por*:** esta analogia foi usada no contexto da Lei de Direitos Autorais do Milênio Digital dos Estados Unidos (DMCA - Digital Millennium Copyright Act), que penaliza instituições que contribuem com a violação de direitos autorais (desenvolvimento de software para violar a proteção aos direitos autorais, etc.). O contra-argumento nesses casos foi de que os desenvolvedores de software, como fabricantes de VCR e copiadora, não conseguem antecipar se seus produtos serão usados ilegalmente.

Esta analogia foi usada nas ações judiciais contra os desenvolvedores de software semelhantes ao Napster para compartilhamento de arquivos peer-to-peer (P2P), como o Grokster e o StreamCast.

Internet – rodovia

Semelhanças: a rodovia é para o transporte no mundo real o mesmo que a Internet é para a comunicação no mundo virtual.

Diferenças: além do aspecto do transporte, não existem semelhanças entre a Internet e as rodovias. A Internet movimenta materiais intangíveis (dados), ao passo que as rodovias facilitam o transporte de mercadorias e pessoas.

RODOVIAS E A INTERNET

Usada por: a analogia da rodovia foi usada amplamente no meio dos anos 90, após Al Gore alegadamente ter cunhado o termo "autoestrada da informação". O termo "estrada" também foi usado pelo governo alemão para justificar a introdução de uma lei mais rígida de controle de conteúdo da Internet em junho de 1997:

É uma lei liberal que nada tem a ver com censura, mas que claramente define as condições sobre o que o provedor pode e não pode fazer. A Internet é um meio de transportar e distribuir conhecimento... assim como acontece com as rodovias, é necessário haver diretrizes para ambos os tipos de tráfego.[17]

Internet – alto-mar

Semelhanças: inicialmente, esta analogia tinha como base o fato de que, assim como o alto-mar, a Internet parece ir além da jurisdição nacional.

Diferenças: Hoje em dia, claramente, a maior parte da Internet está dentro do âmbito de certa jurisdição nacional. A infraestrutura técnica através da qual o tráfego da Internet é canalizado é de propriedade de empresas privadas e estatais, geralmente operadoras de telecomunicações. A analogia mais próxima à Internet no campo marítimo seriam os containers de transporte de empresas de navegação.

Com relação aos instrumentos jurídicos, a Convenção sobre o Direito do Mar regula as atividades que vão além da jurisdição nacional, como as atividades em alto-mar. Não há nada equivalente no campo das telecomunicações da Internet.

Usada por: esta analogia é usada por aqueles que defendem a regulação internacional da Internet. Concretamente, essa analogia sugere o uso do conceito advindo da antiga lei Romana *res communis omnium* (isto é, o espaço como patrimônio da humanidade a ser regulado e adquirido por todas as nações) para a Internet, da mesma forma que tal conceito é usado para a regulação do alto-mar.

Classificação de questões de governança da Internet

A governança da Internet é um campo novo e complexo que requer um mapeamento e classificação conceitual inicial. A sua complexidade está relacionada a sua natureza multidisciplinar, englobando

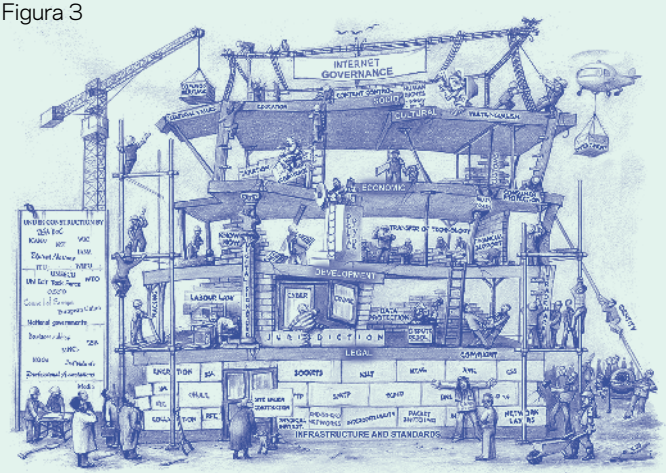
17 Citado em Mock K, Armony L (1998) Hate on the Internet. Acessível em <http://archive.is/M70XS> [acessado em 13 de fevereiro de 2014].

vários aspectos, entre os quais os aspectos tecnológicos, socioeconômicos, de desenvolvimento, jurídico e político.

A necessidade prática de classificação foi claramente definida durante o processo da CMSI. Na primeira etapa, durante a preparação para a cúpula de Genebra (2003), muitos atores, inclusive estados-nações, apresentaram dificuldade em compreender a complexidade da governança da Internet. O mapeamento conceitual, elaborado por meio de diversas contribuições acadêmicas e do relatório do GTGI, contribuíram para a realização de negociações mais eficientes no contexto do processo da CMSI. O relatório do GTGI (2004) identificou quatro áreas principais:

- Questões relacionadas à infraestrutura e gestão de recursos críticos da Internet.

Figura 3



- Questões relacionadas ao uso da Internet, inclusive spam, segurança de rede e crime cibernético.
- Questões relevantes à Internet mas que têm impacto para além dela e pelas quais organizações existentes são responsáveis, como direitos de propriedade intelectual (DPI) ou de comércio internacional.

Questões relacionadas aos aspectos de desenvolvimento da governança da Internet, mais especificamente a criação de capacidades nos países em desenvolvimento.

A agenda para o primeiro IGF realizado em Atenas (2006) foi elaborada em torno dos seguintes temas: acesso, segurança, diversidade

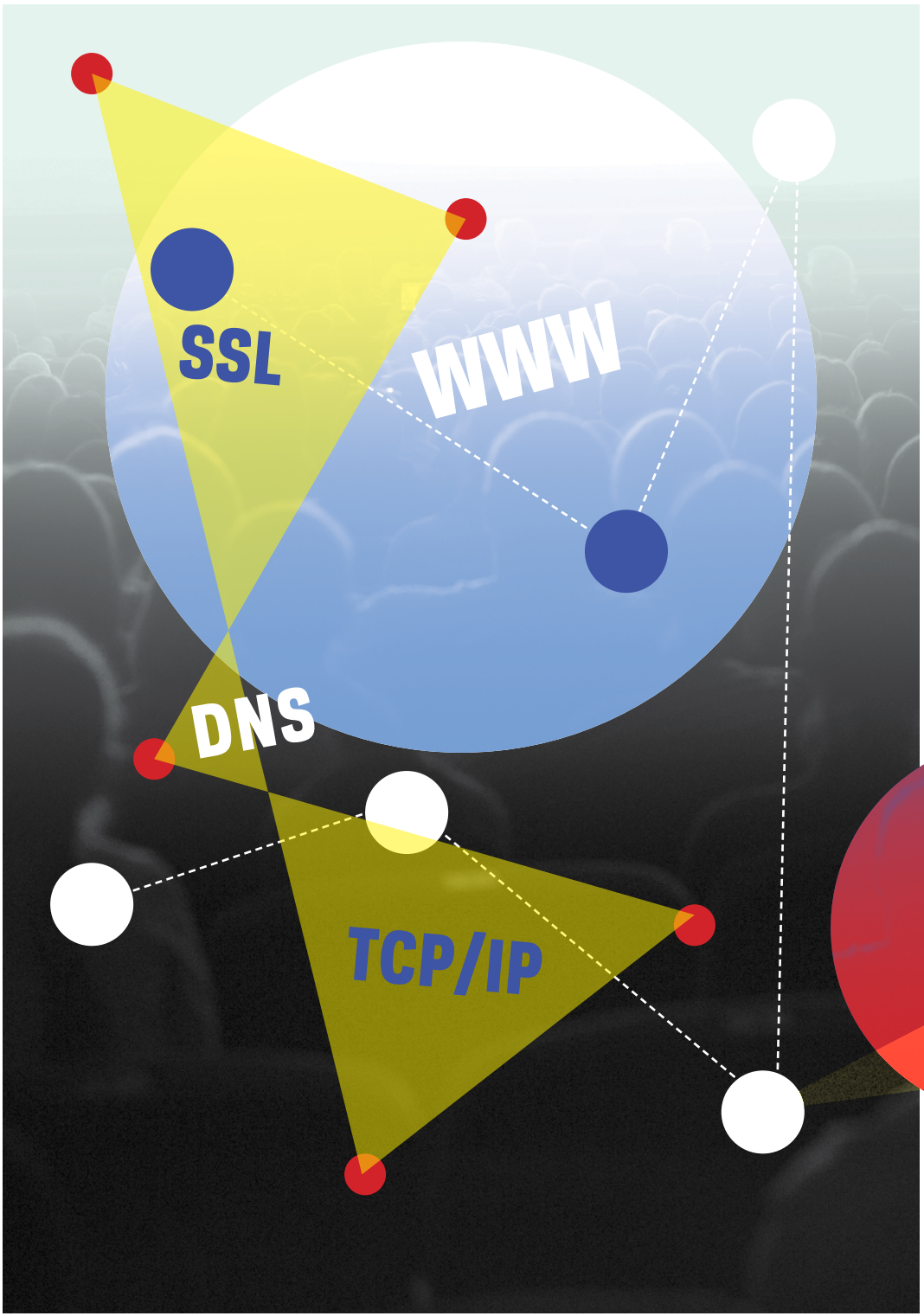
e abertura. No segundo IGF no Rio de Janeiro (2007), uma quinta área temática foi incluída à agenda: a gestão de recursos críticos da Internet. Estas cinco áreas temáticas influenciaram as agendas de todas as reuniões subsequentes do IGF.

Apesar de a classificação sofrer mudanças, a governança da Internet aborda mais ou menos o mesmo conjunto de 40–50 questões específicas, com mudanças na relevância de questões específicas. Por exemplo, embora o spam tenha se destacado na classificação do GTGI em 2004, a sua relevância em políticas diminuiu nos encontros do IGF, nos quais tal assunto se tornou um dos temas menos proeminentes no âmbito da área temática da Segurança. A classificação da Diplo de governança da Internet agrupa as 40–50 principais questões nas cinco cestas a seguir:

- Infraestrutura e padronização
- Jurídica
- Econômica
- Desenvolvimento
- Sociocultural

Esta classificação (Figura 4) reflete tanto as abordagens de políticas mencionadas acima (GTGI, IGF) quanto as pesquisas acadêmicas neste campo. A classificação foi desenvolvida em 1997 com alterações constantes baseadas em feedback de estudantes (um total de 1542 ex-alunos desde 2013), resultados de pesquisas e contribuições do processo de políticas.[18]

18 O termo "cesta" foi introduzido no exercício diplomático durante as negociações da Organização para Segurança e Cooperação na Europa (OSCE).


SSL
WWW
DNS
TCP/IP

Cesta de infraestrutura e padronização

A cesta de infraestrutura e padronização inclui as questões básicas, principalmente técnicas, relacionadas ao funcionamento da Internet. O principal critério para incluir determinada questão nesta cesta é sua relevância para a funcionalidade básica da Internet. Existem dois grupos de questões neste caso.

O primeiro grupo inclui as questões essenciais sem as quais a Internet e a World Wide Web (www) não poderiam existir.[1] Estas questões estão agrupadas nas três camadas a seguir:

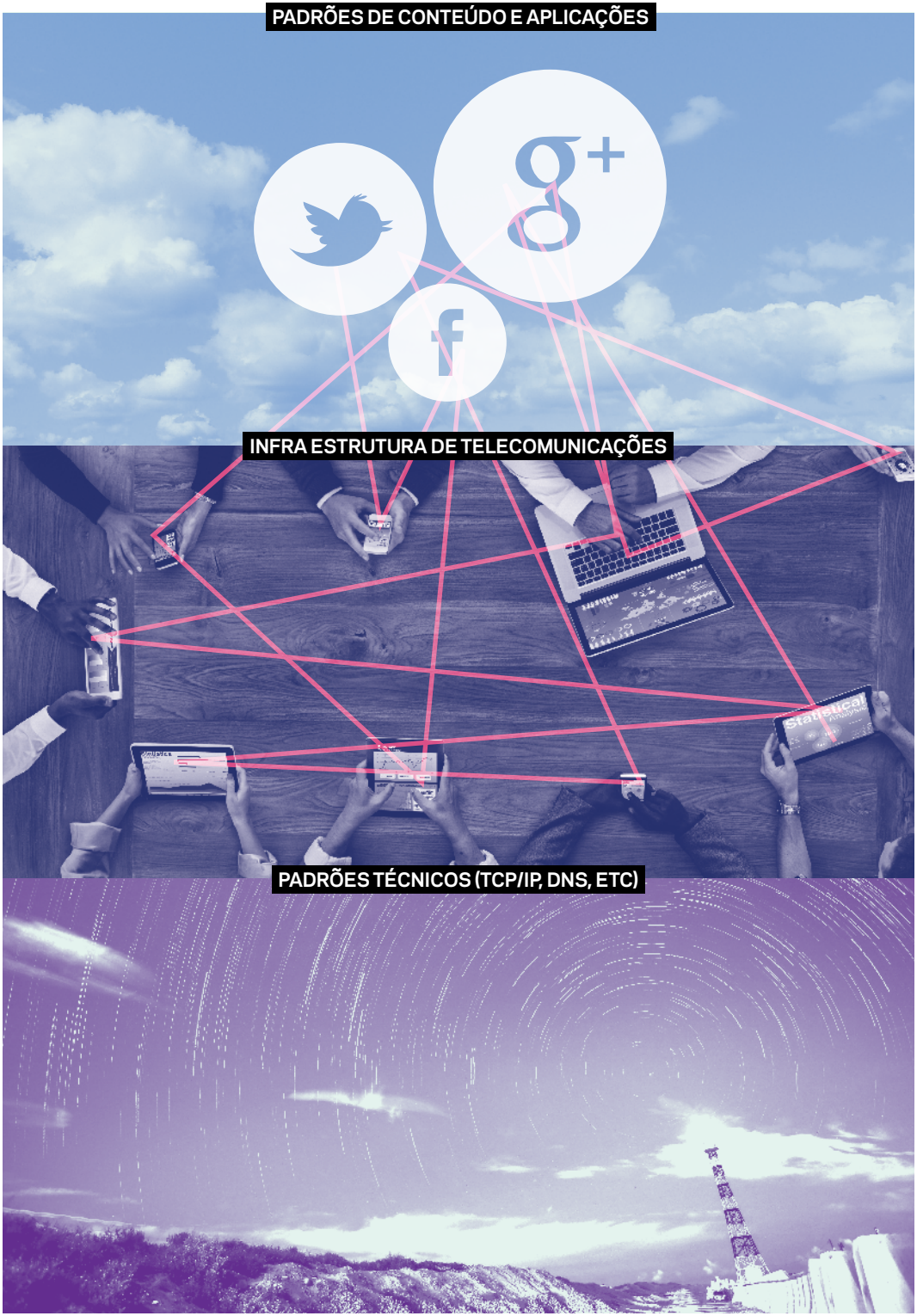
1 A infraestrutura das telecomunicações, através da qual todo o tráfego da Internet flui.

2 Os padrões e serviços técnicos da Internet, a infraestrutura que faz a Internet funcionar (ex. TCP/IP - Transmission Control Protocol/Internet Protocol; DNS: Domain Name System; SSL: Secure Sockets Layer).

3 Os padrões de conteúdo e aplicativos (ex.: HTML: HyperText Markup Language; XML: eXtensible Markup Language).

O segundo grupo consiste em questões relacionadas à preservação da operação segura e estável da infraestrutura da Internet, e inclui cibersegurança, criptografia e spam.

1 Os termos Internet e www às vezes são usados de forma intercambiável; no entanto, existe uma diferença. A Internet é a rede das redes conectada pelo TCP/IP. Às vezes, o termo Internet é usado para englobar tudo, inclusive infraestrutura, aplicativos (e-mail, ftp, Web) e conteúdo. O www é apenas um dos vários aplicativos da Internet, um sistema de documentos interligados conectados com a ajuda do HyperText Transfer Protocol (HTTP).


PADRÕES DE CONTEÚDO E APLICAÇÕES
INFRA ESTRUTURA DE TELECOMUNICAÇÕES
PADRÕES TÉCNICOS (TCP/IP, DNS, ETC)

A infraestrutura de telecomunicações[2]

A situação atual

Os dados da Internet podem viajar por uma diversa gama de meios de comunicação: fios telefônicos, cabos de fibra ótica, satélites, microondas e ligações sem fio. Até mesmo a rede elétrica padrão pode ser usada para retransmitir o tráfego da Internet usando tecnologia de linha de transmissão de energia.[3]

A forma como as telecomunicações são reguladas impacta a governança da Internet diretamente. A infraestrutura de telecomunicações é regulada tanto nacional quanto internacionalmente por diversas organizações públicas e privadas. As principais organizações internacionais envolvidas na regulamentação das telecomunicações incluem a União Internacional de Telecomunicações (UIT), que desenvolveu regras de coordenação entre sistemas de telecomunicação nacionais, a alocação do espectro de rádio e a gestão do posicionamento de satélite; e a Organização Mundial do Comércio (OMC), que teve papel importante na liberalização do mercado de telecomunicações em todo o mundo .[4]

2 Seguindo uma política de neutralidade tecnológica, a União Europeia vem usando o termo "comunicações eletrônicas" em vez de "telecomunicações". Isto abrange, por exemplo, o tráfego da Internet através da matriz eletrônica, que não faz parte da infraestrutura de telecomunicações.

3 A transferência da Internet via matriz eletrônica é chamada de Power Line Communication (PLC). O uso da matriz eletrônica tornaria a Internet mais acessível para muitos usuários. Para uma análise técnica e organizacional desta instalação, consultar Palet J (2003) Addressing the Digital Divide with IPv6-enabled Broadband Power Line Communication, Internet Society, ISOC Member Briefing No. 13. Acessível em <http://www.isoc.org/briefings/013> [Acessado em 13 de fevereiro de 2014].

4 A liberalização dos mercados de telecomunicações pelos membros da OMC foi formalizada in 1998 no chamado Basic Telecommunication Agreement (BTA). Seguindo a adoção do BTA, mais de 100 países iniciaram o processo de liberalização, caracterizado pela privatização dos monopólios nacionais de telecomunicações, a entrada da competição e o estabelecimento de reguladores nacionais. O acordo é formalmente chamado de The Fourth Protocol to the General Agreement on Trade in Services (adotado em 30 de abril de 1996, válido desde 5 de fevereiro de 1998). Acessível em <http://www.wto.org/english/tratop_e/serv_e/4prote_e.htm>[acessado em 13 de fevereiro de 2014].

REGULAÇÕES INTERNACIONAIS DE TELECOMUNICAÇÃO (ITRS)

As Regulações Internacionais de Telecomunicação (ITRs) da UIT, de 1988, facilitaram a liberalização internacional de preços e serviços, bem como possibilitaram um uso mais inovador de serviços básicos no campo da Internet, como linhas alugadas internacionais. Elas ofereceram uma das bases de infraestrutura para a rápida expansão da Internet nos anos 90. As ITRs foram alteradas em dezembro de 2012 durante a CMTI-12 em Dubai; 89 países – a maioria dos países em desenvolvimento – assinaram as ITRs alteradas, enquanto 55 países, entre os quais os EUA e muitos países europeus, não as assinaram.[5]

As funções da UIT e da OMC são relativamente diferentes. A UIT estabelece padrões técnicos voluntários detalhados e regulamentos internacionais específicos de telecomunicações, bem como fornece assistência técnica a países em desenvolvimento.[6] A OMC fornece um quadro para as regras gerais do mercado.[7]

Após a liberalização, o quase monopólio da UIT como a principal instituição para definição de padrões para as telecomunicações foi diminuído por outras agências e organizações internacionais. Ao mesmo tempo, grandes companhias de telecomunicações – tais como AT&T, Cable & Wireless, France Telecom, Sprint, e WorldCom – tiveram a oportunidade de expandir sua cobertura de mercado globalmente. Como a maior parte do tráfego da Internet é transmitido pelas infraestruturas de telecomunicações dessas empresas, elas exercem grande influência sobre os avanços da Internet.

As questões

1. Última milha (last mile)

A "linha de assinantes" ou "última milha" é o nome dado à conexão entre os ISPs e seus clientes individuais. Problemas com as linhas

5 UIT (sem data) Signatories of the Final Acts – CMTI-12. Acessível em <http://www.itu.int/osg/wcit-12/highlights/signatories.html> [acessado em 11 de agosto 2014].

6 Uma das polêmicas em torno da CMSI era a intenção da UIT de se envolver mais no processo de governança da Internet, principalmente no âmbito do domínio administrado pela ICANN. Para mais informações sobre as políticas de Internet da UIT, consultar <http://www.itu.int/osg/csd/intgov/> [acessado em 13 de fevereiro de 2014].

7 Para mais informações sobre o papel da OMC no campo das telecomunicações, consulte <http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm> [acessado em 13 de fevereiro de 2014].

de assinantes são um obstáculo para o uso mais difundido da Internet em muitos países, principalmente países em desenvolvimento. A comunicação sem fio é uma solução de baixo custo possível ao problema da linha de assinantes.[8] Além das opções tecnológicas cada vez mais disponíveis, a solução para o problema da linha de assinantes também depende da liberalização deste segmento do mercado de telecomunicações.

2. A liberalização dos mercados de telecomunicações

Um número considerável de países liberaram seus mercados de telecomunicações com o objetivo de impulsionar o desenvolvimento de novos serviços de telecomunicações ao permitir o acesso à infraestrutura (estatal) existente. No entanto, muitos países em desenvolvimento se veem tendo que fazer uma difícil escolha: liberalizar e expandir o mercado de telecomunicações e torná-lo mais eficiente ou preservar as receitas orçamentárias dos monopólios de telecomunicações existentes. Esta questão foi discutida na Conferência Mundial sobre Telecomunicações Internacionais de 2012 (CMTI-12) e alguns países em desenvolvimento levantaram a questão da redistribuição das receitas dos serviços de comunicação da Internet.[9]

3. O estabelecimento de padrões técnicos de infraestrutura

Padrões técnicos vêm sendo definidos com cada vez mais frequência por instituições privadas e profissionais. Por exemplo, o padrão WiFi, IEEE 802.11b foi desenvolvido pelo Institute of Electrical and Electronic Engineers (IEEE). A certificação de equipamentos compatíveis com WiFi é realizada pela WiFi Alliance.[10] A função de definir e implementar padrões em um mercado em rápida expansão concede a tais instituições considerável influência.

4. A quem pertence o espectro eletromagnético?

O atual regime de gestão do espectro tem como base a assunção de que ele é um recurso escasso que deveria ser administrado por instituições

8 A Letônia e a Moldávia são bons exemplos de como é possível para dar um passo significativo em direção ao rápido desenvolvimento da infraestrutura de telecomunicações por meio da implementação da comunicação sem fio; ver <http://www.isoc.org/isoc/conferences/inet/99/proceedings/4d/4d_2.htm> [acessado em 13 de fevereiro de 2014].

9 Nothias J-C (2012) The hypocrisy threatening the future of the Internet. The Global Journal. Acessível em <http://theglobaljournal.net/article/view/904/> [acessado em 10 de agosto de 2014].

10 Inicialmente, a Wi-Fi Alliance era chamada de Wireless Ethernet Compatibility Alliance (WECA). Recebeu seu nome atual em 2002. Foi formada por alguns dos principais desenvolvedores de equipamentos de telecom, entre os quais: 3Com, Cisco, Intersil, Agere e Nokia.

governamentais, iniciativas regionais (como o Radio Spectrum Committee (RSC) da União Europeia e o Radio Spectrum Policy Group (RSPG) da UIT. O desenvolvimento de novas tecnologias que usam o espectro com mais eficiência que antes fez com que ele fosse concebido como um recurso menos escasso na prática. Por fim, o volume e os limites de uso do espectro irão depender dos avanços tecnológicos. Esta abordagem defende que o regulamento governamental atual deveria ser substituído pelo "espectro aberto", isto é, acesso aberto a todos.

Esta visão apresenta dois possíveis problemas. Um deles. de praticidade, relacionado aos enormes investimentos que as empresas de telecomunicações, principalmente na Europa, fizeram ao adquirir os direitos para operar redes de telefone sem fio da terceira geração.[11] O outro problema é que se o espectro se tornar acessível a todos, isso não necessariamente irá significar que será usado por grande parte das pessoas como um bem público. Em vez disso, será usado por atores com capacidades técnicas para usar o espectro "livre".

O desenvolvimento de novos serviços de telecomunicações por meio do espectro de rádio, especialmente banda larga sem fio e comunicação móvel, aumentou a demanda por radiofrequências, incentivando governos ao redor do mundo a buscarem soluções para acomodar o uso do espectro ótico. Substituir a transmissão análoga conservadora com televisão digital possibilita a liberalização de uma parte importante do espectro de rádio que pode ser alocado para outros serviços – a chamada exclusão digital. A União Europeia desenvolveu um programa regulatório abrangente para gestão do espectro de rádio,[12] enquanto os Estados Unidos adotaram uma abordagem baseada no mercado ao submeter as frequências a processos de leilão.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Situação atual

O TCP/IP é o principal padrão técnico da Internet. Tem como base três princípios: comutação de pacotes, rede fim-a-fim e robustez. A governança da Internet relacionada ao TCP/IP tem dois aspectos importantes:

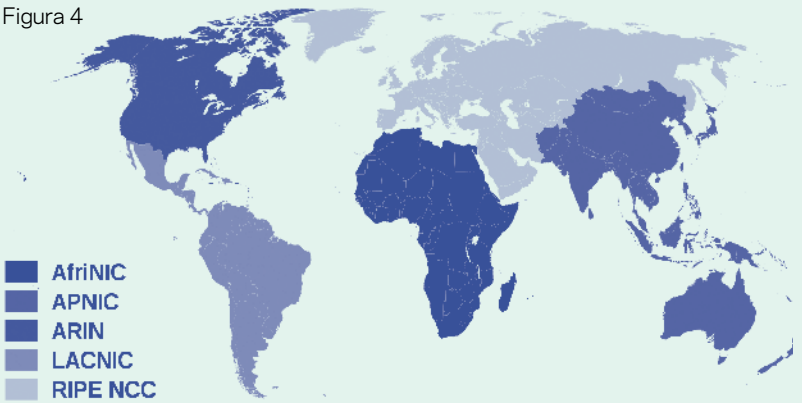
11 Estima-se que este investimento totalize aproximadamente €109, de acordo com a The Economist (2003) Beyond the Bubble Survey: Telecoms. Acessível em <http://www.economist.com/node/2098913> [acesado em 13 de fevereiro de 2014].

12 Para mais informações sobre a política de espectro de radiofrequências da UE ver <http://ec.europa.eu/digital-agenda/en/what-radio-spectrum-policy> [acessado em 13 de fevereiro de 2014].

-A introdução de novo padrões
-A distribuição de números IP

Os padrões TCP/IP são definidos pela Internet Engineering Task Force (IETF). Dada a relevância central destes protocolos à Internet, eles são cuidadosamente protegidos pela IETF. Quaisquer mudanças ao TCP/IP exigem ampla discussão prévia e comprovação de que são uma solução efetiva (ou seja, o princípio do "código de execução"). Os números IP são endereços numéricos únicos que todos os computadores conectados à Internet devem ter. Dois computadores conectados à Internet não podem ter o mesmo número IP. Isto faz dos números IP uma fonte potencialmente escassa.

Figura 4



O sistema para a distribuição dos números IP é organizado hierarquicamente. No topo está a IANA (Internet Assigned Number Authority – subsidiária da Internet Corporation for Assigned Names and Numbers – ICANN), que distribui blocos de números IP a cinco registros regionais da Internet (RIRs). [13] Os RIRs distribuem números IP aos registros locais da Internet (LIRs) e aos registros nacionais da Inter

13 Os atuais RIRs são: ARIN (the American Registry for Internet Numbers), APNIC (the Asia Pacific Network Information Centre), LACNIC (the Latin American and Caribbean IP Address Regional Registry), RIPE NCC (Reseaux IP Européens Network Coordination Centre – cobre a Europa e o Oriente Médio) e o AFRINIC (the African Network Information Centre). A explicação detalhada do sistema RIR está Acessível em <https://www.ripe.net/participate/internet-governance/internet-technical-community/the-rir-system> [acessado em 13 de fevereiro de 2014].

net (RIRs), que por sua vez distribuem números IP a ISPs menores, empresas e pessoas alguns degraus abaixo.

Questões

Como lidar com a limitação dos números IP (a transição para o IPv6)

O banco de números IP no IPv4 (Internet Protocol, versão 4) contém aproximadamente quatro bilhões de números que haviam sido integralmente alocados pela IANA para os cinco RIRs em fevereiro de 2011. A diminuição dos números IPv4 foi acelerada com a introdução em anos recentes de dispositivos com acesso à Internet (como celulares, organizadores pessoais, console de jogos e aparelhos domésticos) e o aumento da conectividade da Internet em todo o mundo. A preocupação de que os números IP pudessem acabar e por fim inibir o futuro desenvolvimento da Internet fez com que a comunidade técnica tomasse três importantes medidas.

-Racionalizar o uso do banco de números IP existente por meio da introdução do Network Address Translation (NAT).

-Abordar os algoritmos de alocação com desperdício de endereço usados pelos RIRs ao introduzir o Classless Inter-Domain Routing (CIDR).

-Introduzir uma nova versão do protocolo TCP/IP – IPv6 – que fornece um banco muito maior de números IP (mais de 340.000.000.000.000.000.000).

A resposta da comunidade técnica da Internet ao problema de uma possível falta de números IP é um exemplo de gestão rápida e proativa. Embora tanto o NAT quanto CIDR ofereçam uma solução rápida para o problema, a solução adequada e de longo prazo é a transição para o IPv6. Apesar de o IPv6 ter sido introduzido em 1996, a sua aplicação tem sido muito gradual, devido à falta de consciência sobre a necessidade de transição, bem como devido a verbas limitadas para investimento em novos equipamentos nos países em desenvolvimento.

Um dos principais desafios relacionados à aplicação do IPv6 é a falta de compatibilidade reversa entre o IPv6 e o IPv4. As redes que usam o IPv6 não conseguem se comunicar com as redes, ainda dominantes, que usam o IPv4. Como é bem provável que as redes que usam o IPV4 e o IPv6 coexistam em um período próximo, é importante garantir que novas redes – com base no IPv6 – não continuem sendo uma ilha. A solução técnica para isso engloba o tunelamento especial entre os dois tipos de rede, que levará ao roteamento mais complexo na Internet e alguns outros problemas colaterais.

Dada a complexidade da transição para o IPv6, os países em desenvolvimento talvez se beneficiem do início atrasado e da possibilidade de introduzir redes baseadas no IPv6 desde o início. Neste processo, esses países em desenvolvimento precisarão de assistência técnica.[14]
Além do problema de transição, o quadro normativo para a distribuição do IPv6 irá requerer a distribuição adequada dos números IP, o que exigirá a introdução de mecanismos abertos e competitivos para atender da melhor forma às necessidades de usuários finais. Mesmo com a introdução do IPv6, ainda poderia haver uma escassez "artificial" dos números IP, se as pessoas responsáveis por alocá-los no nível local, como os ISPs, abusassem de seu poder e ligassem tal alocação, por exemplo, à compra de outros serviços, assim afetando a disponibilidade e o preço dos números IP.

Mudanças no TCP/IP e cibersegurança

A segurança não era uma questão importante para os desenvolvedores originais da Internet, uma vez que naquela época a Internet consistia em uma rede fechada de institutos de pesquisa. Com a expansão da Internet para dois bilhões de usuários no mundo todo e sua crescente importância como ferramenta comercial, a questão da segurança agora está no topo da lista das questões de governança da Internet.
Como a arquitetura da Internet não foi projetada considerando a questão da segurança, a incorporação de um sistema de segurança intrínseco irá demandar mudanças significativas à própria base da Internet, o TCP/IP. O novo protocolo (IPv6) apresenta melhorias de segurança, mas ainda não apresenta uma solução abrangente. Essa proteção exigiria modificações consideráveis no TCP/IP.[15]

14 Para uma discussão mais aprofundada sobre o IPv6, consultar o projeto de pesquisa: IP Allocation and IPv6 por Jean Philémon Kissangou, Marsha Guthrie e Mwende Njiraini, parte do 2005 Internet Governance Capacity Building Programme. Acessível em <http://archive1.diplomacy.edu/poolbin.asp?IDPool=130>[acessado em 13 de fevereiro de 2014].

15 Para uma pesquisa abrangente e altamente técnica do TCP/IP Security, consultar: Chambers C, Dolske J and Iyer J., TCP/IP Security, Department of Computer and Information Science, Ohio State University. Acessível em <http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.htm>[acessado em13 de fevereiro de 2014].

TECNOLOGIA, PADRÕES, E POLÍTICA

A padronização poderia ser a política por outros meios. Os padrões técnicos poderiam ter consequências econômicas e sociais abrangentes, promovendo interesses específicos e alterando o equilíbrio de poder entre negócios concorrentes e/ou interesses nacionais. Padrões são essenciais para a Internet. Por meio de padrões e design de software, os criadores da Internet podem definir de que forma os direitos humanos são usados e protegidos (ex.. liberdade de informação, privacidade e proteção de dados).

Os esforços para criar padrões formais trazem para esfera pública as decisões técnicas particulares tomadas pelos criadores de sistemas; dessa forma, as batalhas comuns podem trazer à tona premissas tácitas e conflitos de interesse. A própria paixão com que partes envolvidas contestam as decisões sobre os padrões deveria nos servir de alerta sobre o sentido mais profundo dos aspectos práticos.

Mudanças no TCP/IP e o problema da banda larga limitada

Para facilitar o fornecimento de conteúdo multimídia (ex., telefonia da Internet, ou vídeo sob demanda), é necessário oferecer um serviço de qualidade (QoS) capaz de garantir um nível mínimo de desempenho. O QoS é especialmente importante em aplicativos sensíveis a atrasos, como a transmissão de eventos ao vivo, e conseguir tal QoS costuma ser difícil devido às limitações de banda larga. A introdução do QoS talvez exija mudanças no IP e até mesmo um possível desafio para o princípio da neutralidade da rede.

O Sistema da Nomes de Domínio (DNS)

Situação atual

O DNS lida com os endereços da Internet (como www.google.com) e os transforma em números IP (o esquema simplificado deste processo está ilustrado na Figura 8). O DNS consiste em servidores-raiz, servidores de domínio de topo (TLD) e uma grande quantidade de servidores DNS localizados em todo o mundo.[16]

O DNS inclui três tipos de domínios de topo: genérico (gTLD), código de país (ccTLD) e patrocinado (sTLD). Os gTLDs incluem domínios

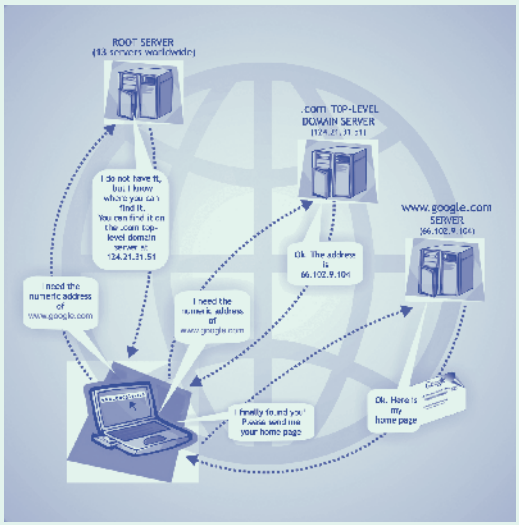
16 Um dos poucos documentos de referência sobre o sistema de nome de domínio (DNS) é o RFC 1591 (março de 1994), que especifica a estrutura de governança do DNS. Acessível em <http://www.ietf.org/rfc/rfc1591.txt> [acessado em 13 de fevereiro de 2014].

que poderiam ser obtidos por qualquer pessoa (.com, .info, .net, e .org). Desde 2014, muitos outros gTLDs foram adicionados, como .pub, .بازار (bazaar), .rentals, .ngo, ou .游. Os sTLDs são limitados a um grupo específico. Por exemplo, o sTLD ".aero." é o registro aberto para o setor de transporte aéreo. Os ccTLDs designam países ou territórios específicos (.uk, .cn, .in).

VER A SEÇÃO 3
PARA UMA DISCUSSÃO MAIS APROFUNDADA SOBRE PROPRIEDADE INTELECTUAL

Para cada gTLD existe um registro que mantém uma lista de endereço. Por exemplo, o gTLD .com é administrado pela VeriSign. A função de vendedor é desempenhada pelos agentes de registro. A ICANN coordena de forma geral o sistema DNS, fechando acordos e homologando registros e agentes de registro. Uma parte importante da gestão do DNS é a proteção de marcas registradas e a resolução de litígios. O princípio "quem chegar primeiro é atendido primeiro" da alocação do nome de domínio adotado no início da Internet desencadeou o fenômeno conhecido como ciberespeculação, a prática de registrar nomes de domínio que poderiam ser revendidos mais tarde. A Política para Resolução Uniforme de Litígios sobre Nomes de Domínios (UDRP - Uniform Dispute Resolution Policy) desenvolvida pela ICANN e a Organização Mundial da Propriedade Intelectual (OMPI) contribuíram com mecanismos que reduziram significativamente a ciberespeculação. A propriedade intelectual é discutida de forma mais detalhada no Pacote Jurídico.

Figura 5



Outro elemento importante na pesquisa da atual organização da governança do DNS é a administração dos ccTLDs. Atualmente, alguns códigos de países ainda são administrados por diversas instituições ou pessoas que receberam acreditação no início da Internet, quando alguns governos não tinham nenhum interesse nesses assuntos.

Questões

A criação de novos nomes de domínio genéricos

Tecnicamente, a criação de novos TLDs é quase ilimitada. No entanto, a introdução de novos gTLDs tem sido um processo lento e debatido.[17] Após seis anos de consultas e avanços no novo plano de ação, a ICANN iniciou a implementação de um novo programa gTLD em 2012. Nos termos do novo programa, qualquer organização no mundo poderia se candidatar para administrar um novo registro gTLD, inclusive em scripts que não são de idioma latino. A principal oposição à criação de novos gTLDs originária do lobby das marcas registradas se referia à proteção de suas marcas registradas no contexto do número crescente de domínios e do aumento da ciberespeculação. Apesar de o debate sobre a introdução de novos gTLDs prosseguir, o programa já foi implementado e está operacional.

Sob pressão para introduzir novos gTLDs, a ICANN iniciou consultas para planejar um novo plano de ação no campo, que abordaria a resolução de pedidos concorrentes por gTLDs, o risco de ciberespeculação, questões da moralidade pública, registro de taxas, entre outras questões. A propriedade intelectual não era a única preocupação neste processo. A situação mais ilustrativa foi a proposta de introduzir o domínio .xxx para materiais adultos.[18] Iniciada em 2000 e resubmetida em 2004, a proposta foi rejeitada pelo Conselho da ICANN em março de 2007. A principal crítica a esta decisão foi que a ICANN elaborou tal proposta por pressão do governo dos Estados Unidos, que se opôs fortemente contra sua introdução,[19] o que levou a muitas reações contrárias ao

17 Uma visão geral dos gTLDs com um link para a lista de todos os TLDs está Acessível em <http://www.icann.org/en/resources/registries/about> [acessado em 13 de fevereiro de 2014].

18 O texto da proposta está Acessível em <http://archive.icann.org/en/tlds/stld-apps19mar04/xxx.htm>; a retrospectiva do aplicativo .XXX , na ata da reunião de 30 de março de 2007 quando foi rejeitado pelo conselho da ICANN, está Acessível em <https://www.icann.org/resources/board-material/resolutions-2007-03-30-en#_blank> [acessado em 13 de fevereiro de 2014].

19 O governo dos EUA não usou nenhum procedimento da ICANN. Usou sua autoridade de facto por meio de uma carta enviada pelo Departamento de Comércio dos EUA ao Presidente da ICANN.

governo norte-americano. Entre essas reações, estavam vozes céticas que alegavam que o .xxx não seria interessante para a indústria do sexo na Internet devido ao risco de ser excessivamente filtrado. A questão foi retomada em junho de 2010, após nova submissão; o Conselho da ICANN analisou positivamente o pedido para o domínio .xxx, que foi por fim aprovado como uma sTLD em 2011. Esta decisão também reabriu a discussão sobre o papel da ICANN nas questões de políticas públicas. Outras polêmicas talvez continuem a surgir com relação aos gTLDs para comunidades culturais e linguísticas. Em 2003, a ICANN lançou o novo domínio .cat para o idioma catalão – o primeiro domínio lançado para um idioma.[20] Esta decisão não encontrou oposição do governo espanhol, mas poderia haver casos no qual as comunidades culturais e linguísticas com o mesmo pedido talvez tivessem aspirações de se tornar uma nação e este aspecto talvez gerasse polêmicas e conflitos com os países existentes.

A proteção de indicadores geográficos parecia ser outra batata quente: a ICANN parou o processo de delegação da .amazon à Amazon (a loja online) após grande protesto de países latino-americanos em seus Comitês Consultivos para Assuntos Governamentais (GAC). A delegação de .wine/.vin tem sido fortemente contestada pela Suíça e pela França, bem como por muitos outros países. Quando a ICANN atribuiu o nome de domínio .Africa ao consórcio liderado pela Comissão da União Africana esta decisão foi contestada por uma empresa privada.[21]

A administração de domínios de países[22]

A administração dos ccTLDs envolve três questões importantes. A primeira se refere a uma decisão que geralmente causa polêmica no âmbito da política, a saber, quais códigos de países deveriam exatamente ser registrados ao lidar com países e entidades cujo status internacional não é claro ou é controverso (ex., países recém-independentes, movimentos de resistência). Uma questão polêmica foi a alocação de um nome de domínio para a Autoridade Palestina. Ao justificar a decisão de alocar

20 O formulário de requerimento para registro do domínio .cat: <http://archive.icann.org/en/tlds/stld-apps-19mar04/cat.htm>[acessado em 13 de fevereiro de 2014]

21 Relatório Resumido ICANN 50. Plataforma Internet Genebra. Acessível em <http://www.giplatform.org/resources/gip-summary-report-icann-50>[acessado em 9 de agosto de 2014].

22 O sítio web da UIT contém uma bibliografia abrangente dos materiais relacionados a Gestão de Domínios de País; a maior parte dos materiais foram entregues na Oficina da UIT sobre Gestão de Domínios de País realizada em Kuala Lumpur. Acessível em <http://www.itu.int/ITU-T/worksem/cctld/kualalumpur0704/contributions/index.html> [acessado em 13 de fevereiro de 2014].

o TLD .ps, a IANA reiterou o princípio de alocação de nomes de domínio em conformidade com o padrão ISO 3166 para códigos de países, conforme proposto por Jon Postel, um dos fundadores da Internet.[23]
A segunda questão se refere a quem deveria administrar os ccTLDs. Muitos países vêm tentando ganhar controle sobre seus domínios de país, considerados recursos nacionais. Governos nacionais escolheram uma ampla gama de abordagens normativas.[24] A transição (re-delegação) a uma nova instituição que administrará o ccTLD (delegado) dentro de cada país somente é aprovada pela ICANN se não houver nenhuma oposição de quaisquer setores do país. Dada a importância desta questão e a ampla gama de abordagens, houve duas iniciativas importantes no nível internacional para apresentar certo nível de harmonização. A primeira, os Princípios GAC,[25] foi adotada pelo GAC da ICANN, que propôs normas e procedimentos especificados para a re-delegação da administração do ccTLD. A segunda se trata das Melhores Práticas, proposta pela World Wide Alliance of Top-Level Domains (junho de 2001).
A terceira questão está relacionada à relutância de muitas operadoras de domínio de país em se tornarem parte do sistema ICANN. Até o momento, a ICANN não conseguiu reunir operadoras de domínio de país sob seu guarda-chuva. As operadoras de domínio de país estão organizadas em nível regional (Europa – CENTR, África – AFTLD, Ásia

23 O Relatório da IANA sobre o domínio de topo de código de país para a Palestina está Acessível em <http://www.iana.org/reports/ps-report-22mar00.htm> [acessado em 13 de fevereiro de 2014].

24 Por exemplo, a África do Sul usou seus direitos soberanos como argumento para retomar o controle de seu domínio de país. Uma lei recém-promulgada especifica que o uso do domínio do país fora dos parâmetros prescritos pelo governo sul-africano será considerado um crime. O modelo brasileiro da gestão de domínios de país é geralmente citado como exemplo de sucesso da abordagem multissetorial. O órgão nacional responsável pelos domínios brasileiros está aberto a todos os principais participantes, inclusive autoridades governamentais, o setor empresarial e a sociedade civil. A transferência da gestão dos domínios de país do Camboja do controle não governamental para o controle governamental costuma ser citada como exemplo de transição não exitosa. O governo reduziu a qualidade dos serviços e implementou taxas mais altas, tornando o registro dos domínios do Camboja muito mais difícil. Para mais informações, consultar: Alfonso C (2004) BR: CCTLD An asset of the commons, em MacLean D (ed) Internet Governance: A Grand Collaboration. Nova York: TIC ONU Task Force, pp. 291-299; Klien N (2004) Internet Governance: Perspectives from Cambodia em MacLean D (ed) Internet Governance: A Grand Collaboration. Nova York: TIC ONU Task Force, pp. 227-237. Trechos acessíveis em <http://books.google.ro/books?id=pEFAypES4t0C&printsec=frontcover&hl=ro#v=onepage&q&f=false> [acessado em 13 de fevereiro de 2014].

25 ICANN (2005) Principles for the Delegation and Administration of Country Code Top-Level Domains. Acessível em <http://archive.icann.org/en/committees/gac/gac-cctldprinciples-23feb00.htm > [acessado em 13 de fevereiro de 2014].

– APTLD, América do Norte – NATLD e América do Sul – LACTLD). A ICANN está elaborando Modelos de Responsabilidade como uma forma menos formal de desenvolver ligações com as operadoras de domínio de país.

Nomes de domínio internacionalizados

A Internet era originariamente um meio cujo idioma predominante era o inglês. Por meio do crescimento rápido, ela se tornou um instrumento global de comunicação com um número crescente de usuários não falantes do idioma inglês. Por muito tempo, a falta de elementos multilíngues na infraestrutura da Internet era uma das principais limitações para seu futuro desenvolvimento.

Em maio de 2010, após um longo período de testes e incertezas políticas, a ICANN passou a aprovar TLDs em uma ampla gama de scripts, inclusive Chinês, Árabe e Cirílico. A introdução de nomes de domínio internacionalizados (IDNs) é considerada um dos principais êxitos do regime de governança da Internet.

Servidores-raiz

No topo da estrutura hierárquica do DNS, os servidores-raiz atraem muita atenção, principalmente em discussões sobre planos de ação e discussões acadêmicas no âmbito das questões de governança da Internet.

Situação atual

A função e robustez do DNS podem ser exemplificadas analisando a preocupação de a Internet entrar em colapso e os servidores-raiz serem consequentemente desabilitados. Primeiramente, existem 13 servidores-raiz distribuídos pelo mundo, o maior número tecnicamente possível: 10 nos Estados Unidos, 1 na Suécia, 1 nos Países Baixos e 1 no Japão; dos 10 existentes nos Estados Unidos, muitos são operados por órgãos governamentais do país. Se um servidor cair, os 12 remanescentes continuam funcionando. Mesmo se todos os 13 servidores-raiz caíssem simultaneamente, a resolução dos nomes de domínio em endereços IP (a principal função dos servidores-raiz) continuariam em outros servidores de nomes de domínio, distribuídos hierarquicamente na Internet.[26]

26 A lista de servidores da zona-raiz, os seus nodos e posições e as organizações de gerenciamento está acessível em <http://www.root-servers.org> [acessado em 13 de fevereiro de 2014].

Portanto, centenas de servidores de nomes de domínio contêm cópias do arquivo de zona-raiz e uma queda imediata e catastrófica da Internet não poderia ocorrer. Levaria certo tempo antes que consequências funcionais sérias fossem percebidas e nesse tempo seria possível reativar os servidores originais ou criar servidores novos.

O sistema de servidores-raiz é consideravelmente fortalecido pelo sistema AnyCast,[27] que replica servidores-raiz em todo o mundo. Isso oferece muitas vantagens, inclusive maior robustez ao DNS e maior rapidez na resolução de endereços da Internet (com o sistema AnyCast, os servidores de resolução ficaram mais próximos dos usuários finais).

Os 13 servidores-raiz são administrados por diversas organizações:[28] instituições acadêmicas/públicas (6), empresas comerciais (4) e instituições governamentais (3). As instituições que administram servidores-raiz recebem um arquivo de zona-raiz proposto pela IANA (ICANN) e aprovado pelo governo dos Estados Unidos (Departamento de Comércio). Uma vez aprovado o conteúdo pelo Departamento de Comércio, ele é inserido no servidor-raiz mestre operado pelo VeriSign nos termos do seu contrato com o referido Departamento.[29] O arquivo no servidor-raiz mestre é, na sequência, automaticamente replicado em todos os outros servidores-raiz. Assim sendo, em teoria é possível para o governo dos Estados Unidos realizar mudanças unilaterais em todo o DNS. Isto é uma fonte de preocupação para muitos governos.

Questões

Internacionalização do controle dos servidores-raiz

Muitos países externaram sua preocupação sobre o acordo atual no qual a tomada de decisão final sobre o conteúdo dos servidores-raiz continua sendo responsabilidade de um país (os Estados Unidos). Houve muitas propostas no processo de governança da Internet, entre as quais a adoção da convenção raiz, que colocaria a comunidade internacional no comando da supervisão dos planos de ação dos servidores-raiz ou, pelo menos, concederia aos estados-nações direitos sobre seus próprios nomes de domínio nacionais.

27 ISC Inc. (2003) Hierarchical Anycast for Global Distribution. Acessível em <http://ftp.isc.org/isc/pubs/tn/isc-tn-2003-1.htm> [acessado em 13 de fevereiro de 2014].

28 Servidores-raiz da IANA. Acessível em <http://www.iana.org/domains/root/servers> [acessado em 9 de agosto de 2014].

29 O arquivo de zona-raiz está disponível ao público e <http://www.iana.org/domains/root/files> [acessado em 9 de agosto de 2014].

Novas possibilidades para soluções estão abertas com o anúncio do governo dos EUA (NTIA) de renunciar à supervisão da IANA e passá-la a novos mecanismos/órgãos. O processo de transição, cuja expectativa de conclusão é 30 de setembro de 2015, deverá ser norteado pelos seguintes princípios[30]:

-Apoiar e melhorar o modelo de multissetoriais.

-Manter a segurança, estabilidade e resiliência do DNS da Internet.

-Atender às necessidades e expectativas dos clientes e parceiros globais referentes aos serviços da IANA.

-Manter a abertura da Internet.

Servidores-raiz alternativos – viabilidade e riscos

A criação de um servidor raiz alternativo é tecnicamente simples. A principal questão é quantos seriam os servidores do referido servidor alternativo ou, mais precisamente, quantos computadores na Internet o sinalizariam quando da resolução de nomes de domínio. Sem os usuários, qualquer DNS alternativo se torna inútil. Algumas tentativas de criar um DNS alternativo foram feitas: Open NIC, New.net e Name.space. A maioria delas não deu certo, representando apenas uma pequena porcentagem de usuários da Internet.

Discussão conceitual: sistema de servidor-raiz único x alternativo

Por um bom tempo, o princípio do servidor-raiz único era considerado um dos principais mantras da Internet, que supostamente não deveria ser abordado ou discutido. Diversos argumentos foram apresentados para evitar quaisquer debates sobre alternativas ao servidor-raiz único. Um dos argumentos é que o atual sistema (servidor-raiz único) evita o risco de o DNS ser usado por alguns governos para a censura.[31] No entanto, o argumento da censura, contrário a mudanças das normas

30 A NTIA (2014) anuncia intenção de transferir as principais funções dos nomes de domínio da Internet. Acessível em <https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions> [acessado em 9 de agosto de 2014].

31 As autoridades norte-americanas acreditam que a Internet é valiosa demais para ser administrada ou para ficar sob controle de um órgão internacional como a ONU: "O risco é a burocratização da Internet e da inovação", afirmou Michael Gallagher, funcionário do Departamento de Comércio dos EUA que administrou o vínculo do governo com a ICANN. O Sr.Gallagher e outros apoiadores da ICANN também apontaram que os países que mais demandam contribuição internacional – China, Líbia, Síria e Cuba – possuem governos não democráticos. Permitir que estas nações influenciem como a Internet funciona poderia prejudicar a liberdade de expressão, eles afirmaram. (Fonte: Rhoads C [2006] Endangered Domain: In Threat to Internet's Clout, Some Are Starting Alternatives. The Wall Street Journal, 19 de janeiro de 2006; p. A1).

referentes ao DNS, está perdendo espaço do ponto de vista funcional. Os governos não precisam controlar o sistema DNS ou o arquivo de zona-raiz para introduzir a censura. Eles já contam com ferramentas mais eficientes, com base na filtragem do tráfego da Web.

Um argumento mais sólido é o de que quaisquer servidores-raiz alternativos poderiam levar à fragmentação e até mesmo à desintegração final da Internet, incluindo um possível cenário de desintegração violenta. A fragmentação da Internet poderia colocar em perigo uma das principais funções da Internet – o sistema de comunicação global unificado. O quão real é este perigo? Vittorio Bertola faz uma análise abrangente deste desafio.[32]

O papel dos Estados Unidos no gerenciamento dos servidores-raiz –o paradoxo do poder

A possibilidade de remover os nomes de domínio de outros países da Internet tem sido frequentemente discutida nos debates sobre a principal função dos EUA no gerenciamento dos servidores-raiz. O poder potencial de remover um país da Internet (ao eliminar o nome de domínio do país) dificilmente pode ser considerado como um poder, pois não tem utilidade efetiva. O principal elemento do poder é forçar o outro lado a agir da forma desejada por quem tem o poder. O uso do poder dos Estados Unidos poderia gerar consequências não intencionais, entre as quais fazer com que países e regiões estabeleçam suas próprias Internets. Diante de tal cenário, a Internet talvez se desintegrasse e os interesses dos EUA enfrentariam perigos (a predominância dos valores dos Estados Unidos na Internet, o idioma inglês como a lingua franca da Internet, a predominância de empresas na área do comércio eletrônico e de serviços da Internet baseadas nos Estados Unidos). Este poder sobre os servidores-raiz não tem sido utilizado nem mesmo no caso de conflitos militares entre os Estados Unidos e outros países (ex., Iugoslávia, Iraque e Líbia).

Acesso à Internet: Provedores de serviços da Internet (ISPs)

Como os ISPs conectam usuários finais à Internet, eles são os que cumprem as normais legais da Internet de forma mais direta e simples. É por isso que muitos países começaram a concentrar seus esforços no cumprimento da lei nos ISPs.

32 Bertola V (sem data) Oversight and multiple root server systems. Acessível em <http://wgig.org/docs/book/Vittorio_Bertola.htm> [acessado em 13 de fevereiro 2014].

Questões

Monopólios das telecomunicações e os ISPs

É comum em países onde há monopólios das telecomunicações que tais monopólios também forneçam o acesso à Internet. Os monopólios excluem outros ISPs da entrada neste mercado e inibem a competitividade, resultando em preços mais altos e frequentemente QoS mais baixa, além de não conseguir reduzir a exclusão digital. Em alguns casos, os monopólios das telecomunicações toleram a existência de outros ISPs, mas interferem no nível operacional (ex., fornecem banda larga menor ou provocam interrupções nos serviços).

Responsabilidade dos ISPs sobre direitos autorais

Comum a todos os sistemas jurídicos é o princípio de que o ISP não pode ser responsabilizado por hospedar materiais que violam direitos autorais quando tal ISP não tem conhecimento da situação. A principal diferença reside na ação judicial tomada após o ISP ser informado de que o material que está hospedando viola os direitos autorais.

As leis dos EUA e da UE adotam o procedimento de Notificação e Retirada, que solicita ao ISP a remoção de tal material para evitar que ele seja processado. A lei do Japão adota um procedimento mais equilibrado, por meio do procedimento Notificação-Notificação e Retirada, que concede ao usuário do material o direito de reclamar contra a solicitação de remoção.

A abordagem de conferir responsabilidade limitada aos ISPs tem sido, no geral, apoiada por precedentes. Alguns dos casos mais importantes nos quais os ISPs foram isentados da responsabilidade de hospedar materiais que violaram a lei dos direitos autorais são o Caso da Cientologia (Países Baixos),[33] RIAA vs Verizon (Estados Unidos)[34], SOCAN vs

33 "O Tribunal de Recursos de Haia decidiu contra a Igreja da Cientologia em seu processo de violação de direitos autorais contra a escritora holandesa e sua ISP, XS4ALL. A escritora, ex-praticante da cientologia, publicou em um sítio web partes de documentos confidenciais da Igreja, e a igreja a processou nos termos da Lei Holandesa dos Direitos Autorais de 1912. Em 1999, o Tribunal Distrital decidiu a favor dos réus, citando preocupações com a liberdade de expressão. No entanto, tal tribunal também decidiu que os ISPs deveriam ser responsabilizados por materiais publicados que pudessem violar os direitos autorais existentes. O Tribunal de Recursos ratificou a primeira decisão, mas anulou a segunda, afirmando que os ISPs não eram responsáveis pelos materiais publicados". Para mais informações, consultar Gelman L (2003) Church of Scientology Loses Copyright Infringement Case in Dutch Court. Acessível em <http://cyberlaw.stanford.edu/packets001638.shtml> [acessado em13 de fevereiro de 2014].

34 Para mais informações sobre este caso ver Electronic Privacy Information Center (2004) RIAA vs Verizon. Acessível em <http://epic.org/privacy/copyright/verizon/> [acessado em 13 de fevereiro de 2014].

CAIP (Canadá)[35] e mais recentemente Scarlet vs SABAM (Bélgica).[36] Não obstante, os anos recentes testemunharam pressão crescente sobre o ISPs para lidar com as questões de direitos autorais, uma vez que sua posição como intermediadores entre usuários finais e conteúdo da Internet os coloca na melhor posição para controlar o acesso. Especulou-se sobre o referido argumento na promoção das disposições jurídicas como a Lei Hadopi na França, obrigando os ISPs a intervir no caso de suspeitas de violação aos direitos autorais.

O papel dos ISPs nas políticas de conteúdo

VER A SEÇÃO 3
PARA UMA DISCUSSÃO MAIS APROFUNDADA SOBRE PROPRIEDADE INTELECTUAL

Sob crescente pressão oficial, os ISPs estão gradualmente, embora com relutância, envolvendo-se com políticas de conteúdo (ex., conteúdo difamatório ou fraudulento). Ao agir dessa forma, eles talvez tenham que seguir dois caminhos possíveis. O primeiro é o cumprimento da regulação governamental e o segundo, que tem como base a autoregulação, é para os ISPs decidirem por conta própria o que seria um conteúdo adequado. Isto cria o risco de privatizar o controle de conteúdo, com os ISPs assumindo as responsabilidades dos governos.

O papel dos ISPs nas políticas antispams

Os ISPs são frequentemente considerados as principais instituições envolvidas com iniciativas antispam. Geralmente, os ISPs têm suas próprias iniciativas de redução de spam, por meio de filtragem técnica ou pela aplicação de políticas antispam. O relatório da UIT sobre spam afirma que os ISPs deveriam ser responsáveis pelo spam e propõe um código de conduta antispam, que deveria incluir duas provisões fundamentais:

35 A Suprema Corte do Canadá rejeitou o argumento da Sociedade dos Compositores, Autores e Editores de Música do Canadá de que os ISPs canadenses deveriam pagar royalties porque alguns de seus clientes baixaram obras protegidas por direitos autorais (SOCAN vs CAIP). Para mais informações acessar <http://www.canlii.org/en/ca/scc/doc/2004/2004scc45/2004scc45.html> [acessado em 13 de fevereiro de 2014].

36 "A SABAM (sociedade coletiva da Bélgica – Société belge des auteurs, compositeurs et éditeurs) queria que o ISP Scarlet instalasse um sistema de filtragem geral para todas as comunicações de entrada e saída que passassem por seus serviços, bem como que bloqueasse comunicações possivelmente ilegais. Na Primeira Instância, embora tenha recusado a responsabilidade do ISP, o Tribunal de Bruxelas concluiu que a reivindicação da SABAM era legítima e que o sistema de filtragem tinha que ser empregado. A Scarlet recorreu e o processo foi enviado ao Tribunal de Justiça da União Europeia. Em sua decisão, o Tribunal de Justiça decidiu que o sistema de filtragem e bloqueio para todos os clientes por um período ilimitado, in abstracto, e como medida cautelar infringe direitos fundamentais, mais especificamente o direito à privacidade, à liberdade de comunicação e à liberdade de informação. Além disso, viola o direito das ISPs de conduzir negócios". Para mais informações, ver Scarlet v SABAM: a win for fundamental rights and Internet freedoms EDRi-gram newsletter No. 9.23, 30 Novembro de 2011. Acessível em <http://edri.org/edrigramnumber9-23scarlet-sabam-win-fundamental-rights> [acessado em 15 de março de 2014].

- O ISP deve proibir seus usuários de enviar spams.
- O ISP não pode se associar com ISPs que não aceitam um código de conduta similar.[37]

O problema do spam expõe os ISPs a novas dificuldades. Por exemplo, a filtragem antispam da Verizon resultou em processo judicial, pois também bloqueou mensagens legítimas, causando transtorno a usuários que não receberam os e-mails legítimos.[38]

Acesso à internet: provedores de banda larga da Internet (IBPs)

A arquitetura de acesso da Internet consiste em três camadas. Os ISPs que conectam os usuários finais constituem a Camada 3, as camadas 1 e 2 consistem em provedores de banda larga da Internet (IBPs) e a camada 1 consiste nos principais IBPs. Eles costumam estabelecer conexões entre pares[39] com outros IBPs da Camada 1. A principal diferença entre os IBPs da Camada 1 e da Camada 2 é que os IBPs da Camada 1 trocam tráfego entre si, ao passo que os IBPs da Camada 2 têm que pagar tarifas de trânsito aos provedores da Camada.[40] A Camada 1 geralmente é administrada por grandes empresas, como AT&T, Verizon, Level 3 Communications, Sprint, e NTT Communications.

37 Williams F (2006) ISPs should be liable for spam, says UN report, Financial Times. Acessível em <http://www.ft.com/intl/cms/s/09b837c0-ae02-11da-8ffb-0000779e2340,Authorised=false.html?_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2F09b837c0-ae02-11da-8ffb-0000779e2340.html%3Fsite edition%3Dintl&siteedition=intl&_i_referer=#axzz1l2VhnlN0> [acessado em 13 de fevereiro de 2014].

38 Shannon V (2006) The end user: Junk payout in spam case – Technology – International Herald Tribune. Acessível em <http://www.nytimes.com/2006/04/12/technology/12iht-PTEND13.1523942.html> [acessado em 13 de fevereiro de 2014].

39 Nas redes de computadores, o peering é uma interconexão voluntária de redes de Internet separadas administrativamente com o objetivo de trocar tráfego entre clientes de cada rede. A definição pura de peering é settlement free (livre de custos) ou sender keeps all (o emissor fica com tudo), o que significa que as partes não têm que pagar uma a outra pela troca de tráfego; em vez disso, as suas receitas advêm de seus próprios clientes. A prática de peering requer interconexão física das redes, a troca de informações de roteamento por meio do Border Gateway Protocol (BGP) e geralmente é acompanhada por acordos de peering sob formalidades variadas, desde "apertos de mão" a contratos extensos. (Fonte: Wikipédia).

40 Os Provedores de Banda Larga de Internet Camada 2 geralmente são chamados de ICP (Internet connection points) ou Internet gateways.

Questões

A infraestrutura da Internet deveria ser considerada serviço público?

Os dados da Internet podem circular em qualquer meio de telecomunicações. Na prática, instalações como os backbones da Camada 1 (isto é, rotas principais de dados entre redes grandes estrategicamente interconectadas e roteadores centrais na Internet), que frequentemente têm cabos óticos e ligações via satélite, tornaram-se cruciais para o funcionamento da Internet, sendo que essa posição crucial dentro da rede da Internet outorga a seus donos poder de mercado para impor preços e condições para a prestação de seus serviços.[41] Por fim, o funcionamento da Internet poderia depender de decisões por parte de donos de outros backbones centrais.

A CONFIABILIDADE PODE SER GARANTIDA?

É possível para a comunidade global da Internet solicitar garantia das maiores empresas da Internet e operadoras de telecomunicações de que a infraestrutura crítica da Internet funcione de forma confiável? A tendência em discussão é a imposição de determinados requisitos públicos sobre as operadoras privadas de infraestrutura da Internet.

Os IBPs e a infraestrutura crítica

No início de 2008, houve uma interrupção em um dos principais cabos da Internet no Mediterrâneo, perto do Egito. Este incidente colocou em perigo o acesso à Internet em uma vasta região que se estendia até a Índia. Dois incidentes similares aconteceram em 2007 (o cabo de Internet perto de Taiwan e o principal cabo de In-

41 Dois casos relacionados foram mencionados em Spaink K (2002) Freedom of the Internet, our new challenge. Acessível em <http://www.spaink.net/english/osce_internetfreedom.html> [acessado em 13 de fevereiro de 2014]. No primeiro caso, uma ação judicial foi interposta contra uma página da Web com conteúdo nazista duvidoso hospedado pelo Flashback na Suécia. Os tribunais decidiram que a página não violava as leis suecas antinazistas. Contudo, um ativista antinazista dedicado organizou uma forte campanha contra a Flashback, dessa forma pressionando o ISP da Flashback, a Air2Net, e o principal operador de backbone, o MCI/WorldCom. Sob pressão desta campanha, o MCI/WorldCom decidiu desconectar a Flashback, apesar da falta de fundamentação jurídica para isso. A tentativa da Flashback de encontrar um provedor alternativo não deu certo, uma vez que a maioria deles também estava conectada pelo backbone operado pelo MCI/WorldCom. O segundo caso ocorreu nos Países Baixos. Um pequeno provedor ISP holandês, o Xtended Internet, foi desconectado por seu provedor upstream baseado nos Estados Unidos sob pressão do lobby da cientologia.

ternet do Paquistão), mostrando claramente que a infraestrutura da Internet é parte de uma infraestrutura crítica nacional e global. A interrupção dos serviços de Internet podem afetar a economia geral e a vida social de determinada região. A possibilidade de haver interrupção levanta algumas questões:

- Os principais cabos de Internet estão adequadamente protegidos?
- Quais são as respectivas funções dos governos nacionais, das organizações internacionais e das empresas privadas na proteção dos cabos de Internet?
- De que forma podemos administrar os riscos associados a possível interrupção dos principais cabos de Internet?

Liberalização das telecomunicações e o papel dos ISPs e IBPs

Existem visões opostas sobre até que ponto os ISPs e IBPs devem estar sujeitos aos instrumentos internacionais existentes. Os países desenvolvidos argumentam que a liberalização das regras concedida pela OMC às operadoras de telecomunicações também pode ser estendida aos ISPs. Uma interpretação restritiva enfatiza o fato de que o regime das telecomunicações da OMC se aplica somente ao mercado das telecomunicações. A regulação do mercado de ISP requer novas regras da OMC.

Neutralidade da rede

O sucesso da Internet reside em seu design, que tem como base a neutralidade da rede. Desde o início, o fluxo de todo o conteúdo na Internet, oriundo de start-ups ou de empresas grandes, era tratado sem discriminação. Novas empresas e inventores não precisavam de permissão ou de poder de mercado para inovar na Internet.

A relevância da neutralidade da rede para o êxito da Internet é elemento-chave. O debate tem atraído uma ampla gama de atores: desde o Presidente dos Estados Unidos a ativistas de base a favor dos direitos humanos. A forma com que a neutralidade da rede é tratada pode influenciar o futuro desenvolvimento da Internet.

Situação atual

Paradoxalmente, o controle de tráfego da Internet sempre esteve presente. Desde o início da conexão via modem de linha discada à Internet, existe uma lacuna entre a banda disponível e as necessidades de banda do usuário. Para enfrentar este desafio e fornecer serviço de qualidade, as operadoras de Internet (empresas de telecomunicações e ISPs) – também comumente denominadas de carriers – usaram

diversas técnicas de controle de tráfego para priorizar determinado tráfego. Por exemplo, o tráfego de Internet que transmite conversas de voz por meio de serviços VoIP (ex., Skype) deveria ter prioridade sobre o tráfego que transmite simples e-mails: podemos ouvir atrasos nas mensagens de voz do Skype, mas não percebemos pequenos atrasos na troca de e-mails. A necessidade de controlar o tráfego é especialmente importante hoje, com o aumento das demandas por banda larga de alta qualidade: uma quantidade crescente de usuários faz regularmente chamadas de voz e vídeo na Internet (Skype, Google Hangout, teleconferências), joga jogos online ou veem programas de televisão e filmes em alta definição (HD) (ex., serviços como Hulu ou Netflix). O controle de tráfego é importante para a comunicação sem fio, por um lado devido à expansão do uso dos dispositivos móveis e, por outro lado, devido aos limites técnicos do espectro sem fio.[42] O prognóstico da Cisco é que até 2020 em torno de 50 bilhões de dispositivos estarão conectados à Internet no âmbito do conceito em expansão da Internet das Coisas.[43]

O controle de tráfego está se tornando cada vez mais sofisticado com relação ao roteamento do tráfego de Internet da melhor forma para o fornecimento de um serviço de qualidade, evitando o congestionamento e eliminando a latência e a instabilidade. A primeira discordância na interpretação dos princípios da neutralidade da rede discutiu se o controle de tráfego de modo algum deveria ser permitido. Os puristas da neutralidade da rede argumentaram que " todos os bits são criados iguais" e que todo o tráfego da Internet deve ser tratado igualmente. As telecoms e os ISPs contestaram este ponto de vista, argumentando que são os usuários que devem ter acesso igual aos serviços da Internet e caso isso aconteça, o tráfego à Internet não deve ser tratado com igualdade. Se houver igualdade de tratamento no tráfego de vídeo e e-mail, os usuários não terão uma boa recepção de streaming de vídeo, porém não notariam alguns segundos de atraso no recebimento de e-mails. Nem mesmo os puristas da neutralidade contestaram essa lógica.

42 As tecnologias de transmissão de sinal – tanto sem fio (ex. LTE) quanto de cabos óticos (ex. DWDM) prometem resolver o problema do "esgotamento da banda larga" por meio de muito mais especificações de banda larga (até terabits por segundo). A relação demanda-oferta, porém é permanente.

43 Cisco (sem data) The Internet of Things. Acessível em <http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html>[acessado em 10 de agosto de 2014].

Questões

No debate da neutralidade da rede, há crescente consenso que é necessário um controle de tráfego adequado. A principal questão é como interpretar o adjetivo "adequado". Existem duas áreas além das questões técnicas – econômicas e de direitos humanos – nas quais os debates sobre controle de tráfego e neutralidade da rede são especialmente acalorados.

Questões econômicas

Durante as últimas décadas, muitas operadoras de rede relevantes – inclusive as telecoms e os ISPs – alteraram seus modelos de negócios: além de fornecerem acesso à Internet a residências e negócios, elas introduziram seus próprios serviços de VoIP (telefonia via Internet) ou IPTV (televisão via Internet), vídeo sob demanda (comparável a alugar), portais de download de música e vídeo, etc. Agora elas estão competindo não somente com seus concorrentes para fornecer conexões mais baratas, mais rápidas e de melhor qualidade, mas também com os provedores de serviços over-the-top (OTT) provedores de conteúdo e serviços como Google, Facebook, Netflix e Skype.

O controle de tráfego talvez seja uma ferramenta importante para tornar o serviço e fornecimento de conteúdo competitivo, priorizando pacotes de acordo com preferências baseadas nos negócios. Por exemplo, determinada operadora poderá decidir diminuir ou proibir totalmente o fluxo de pacote de dados de uma empresa concorrente (como Skype ou Google Voice) a usuários finais por meio de sua rede, ao mesmo tempo priorizando pacotes de dados de seu próprio serviço interno (como a telefonia IP ou televisão via Internet que oferece a seus clientes).[44]

Ao mesmo tempo, as operadoras argumentam que a expansão da demanda da banda larga aumentou o investimento em infraestrutura básica. Ao observar que os provedores de serviços OTT foram os que mais contribuíram para a expansão da demanda e os que mais se beneficiaram com a melhoria da infraestrutura, elas sugerem modelos de políticas de rede multicamadas, que solicitariam aos provedores de serviços OTT que pagassem pelo serviço adicional a clientes das operadoras (usuários finais da Internet) se quisessem a garantia da qualidade do serviço. Em tais casos, o controle de tráfego seria novamente usado por motivos econômicos em vez de técnicos. Para buscar

44 The Economist (2009) America insists on net neutrality: The rights of bits. 24 de setembro. Acessível em <http://www.economist.com/node/14517422> [acessado em 13 de fevereiro de 2014].

maneiras de aumentar as receitas, as telecoms planejaram um novo tipo de ofertas. As tarifas zero oferecidas a clientes de provedores de telecom móveis permitem o uso ilimitado (livre) de aplicativos específicos como o Facebook ou a Wikipédia; embora isso seja definitivamente vantajoso para os clientes, tais tarifas priorizam determinados serviços em detrimento de outros. Além disso, as telecoms se referem a "serviços especializados" – como ofertas de streaming de vídeo em HD que demandam banda larga de alta velocidade ou soluções futuras de e-saúde – que talvez precisem ser oferecidos no futuro e necessitariam de alta qualidade e, consequentemente, tratamentos específicos. Propostas sobre uma Internet de multicamadas têm estado no centro das discussões sobre a neutralidade da rede há anos. A camada de negócios também foi proposta na forma de "serviços adicionais online" pela Verizon e pelo Google na Legislative Framework Proposal for an Open Internet (Proposta de Estrutura Legislativa para uma Internet Aberta)[45] em 2010. Os proponentes argumentam que isto aumentaria as escolhas aos usuários e incentivaria o investimento em infraestrutura; os oponentes temem que a rede de melhor esforço irá sofrer e por fim desaparecer, uma vez que tanto a camada econômica quanto a camada de negócios usariam efetivamente os mesmos "tubos" (ou seja, espectro e cabos sem fio).

Paralelamente, o mercado mudou a forma como a Internet funciona: para reduzir os custos e o tempo de trânsito, os provedores de conteúdo se aproximaram dos usuários ao estabelecer as Redes de Distribuição de Conteúdo (CDNs) – fazendo o cachê de servidores colocados próximos aos pontos IXP ou em grandes telecoms regionais. Isto aumentou o desempenho das redes e os custos – apesar de que somente para as empresas de serviços OTT que têm condições de construir ou alugar CDNs e pagar as empresas de telecomunicações pela instalação.[46]

45 O texto integral da Verizon and Google Legislative Framework Proposal for an Open Internet está acessível em <https://static.googleusercontent.com/media/www.google.com/en//googleblogs/pdfs/verizon_google_legislative_framework_proposal_081010.pdf>acessado em 13 de fevereiro de 2014].

46 McMillan R (2014) What everyone gets wrong in the debate over net neutrality. Acessível em <http://www.wired.com/2014/06/net_neutrality_missing/>[acessado em 10 de agosto de 2014].

INTERNET MULTICAMADAS

O tráfego da Internet atualmente é distribuído com "os melhores esforços": isto não implica em garantia de QoS, velocidade efetiva ou tempo de entrega dos pacotes de dados. Em vez disso, os usuários compartilham a banda disponível e obtêm taxas de bit (velocidade) variáveis, dependendo da carga de tráfego do momento[47] O controle de tráfego, dessa forma, tem um papel importante na real qualidade do serviço oferecido aos usuários finais.

O conceito de Internet mulitcamada se refere a introduzir uma "camada de negócios"à Internet, ou seja, serviços especiais com QoS garantida, além dos melhores esforços. Os proponentes explicam que a camada de negócios funcionaria concomitantemente à "camada econômica" (a Internet como a conhecemos hoje), que continuaria baseada nos melhores esforços; além disso, eles dizem que os provedores de serviços OTT poderiam ainda decidir executar seus serviços por meio da rede de melhores esforços sem custo, caso quisessem isso.

Questões de direitos humanos

As consequências da violação dos princípios da neutralidade da rede não são apenas econômicas. A Internet se tornou muito mais importante do que algo criado visando exclusivamente à economia – ela se tornou um dos pilares da sociedade moderna associada aos direitos humanos, inclusive ao acesso à informação, liberdade de expressão, saúde e educação. Modelos integralmente baseados no lucro (mesmo os que claramente resultam em mais inovação e investimento) podem aumentar o abismo entre os que têm e os que não têm: enquanto os ricos usariam serviços online ilimitados com qualidade total, os pobres por fim acabariam ficando com os serviços inúteis, de melhores esforços ou apenas com os serviços prioritários, escolha que seria feita pelos provedores de serviços de telecomunicações com base nos seus interesses econômicos. Colocar em risco a abertura da Internet poderia, dessa forma, impactar direitos fundamentais .

Além disso, a capacidade de controlar o tráfego de rede com base na origem ou no destino, no serviço ou no conteúdo, poderia oferecer às autoridades a oportunidade de filtrar o tráfego da Internet com conteúdo condenável ou delicado relacionado aos valores político, ideológico, religioso ou cultural de determinado país, ou a outros

47 A banda larga (bit rate) acordada em um contrato com o ISP é, na verdade, somente o máximo de banda acessível em vez da velocidade efetiva garantida.

valores. Isto abre possibilidades para a censura política por meio do controle do tráfego da Internet.

USUÁRIOS OU CLIENTES?

O debate da neutralidade da rede desencadeia diferenças linguísticas. Os proponentes da neutralidade da rede priorizam os "usuários" da Internet, enquanto os outros – principalmente os atores comerciais – os descrevem como "clientes". Usuários da Internet são mais do que simplesmente clientes; o termo "usuário" implica participação ativa no desenvolvimento da Internet por meio de redes sociais, blogs e outras ferramentas e o papel importante que eles desempenham na hora de decidir o futuro da Internet. Os clientes, por outro lado, como quaisquer outros clientes, podem escolher se querem ou não comprar os serviços ofertados. O status deles na Internet se baseia no contrato com o ISP e as regras de proteção dos clientes. Além disso, os clientes não devem ter nenhum papel em decidir a forma de funcionamento da Internet.

Quem são os principais atores e quais são seus argumentos?
A posição dos principais atores está sempre mudando. Por exemplo, a proposta de 2010 do Google-Verizon 2010 para uma abordagem intermediária à neutralidade da rede mexeu no posicionamento dos principais atores.[48] O Google foi considerado um dos principais proponentes da neutralidade da rede; entre outros proponentes estão defensores dos consumidores, empresas online, algumas empresas de tecnologia, diversas empresas grandes de aplicativos de Internet, entre as quais Yahoo!, Vonage, Ebay, Amazon, EarthLink, e empresas de software como a Microsoft.

Entre os que são contrários à neutralidade da rede estão as principais empresas de telecomunicações, ISPs, produtores de equipamentos e hardware de rede e produtores de materiais de vídeo e multimídia. Os argumentos que usam contra qualquer regulação relacionada têm como prioridade o mercado, a começar pela necessidade de oferecer o que os clientes querem. Em direção oposta às tendências comuns das operadoras de telecomunicações contra qualquer regulação da neutralidade da rede, a proposta da ETNO ao CMTI-12 requisitava regulação internacional –evitando que outras regulações nacionais protegessem a neutralidade da rede! No entanto, seus pares nos Esta-

48 Ogg E (2010) Report: Google, Verizon reach Net neutrality deal. Acessível em <http://news.cnet.com/8301-31021_3-20012703-260.html?tag=mncol;mlt_related> [acessado em 13 de fevereiro de 2014].

dos Unidos, como a Verizon, são contrários às iniciativas da ETNO.[49] Existem quatro principais argumentos no debate sobre a neutralidade da rede *(Tabela 1)*.

Princípios básicos

Em anos recentes, os debates sobre políticas e regulamentos da neutralidade da rede cristalizaram alguns princípios fundamentais de tal neutralidade da rede:[50]

-Transparência: As operadoras devem fornecer informações completas e exatas sobre suas práticas de gestão de rede, capacidade e qualidade de seus serviços aos clientes, de forma que sejam compreensíveis para o usuário médio.

-Acesso: Os usuários deveriam poder ter acesso irrestrito a qualquer conteúdo, serviço ou aplicativo [jurídico] [com garantia de qualidade mínima do serviço para uso significativo, conforme indicado pelo regulador] ou poder conectar qualquer hardware que não prejudique a rede.

- (Não)discriminação: Os operadores não deveriam fazer nenhuma discriminação [ou discriminação razoável] do tráfego com base no(a):

- Origem do emissor ou receptor.

-Tipo de conteúdo, tipo de aplicativo e serviço [com concorrência justa – sem discriminação contra concorrentes indesejados ou serviços de provedores de OTT].

-"Razoável" poderia ser qualquer prática para benefício público (garantir a qualidade do serviço, a segurança e a resiliência da rede, inovações e mais investimentos, redução dos custos etc.) e não somente para vantagens comerciais.

Entre outros princípios debatidos com mais frequência em fóruns internacionais como as reuniões do IGF e o diálogo EuroDig estão:

-A preservação da liberdade de expressão, o acesso à informação e escolha.

-A garantia da qualidade mínima do serviço, da segurança e da resiliência da rede.

-A preservação de incentivos para investimentos.

-O estímulo às inovações [inclusive oportunidades para novos modelos de negócios e negócios inovadores, isto é, novos participantes].

49 McCullagh D (2012) European ISPs defend U.N. Internet tax. Acessível em <http://news.cnet.com/8301-13578_3-57496581-38/european-isps-defend-u.n-internet-tax/> [acessado em 13 de fevereiro de 2014].

50 Os elementos que ainda são polêmicos e a serem negociados no futuro estão em colchetes.

-A definição de direitos, funções e responsabilidades de todas as partes envolvidas (prestadores de serviços, reguladores e usuários), inclusive o direito de recurso e reparação.
- A prevenção de práticas anticoncorrenciais.
- A criação de um ambiente de mercado que possibilitaria aos usuários escolher e alterar com facilidade sua operadora de rede.
- A proteção do interesse de pessoas menos favorecidas, como pessoas com deficiência e usuários e empresas nos países em desenvolvimento.
- A manutenção da diversidade de conteúdo e serviços.

Abordagens políticas

Com o debate da neutralidade da rede, outra questão veio à tona: qual a função dos legisladores e reguladores com relação à política de banda larga e às práticas das operadoras? Um dos principais desafios dos reguladores é decidir se atuam antecipadamente (ex-ante), com o objetivo de evitar possíveis violações ao princípio da neutralidade da rede, ou se respondem com base na jurisprudência (ex-post) após a ocorrência da violação (e se ela ocorrer). Um dos desafios enfrentados pelos legisladores e formuladores de políticas é decidir se o problema deve ser tratado por meio de "lnormas vinculadas" – codificando os princípios à legislação – ou se uma "TES (hard law)" (diretrizes e políticas) é suficiente.[51]

Países desenvolvidos

Em resposta ao processo envolvendo a Comcast, a Comissão Federal de Comunicações dos Estados Unidos (FCC) adotou as diretrizes da neutralidade da rede como uma atualização de seus documentos programáticos de 2005,[52] que expressavam a necessidade de acessar e escolher conteúdo e dispositivos, e abordavam as questões da discriminação e transparência. Paralelamente, as decisões da FCC de apoio à neutralidade da rede foram rejeitadas no início de 2014 pelo tribunal de recursos dos Estados Unidos com base no mandato limitado da FCC. O tribunal de recursos obrigou a FCC a considerar liberar para as telecoms algum tipo de serviço "pague para obter preferência" ou a reclassificação da banda larga como um serviço público, dessa forma conseguindo autorização para fazer cumprir a neutralidade da rede. O quadro regulatório da UE sobre a comunicação eletrônica tem como

51 Radunovic V (2012) Network Neutrality in law – a step forwards or a step backwards? Diplo Blog. Acessível em <http://www.diplomacy.edu/blog/network-neutrality-law-%E2%80%93-step-forwards-or-step-backwards> [acessado em 13 de fevereiro de 2014].

52 FCC (2005) Policy statement. Acessível em <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf> [acessado em 13 de fevereiro de 2014].

TABELA 1

Argumento	*Proponentes*	*Opositores*
Argumento passado/futuro	Novas empresas de Internet foram desenvolvidas graças à arquitetura aberta da Internet e os usuários finais estão se beneficiando da inovação e da diversidade de serviços graças à neutralidade da rede. A neutralidade da rede irá preservar a arquitetura da Internet que possibilitou o desenvolvimento rápido e inovador da Internet até o momento.	O controle do tráfego é inevitável e a neutralidade nunca existiu. Além disso, já existem serviços arrendados não neutros, como as VPNs (redes privadas virtuais). Sem as restrições da neutralidade da rede, as empresas de Internet conseguem desenvolver novos serviços que serão de interesse do cliente, com QoS garantida.
Argumento Econômico	Sem a neutralidade da rede, a internet vai parecer TV a cabo: algumas poucas grandes empresas irão controlar o acesso e a distribuição de conteúdo, decidindo o que os usuários irão ver e qual o valor para ver tal conteúdo. Novos participantes e pequenas empresas não terão oportunidade para se desenvolver, principalmente nos países em desenvolvimento. Os prestadores de serviços OTT já pagam bastante para as telecoms por suas conexões de Internet e investem em infraestrutura, tais como servidores de cache.	Sem as restrições da neutralidade da rede em contratos comerciais com provedores de conteúdo e serviços, as operadoras de telecoms arrecadarão recursos, fazendo com que tenham maior interesse em investir em melhor infraestrutura. Uma melhor infraestrutura é o incentivo para novos serviços e inovações, mais personalizados de acordo com as necessidades do cliente, aumentando a receita para todos. Os provedores de serviços OTT também encontrarão valor em possíveis serviços inovadores com QoS, possibilitados pelas operadoras, se não forem limitados pelas disposições da neutralidade da rede.

Argumento ético	A Internet é o resultado de desenvolvimentos realizados por voluntários durante décadas. Eles investiram tempo e criatividade no desenvolvimento de tudo que existe na Internet, desde protocolos técnicos até conteúdo. A Internet é mais que um negócio – tornou-se patrimônio global da humanidade. Não é justificável que os frutos resultantes do investimento de uma enorme quantidade de tempo e criatividade sejam colhidos por apenas algumas empresas que limitarão a Internet a modelos de negócios restritos ao quebrar a neutralidade da rede, transformando a criatividade de muitos no lucro de poucos.	A neutralidade da rede é questionável eticamente porque as operadoras têm que investir na manutenção e expansão da infraestrutura da Internet para incentivar novos serviços, enquanto a maioria dos benefícios são usufruídos pelas empresas de "conteúdo" da Internet, como Google, Facebook e Amazon.
Argumento da regulação	A neutralidade da rede deve ser imposta pelo governo para preservar o interesse público. Qualquer forma de autorregulação deixará espaço para as operadoras violarem o princípio da neutralidade da rede. O mercado aberto não é suficiente uma vez que as grandes telecoms globais estão no centro da infraestrutura da Internet. Mesmo que haja a possibilidade de escolha, isto nem sempre é realizado porque os usuários precisam ter conhecimento técnico e jurídico, bem como consciência das consequências das várias escolhas disponíveis.	O desenvolvimento da Internet ocorreu devido à regulação pouco rígida ou devido à regulação nenhuma. A regulação rígida por parte do governo poderia bloquear a criatividade e o futuro desenvolvimento da Internet. O mercado aberto é baseado na escolha e os usuários sempre podem trocar de provedor de Internet se não estiverem satisfeitos com a oferta. A escolha do usuário e o mercado eliminarão as ofertas ruins e manterão as boas.

meta proteger a liberdade de expressão, a escolha do usuário e os direitos de acesso, em conjunto com o princípio da transparência; por outro lado, também enfatiza a necessidade de haver investimentos, concorrência justa sem discriminação e oportunidades para novos modelos de negócios, inclusive negócios inovadores.[53] Em 2004, o Parlamento Europeu adotou a Regulação do Mercado Único de Telecomunicações, com disposições claras sobre a neutralidade da rede (inclusive uma definição rigorosa e um quadro sólido para "serviços especializados").[54] Brasil,[55] Chile,[56] Eslovênia e os Países Baixos protegem a neutralidade por meio de leis nacionais.

Países em desenvolvimento

Devido à infraestrutura e banda larga limitadas, os reguladores dos países em desenvolvimento priorizam a política do uso aceitável – preços acessíveis e acesso justo para todos. Alguns levantam preocupações sobre a não discriminação transnacional, afirmando que o tráfego de todos os países deve ser tratado da mesma forma, sem preferência baseada nos custos de terminais. Além disso, certos países são mais sensíveis a aspectos culturais, políticos ou éticos internos, compreendendo assim o termo "uso (in)adequado" e seu controle de forma diferente dos outros países. Surgiram preocupações sobre a possibilidade dos modelos inovadores dos países desenvolvidos prejudicarem os mercados em desenvolvimento: ao priorizar os serviços de grandes empresas da Internet, os negócios e a concorrência emergentes seriam, além disso, reduzidos, ameaçando a inovação, o conteúdo e os serviços locais, bem como a diversidade da mídia. Algumas importantes políticas formais ou práticas regulatórias sobre a neutralidade da rede, no entanto, surgiram dos países em desenvolvimento. Entre outras posições poderão estar copiar o modelo emergente dos EUA e autorizar as telecoms nacionais a cobrar as OTTs globais pela preferência, dessa

53 Kroes N (2010) Net neutrality in Europe. Discurso dado pelo Vice Presidente da Comissão Europeia Comissário para Agenda Digital. Acessível em <http://europa.eurapid/press-release_SPEECH-10-153_en.htm?locale=en> [acessado em 13 de fevereiro de 2014].

54 La Quadrature du Net (2014) Net neutrality: a great step forward for the free Internet. Acessível em <http://www.laquadrature.net/en/net-neutrality-a-great-step-forward-for-the-free-internet> [acessado em 11 de agosto de 2014].

55 A versão em inglês do Marco Civil brasileiro está acessível em <http://giplatform.org/resources/text-brazils-new-marco-civil> [acessado em 10 de agosto de 2014].
Nota do tradutor: o endereço foi substituído por <https://www.publicknowledge.org/documents/marco-civil-english-version> [acessado em 6 de março de 2017].

56 TechnoLlama (2012) Chile enforces net neutrality for the first time, sort of. Acessível em <http://www.technollama.co.uk/chile-enforces-net-neut rality-for-the-first-time-sort-of> [acessado em 13 de fevereiro de 2014].

forma incrementando as receitas das telecoms incumbentes; ou, pelo contrário, fazendo cumprir a neutralidade da rede nacionalmente para convencer as OTTs a operarem fora dos Estados Unidos.

Organizações internacionais e ONGs

Muitas organizações internacionais e grupos de usuários também desenvolveram posições políticas referentes à neutralidade da rede. O Conselho da Europa (CoE), em sua Declaração do Comitê de Ministros sobre neutralidade da rede, enfatiza os direitos fundamentais à liberdade de expressão e informação;[57] a Internet Society (ISOC) promove sua abordagem voltada ao usuário que predominantemente enfrenta os problemas relacionados ao acesso, à escolha e transparência por meio do debate Open Inter-networking em vez do debate relacionado à neutralidade da rede.[58] O Diálogo Transatlântico de Consumidores (TACD), fórum das organizações de consumidores dos EUA e da UE, enfatizam ainda a exigência por comportamentos não discriminatórios por parte das carriers, solicitando que os EUA e a EU autorizem os reguladores a atuarem como protetores dos direitos dos usuários.[59] A neutralidade da rede e a Internet multicamadas foram bastante debatidas no processo da CMTI-12. O documento final da NETmundial em 2014 não incluiu a neutralidade da rede entre os princípios acordados, mas abriu para mais discussões sobre o tema, principalmente por parte do IGF, durante o IGF 2014.

Muitas ONGs estão especialmente preocupadas com o futuro do conteúdo e dos serviços online não comerciais e tampouco concorrentes, solicitando que sejam transmitidos por qualquer rede de carriers igual às redes comerciais. Também enfatizam os direitos dos grupos marginalizados – principalmente pessoas com deficiência – de usar conteúdo, serviços e aplicativos (inclusive os que demandam banda larga de alta velocidade) para suas necessidades e sem quaisquer limites.

57 O texto integral da Declaração de 2010 do Comitê de Ministros sobre neutralidade da rede do Conselho da Europa está Acessível em <https://wcd.coe.int/ViewDoc.jsp?id=1678287> [acessado em 13 de fevereiro de 2014].

58 A ISOC considera o conceito de neutralidade da rede mal definido, e em vez disso discute a inter-rede aberta continuada. Acessível em <http://www.internetsociety.org/articles/internet-society-publishes-statement-open-inter-networking> [acessado em 13 de fevereiro de 2014]. A sua consulta pública de 16 de maio de 2010 sobre a Neutralidade da Rede afirma: Em vez de simplesmente focar nas várias possibilidades de definições de Neutralidade da Rede, a Internet Society acredita ser mais adequado se concentrar mais no imperativo da preservação do modelo de Internet aberto e voltado ao usuário, que tem tido tanto êxito até o momento.

59 TACD (sem data) TACD calls for Net Neutrality. Acessível em <http://tacd.org/?option=com_content&task=view&id=162&Itemid=43> [acessado em 13 de fevereiro de 2014].

Questões em aberto

Existem inúmeras questões em aberto referentes à agenda do debate sobre neutralidade da rede:

- Onde deveria estar o equilíbrio entre os efeitos do bem público da Internet e direitos dos usuários (e humanos) por um lado, e os direitos dos provedores de inovar no âmbito de suas redes por outro lado?
- O mercado não regulado de concorrência aberta, conforme defendido pelas carriers, ofereceria escolha ilimitada (ou suficiente) aos usuários? E os usuários seriam capazes de tomar decisões relevantes?[60] Ou deveriam os reguladores inevitavelmente ser incumbidos de atuar como protetores e, em caso positivo, com que autoridade?
- De que forma diferentes abordagens jurídicas e regulatórias impactariam o mercado da banda larga e investimentos e inovações futuras?
- Quais são as implicações da (não) neutralidade da rede para os países em desenvolvimento?
- Quais são as implicações da Internet multicamadas para a concorrência, a inovação, o investimento e os direitos humanos?
- As tarifas zero ou o desenvolvimento das CDNs deveriam ser considerados "Internet em camadas"?
- A OTT dominante – tanto provedores de conteúdo quanto provedores de serviços – irá achar que a Internet em camadas e possíveis novos serviços são um modelo de negócios lucrativo também? Em tal caso, elas serão capazes de adaptá-los a fim de incluir os usuários de países em desenvolvimento ou estes serão deixados de fora?
- As operadoras de telecom conseguirão inovar seus modelos de negócios para aumentar suas receitas sem violar a neutralidade da rede (seguindo exemplos exitosos do iTunes, Google e outros provedores de serviços OTT, e as potenciais parcerias entre os provedores de serviços OTT e as operadoras)[61]?
- A necessidade de haver controle de tráfego por motivos técnicos (de qualidade) será algo ultrapassado no futuro, devido a avanços na tecnologia das carriers?

60 Radunovic V (2012) Can free choice hurt open Internet markets? Diplo Blog. Dsiponível em <http://www.diplomacy.edu/blog/can-free-choice-hurt-open-internet-markets> [acessado em 13 de fevereiro de 2014].

61 Chetan Sharma lista algumas das oportunidades interessantes de cooperação entre OTTs e operadoras de celular, como a análise das condições de rede em tempo real, o compartilhamento de informações sobre o comportamento do usuário, localização e presença (dentro dos limites das regulações sobre privacidade) ou a cobrança de serviços de terceiros por meio da assinatura de serviços planos de celular. Acessível em <http://synergy.syniverse.com/2012/05/mobile- operators-and-otts-building-a-win-win-partnership/> [acessado em 13 de fevereiro de 2014].

- De que forma a crescente dependência das nuvens e da Internet das Coisas influenciaria o debate sobre neutralidade da rede e vice versa?
- O debate deveria ultrapassar o âmbito do controle de tráfego nas carriers, adentrando o âmbito da gestão de conteúdo e aplicativos nos provedores de conteúdo e aplicativos como Google, Apple ou Facebook?
- A proteção ao consumidor continuará sendo intrinsecamente ligada à neutralidade da rede?
- Se a neutralidade da rede for "derrotada", quais princípios sustentarão a proteção ao consumidor no futuro?

Padrões Web

No final dos anos 80, a batalha dos padrões de rede havia acabado, o TCP/IP gradualmente se tornou o principal protocolo de rede, marginalizando outros padrões como o X-25 apoiado pela UIT (parte da arquitetura da Interconexão de Sistemas Abertos) e muitos padrões proprietários, como o SNA da IBM. Embora a Internet facilitasse a comunicação normal entre uma variedade de redes via TCP/IP, o sistema ainda não contava com padrões comuns de aplicativos.

A solução foi desenvolvida por Tim Berners-Lee e seus colegas na CERN (a Organização Europeia para a Pesquisa Nuclear) em Genebra, consistindo em um novo padrão para compartilhamento de informações via Internet, chamado HTML (HyperText Markup Language, na verdade apenas uma simplificação do existente padrão ISO chamado SGML– Standard Generalized Markup Language). O conteúdo exibido na Internet tinha que ser primeiramente organizado de acordo com os padrões HTML. O HTML, como base da World Wide Web, abriu espaço para o crescimento exponencial da Internet.

Desde sua primeira versão, o HTML tem sido continuamente atualizado com novas funcionalidades. A crescente relevância da Internet colocou a questão da padronização do HTML em evidência. Isto foi especialmente importante durante a Guerra dos Navegadores entre a Netscape e a Microsoft, quando cada empresa tentou fortalecer sua posição no mercado ao influenciar os padrões HTML. Enquanto o HTML básico somente lidava com textos e fotos, novos aplicativos da Internet exigiam tecnologias mais sofisticadas para o gerenciamento de base de dados, vídeos e animações. Tal variedade de aplicativos exigia consideráveis esforços de padronização para garantir que o conteúdo pudesse ser adequadamente visualizado pela maioria dos navegadores de Internet.

A padronização dos aplicativos entrou em uma nova fase com o surgimento do XML (eXtended Markup Language), que ofereceu maior flexibilidade ao estabelecimento de padrões para conteúdo da Internet. Novos conjuntos de padrões XML também foram introduzidos. Por exemplo, o padrão para a distribuição de conteúdo sem fio é chamado Wireless Markup Language (WML). A padronização de aplicativos é realizada principalmente no âmbito do quadro do W3C, liderado por Tim Berners-Lee. É interessante observar que apesar de sua grande relevância para a Internet, até o momento o W3C não tem atraído muita atenção com relação ao debate sobre governança da Internet.

Computação em nuvem

A computação em nuvem poderia ser descrita como a transferência dos dados dos discos rígidos no computador para servidores nas nuvens (isto é, grandes parques de servidores). A primeira onda de computação em nuvem começou com o uso dos servidores de correio online (Gmail, Yahoo!), aplicativos de mídia social (Facebook, Twitter) e aplicativos online (Wikis, blogs, Google docs). Além dos aplicativos rotineiros, a computação em nuvem é extensivamente usada em software para negócios. Cada vez mais os ativos digitais estão sendo transferidos dos discos rígidos para a nuvem. Os principais atores da computação em nuvem são o Google, a Microsoft, a Apple, a Amazon e o Facebook, que têm ou planejam desenvolver grandes parques de servidores.

Nos primórdios da computação, existiam computadores mainframe potentes e estações de trabalho "burras"(dumb). A energia ficava no centro. Após isso, durante um bom tempo, com os aplicativos dos PCs e dos Windows, a energia do computador migrou para a periferia. A computação em nuvem fechará o ciclo? Iremos ter alguns poucos computadores centrais grandes/parques de servidores e bilhões de unidades burras na forma de notebooks, monitores e celulares? A resposta a esta e outras perguntas precisará de tempo. Atualmente, conseguimos identificar algumas questões de governança da Internet que muito possivelmente surgirão paralelamente ao desenvolvimento da computação em nuvem.

- Com mais serviços prestados online, a sociedade moderna aumentará sua dependência da Internet. No passado, quando a Internet caía, não conseguíamos mandar e-mail ou navegar na Internet. Na era da computação em nuvem, talvez não consigamos nem escrever textos ou fazer cálculos. Esta alta dependência da Internet implicará em grande pressão sobre sua robustez e confiabilidade.

- Com uma maior quantidade de nossos dados pessoais armazenados nas nuvens, a questão da privacidade e da proteção dos dados se tornará central. Teremos controle sobre nossos arquivos de texto, e-mails e outros dados? As operadoras das nuvens poderiam usar esses dados sem permissão? Quem terá acesso aos nossos dados?
- Com um volume crescente de ativos de informação se tornando digital, os países talvez se sintam desconfortáveis em ter ativos nacionais de informação fora de suas "fronteiras" nacionais. Talvez tentem criar nuvens nacionais ou regionais ou assegurar que as nuvens existentes sejam administradas com alguma supervisão internacional. A nacionalização das nuvens poderia ser ainda mais acelerada pelo fato de que todas as principais operadoras neste campo estão baseadas nos Estados Unidos. Alguns desses países argumentam que o atual debate com foco na ICANN poderá ser substituído por um debate sobre governança da Internet com foco na regulação da computação em nuvem.
-Para diversas operadoras de computação em nuvem, a questão dos padrões está se tornando muito importante. A adoção de padrões comuns irá garantir uma transferência tranquila dos dados entre nuvens diferentes (ex., do Google para a Apple). Uma possibilidade que está sendo discutida é a adoção de padrões abertos pelos principais atores da computação em nuvem.

A governança da Internet referente à computação em nuvem provavelmente surgirá com a interação de vários atores e órgãos. Por exemplo, a UE está preocupada com a questão da privacidade e proteção de dados. O acordo Safe Harbour que supostamente solucionaria o problema dos diferentes regimes de privacidade nos EUA e na UE não funciona bem. Com mais dados digitais cruzando o Oceano Atlântico, a UE e os EUA terão que abordar a questão da proteção da privacidade de acordo com o regulamento da UE por empresas dos Estados Unidos, as principais operadoras na computação em nuvem. Esta questão ganhou maior destaque após as revelações de Snowden sobre a vigilância em massa. Quando se trata de padrões, é bem provável que as principais empresas cheguem em um acordo entre si. O Google já começou a avançar bastante com relação aos padrões abertos, ao estabelecer a Data Liberation Front, cujo objetivo e garantir a transição suave de dados entre diferentes nuvens. Estes são os primeiros componentes básicos que tratarão da questão da governança da Internet relacionada

à computação em nuvem. Outras provavelmente surgirão como soluções para problemas reais de políticas.

Convergência: Multimídia, Telecomunicações e Internet

Historicamente, a telecomunicação, a radiodifusão e outras áreas relacionadas eram segmentos setoriais separados; usavam tecnologias diferentes e eram regidos por diferentes regulações. O uso amplo e predominante da Internet auxilia a convergência de plataformas tecnológicas na prestação de serviços de telecomunicações, radiodifusão e informações. Hoje, podemos realizar chamadas telefônicas, assistir TV e compartilhar músicas em nosso computador via Internet. Há apenas alguns anos, isto era feito por diferentes sistemas tecnológicos.

No campo da telecomunicação tradicional, o principal ponto de convergência é o VoIP. A crescente popularidade dos sistemas VoIP como o Skype tem como base um preço mais baixo, a possibilidade da integração das linhas de comunicação de dados e voz e o uso de ferramentas avançadas baseadas em dispositivos de PC e dispositivos móveis. Com o YouTube e serviços similares, a Internet também está entrando em convergência com serviços tradicionais de multimídia e entretenimento. Embora a convergência tecnológica esteja evoluindo rapidamente, as suas consequências econômicas e jurídicas demandarão tempo para evoluir.

Questões

As implicações econômicas da convergência

No nível econômico, a convergência começou a redefinir mercados tradicionais ao colocar empresas que anteriormente operavam em domínios separados em concorrência direta. As empresas usam estratégias diferentes, sendo que a abordagem mais frequente é a de incorporação e aquisição.

A necessidade de haver um quadro jurídico

O sistema jurídico foi o que mais demorou para se adaptar às mudanças causadas pela convergência tecnológica e econômica. Cada segmento –telecomunicação, radiodifusão e fornecimento de informações – tem seu próprio quadro regulatório específico. Esta convergência suscita várias questões relacionadas à governança e regulação:

- O que acontecerá aos regimes nacionais e internacionais existentes em campos como a telefonia e a radiodifusão?


OneStep
POLAROID LAND CAMERA

- Novos regimes serão desenvolvidos priorizando basicamente a Internet?
- A regulação da convergência deveria ser feita por autoridades públicas (organizações governamentais e internacionais) ou por meio da autorregulação?

Alguns países, como a Malásia e a Suíça, bem como a UE, começaram a apresentar respostas a estas perguntas. A Malásia adotou a Lei das Comunicações e Multimídia em 1998, definindo um quadro geral para a regulação da convergência. O quadro regulatório da UE para as comunicações eletrônicas, transpostas para leis nacionais, é outro passo nessa direção, bem como as leis e os regulamentos sobre telecomunicações da Suíça.

O risco da convergência: a fusão entre as operadoras de cabo e os ISPs

Em muitos países, a Internet banda larga foi introduzida pelas redes de cabo, principalmente nos Estados Unidos, onde a Internet a cabo predomina bastante sobre a ADSL (linha digital assimétrica para assinante), a outra principal opção de Internet banda larga. Quais os riscos associados a esta convergência?

Algumas partes argumentam que o buffering (armazenamento temporário de dados) das operadoras de cabo entre os usuários e a Internet poderia ser um obstáculo para o princípio da neutralidade da rede. A principal diferença entre ADSL e cabo é que o cabo não é regulado pelas chamadas regras comuns das carriers que se aplicam ao sistema de telefonia e especificam que o acesso deveria ser não discriminatório. As operadoras de cabo não estão sujeitas a estas regras, concedendo-lhes controle completo sobre o acesso à Internet de seus assinantes. Elas podem bloquear o uso de determinados aplicativos e controlar o acesso a determinados materiais. As possibilidades de vigilância e consequentemente a capacidade de violar a privacidade são muito maiores com a Internet a cabo uma vez que o acesso é controlado por meio de um sistema similar às redes de área local (LANs), que oferecem um alto nível de controle direto dos usuários.

Em um artigo sobre esta questão, a União de Liberdades Civis dos Estados Unidos apresenta o exemplo a seguir sobre os riscos dos monopólios de Internet a cabo: "Isso se assemelha à companhia telefônica que tem autorização para ser proprietária de restaurantes e depois fornece um bom serviço e sinal claro aos clientes que telefonam para o Domino's e sinais ocupados, desconectados

e estáticos para os que telefonam para a Pizza Hut".[62]

Este problema de convergência poderá ser solucionado decidindo se a Internet a cabo é um "serviço de informação" ou um "serviço de telecomunicação". No caso deste último, terá que ser regulada pelas leis comuns das carriers.

Cibersegurança

Situação atual

A Internet foi originalmente projetada para ser usada em um ciclo fechado composto principalmente de acadêmicos. A comunicação era aberta. A segurança não era uma preocupação.

A cibersegurança ganhou destaque com a expansão da Internet para além do círculo dos pioneiros da Internet. A Internet reiterou o antigo truísmo de que a tecnologia pode ser facilitadora e ameaçadora. Aquilo que pode ser usado a favor da sociedade também pode ser usado contra ela. As questões de cibersegurança podem ser classificadas de acordo com três critérios:

- Tipo de ação. A classificação baseada no tipo de ação poderá incluir intercepção de dados, interferência de dados, acesso ilegal, spyware, corrupção de dados, sabotagem, recusa de serviço e roubo de identidade.
- Tipo de perpetrador. Entre possíveis perpetradores estão hackers, cibercriminosos, cibercombatentes e ciberterroristas.
- Tipo de alvo. Há inúmeros alvos em potencial, desde pessoas físicas, empresas privadas e instituições públicas até infraestruturas críticas, governos e ativos militares.

O quadro da cibersegurança inclui princípios de políticas, instrumentos e instituições que lidam com a cibersegurança. É um conceito guarda-chuva que abrange várias áreas:

- A Proteção da Infraestrutura Crítica de Informação é cada vez mais importante porque a infraestrutura crítica global agora depende da Internet. Muitas partes vitais da sociedade global - entre as quais a energia, a água e as finanças - dependem enormemente da Internet e de outras redes de computadores como infraestrutura de informação. Isto inclui não somente o equipamento e as

62 Artigo Técnico da ACLU (2005) No competition: How monopoly control of the broadband Internet threatens free speech. ACLU: Nova York, NY, EUA. Acessível em <https://www.aclu.org/other/monopoly-control-broadband-internet-threatens-free-speech?redirect=technology-and-liberty/monopoly-control-broadband-internet-threatens-free-speech>[acessado em 13 de fevereiro de 2014].

conexões, mas também os protocolos, os centros de dados e os recursos críticos da Internet (CIR). A vulnerabilidade da Internet é a vulnerabilidade da sociedade moderna.

- O crime cibernético é o crime cometido via Internet e sistemas de computador. Inclui crimes antigos, isto é, tradicionais, agora conduzidos através ciberespaço (como diversas fraudes), crimes que evoluíram devido à tecnologia (ex., fraudes de cartões de crédito e abuso infantil), novos crimes que surgiram com a Internet (ex., ataques de recusa de serviço e fraudes pay-for-click) e ferramentas de crimes cibernéticos que são usadas para facilitar outros crimes (ex., botnets). O combate à pornografia infantil é a área mais desenvolvida da cooperação internacional; esta cooperação não está conseguindo, no entanto, desmontar os mercados globais de crimes cibernéticos que oferecem serviços criminais terceirizados e armas digitais fáceis de usar (ex., vírus e botnets) a quase qualquer pessoa.
- Ciberconflitos, frequentemente classificados como guerra cibernética, têm recebido bastante visibilidade da mídia e ainda pouca reflexão sobre políticas e questões jurídicas. Os conflitos cibernéticos podem ser examinados por meio de três principais áreas: conduta de conflitos cibernéticos (isto é, a lei existente, principalmente as Convenções de Haya, pode ser aplicada ao ciberespaço; em caso negativo, quais são os tipos de novos instrumentos jurídicos que deveriam ser desenvolvidos?); armas e desarmamento (isto é, como introduzir as armas cibernéticas no processo de desarmamento); e a lei humanitária (isto é, de que maneira aplicar as Convenções de Genebra aos conflitos).

A cibersegurança, como espaço de políticas, está em sua fase de formação, com a subsequente confusão conceitual e terminológica. Outros termos também estão em discussão geral sem a precisão política necessária: ciberprotestos, ciberterrorismo, cibersabotagem, etc. O ciberterrorismo, em particular, ganhou destaque após o 11/09, quando um número crescente de ataques ciberterroristas foram relatados. Os ciberterroristas usam ferramentas semelhantes aos cibercriminosos, mas para um propósito diferente. Enquanto os cibercriminosos têm como motivação principal os ganhos financeiros, os ciberterroristas buscam causar grandes transtornos e caos.

Iniciativas de políticas de cibersegurança

Muitas iniciativas nacionais, regionais e globais priorizam a cibersegurança. No nível nacional, uma quantidade cada vez maior de

legislações e precedentes tratam da cibersegurança, com foco no combate ao crime cibernético.

No nível internacional, a UIT é a organização mais ativa; elaborou uma grande quantidade de quadros de segurança, arquiteturas e padrões, inclusive o X.509, que fornece a base para a infraestrutura de chaves públicas (PKI), usada, por exemplo, na versão segura do HTTP(S) (HyperText Transfer Protocol (Secure)). A UIT foi além dos aspectos estritamente técnicos e lançou a Agenda Global de Cibersegurança.[63] Esta iniciativa engloba medidas jurídicas, cooperação de políticas e criação de capacidades. Além disso, na CMTI-12, novos artigos sobre segurança e robustez de redes e sobre comunicações eletrônicas em massa não solicitadas (geralmente designadas como spam) foram incluídas nas ITRs.[64]

A Iniciativa da Commonwealth contra crimes cibernéticos(CCI) foi legislada pelos líderes governamentais da Commonwealth em 2011 para aprimorar a legislação e a capacidade dos estados-membros de combater os crimes cibernético.[65] Dezenas de parceiros envolvidos com a CCI auxiliaram países interessados ao realizar missões avaliativas, programas e construção de capacidades e esboços de legislações modelo nos campos do crime cibernético e da cibersegurança em geral.

O G8 tem algumas iniciativas no campo da cibersegurança planejados para melhorar a cooperação entre os órgãos encarregados do cumprimento da lei. Formou o Subgrupo de Crimes de Alta Tecnologia para tratar do estabelecimento da comunicação 24 horas entre centros de cibersegurança dos estados-membros, da qualificação de pessoal e da melhoria de sistemas jurídicos estatais que combaterão o crime cibernético e promoverão a cooperação entre o setor de TIC e os órgãos encarregados do cumprimento da lei.

A Assembleia Geral das Nações Unidas passou diversas resoluções anualmente sobre "desenvolvimentos no campo da informação e das telecomunicações no contexto da segurança internacional", mais especificamente as resoluções 53/70 em 1998, 54/49 em 1999, 55/28 em 2000, 56/19 em 2001, 57/239 em 2002 e 58/199 em 2003. Desde 1998, todas as resoluções subsequentes incluíram conteúdo similar, sem qualquer melhoria significativa. Além destas resoluções rotineiras, a principal

63 Global Cybersecurity Agenda (sem data). Acessível em <http://www.itu.int/osg/csd/cybersecurity/gca/> [acessado em 13 de fevereiro de 2014]

64 UIT (2012) CMTI-12 Final Acts. Acessível em <http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf> [acessado em 10 de agosto de 2014]

65 CCI (sem data) Commonwealth Cybercrime Initiative. Acessível em <http://www.commonwealthcybercrimeinitiative.org/> [acessado em 11 de agosto de 2014].

inovação foi o recente conjunto de recomendações para negociações do tratado de cibersegurança, que foram submetidas ao Secretário Geral das Nações Unidas por 15 estados-membros, entre os quais todos os membros permanentes do Conselho de Segurança da ONU.

Um importante instrumento jurídico relacionado à cibersegurança é a Convenção sobre o Crime Cibernético do Conselho da Europa,[66] que entrou em vigor em 1o de julho de 2004. Alguns países estabeleceram acordos bilaterais. Os EUA possuem acordos bilaterais sobre cooperação jurídica em questões criminais com mais de 20 países (Tratados de Assistência Jurídica Mútua em Matéria Penal – MLATs). Estes acordos também são aplicáveis aos casos de crimes cibernéticos.

O ciberconflito continua sendo uma área com menos avanços em termos de desenvolvimentos de políticas. Ao mesmo tempo, uma quantidade maior de países parece estar desenvolvendo suas próprias ferramentas cibernéticas de guerra e inteligência, conforme apresentado pelo relatório das Nações Unidas de 2010.[67] Em 2013, o Centro de Excelência de Defesa Cibernética Cooperativa da OTAN (CCDCOE) elaborou o Manual Tallinn sobre aplicação do direito humanitário internacional existente referente a entrar em guerras e conduzi-las (jus ad bellum e jus in bello) no ciberespaço.[68]

Uma tentativa dos acadêmicos e dos atores não governamentais de redigir um acordo internacional é a Stanford Draft Convention on Protection from Cyber Crime and Terrorism (Convenção do Projeto Stanford de Proteção contra Crime Cibernético e Terrorismo)[69]. Esta proposta recomenda a criação de um órgão internacional, nomeado de Agência para a Proteção da Infraestrutura da Informação (AIIP).

Questões

Influência da arquitetura da Internet sobre a cibersegurança

A própria natureza da organização da Internet afeta sua segurança. Devemos continuar com a abordagem atual de construção de segu-

66 Council of Europe (2001) Convention on Cybercrime. Acessível em <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> [acessado em 13 de fevereiro de 2014].

67 Relatório da ONU A/65/201 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Acessível em <http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf> [acessado em 10 de agosto de 2014].

68 CCDCOE (2013) The Tallinn Manual. Acessível em <http://www.ccdcoe.org/tallinn-manual.html> [acessado em 10 de agosto de 2014].

69 Sofaer AD et al. (2000) Proposal for an international convention on cybercrime. Acessível em <http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm> acessado em 13 de fevereiro de 2014].

rança sobre uma fundação não segura e preexistente ou devemos modificar a base da infraestrutura da Internet? De que forma essa mudança afetaria outras características da Internet, principalmente sua abertura e transparência? A maior parte dos avanços anteriores dos padrões da Internet tinha como objetivo melhorar o desempenho ou introduzir novos aplicativos. A segurança não era prioridade. Não está claro se a IETF será capaz de mudar padrões de e-mails para oferecer autenticação adequada e, por fim, reduzir os erros de uso da Internet (ex., spam, crimes cibernéticos). Devido à polêmica em torno de quaisquer mudanças nos padrões básicos da Internet, é provável que as melhorias relacionadas à segurança no protocolo básico da Internet sejam graduais e lentas. Mesmo assim, etapas decisivas estão começando a ser implementadas neste sentido; as Extensões de Segurança do Sistema de Nomes de Domínio (DNSSEC)[70]são um bom exemplo ilustrativo. Após quase 12 anos de pesquisas, experiências e debates no âmbito da comunidade técnica, as DNSSEC começaram a ser primeiramente implementadas para alguns ccTLDs, e a partir de 2010 também foram implementadas no nível do servidor-raiz. No entanto, outros desafios são encontrados na adoção em grande escala deste novo padrão de segurança alguns degraus abaixo pelos agentes de registro dos nomes de domínio, as ISPs e os donos de sítios web.[71]Melhorias importantes de segurança, porém, podem ser alcançadas com a configuração adequada dos principais nodos da Internet, como os servidores DNS ao redor do mundo. Diversos incidentes, como a guerra cibernética privada de 2013 entre duas empresas – CyberBunker e Spamhaus – que resultou em congestionamento temporário de grande parte da Internet global, podem ocorrer devido às dezenas de milhões de servidores DNS mal configurados ao redor do mundo conhecidos como open resolvers.[72] Além disso, a introdução do conceito de security-by-design em todas as novas tecnologias, software, hardware e protocolos acrescentaria camadas adicionais de segurança.

70 DNSSEC explained. Acessível em <http://everything.explained.at/DNSSEC/> acessado em 13 de fevereiro de 2014].

71Para uma visão geral do status atual e dos desafios da implementação das DNSSEC ver Marsan C (2012) Will 2012 be the dawn of DNSSEC? 18 de janeiro de 2012 Networkworld. Acessível em http://www.networkworld.com/news/2012/011812-dnssec-outlook-255033.html [acessado em 13 de fevereiro de 2014]. Nota do Tradutor: o endereço foi substituído por <http://www.networkworld.com/article/2184914/security/will-2012-be-the-dawn-of-dnssec-.html> [acessado em 6 de março de 2017].

72 Radunovic V (2013) Waging a (private) cyber war. Acessível em <https://www.diplomacy.edu/blog/waging-private-cyberwar> [acessado em 10 de agosto de 2014]


ARD SNO
ET EDWARD SNOWD

O futuro desenvolvimento do comércio eletrônico exige alto nível de cibersegurança

A cibersegurança costuma ser mencionada como uma das pré-condições para o rápido crescimento do comércio eletrônico. Sem uma Internet segura e confiável, os clientes ficarão relutantes em fornecer informações confidenciais online, como o número do cartão de crédito. O mesmo se aplica ao banco online e ao uso de dinheiro eletrônico. É evidente que existe uma quantidade cada vez maior de ataques exitosos a servidores de empresas para obtenção de dados pessoais e do número de cartão de crédito de clientes, por exemplo, a coleta de mais de 1,2 bilhões de combinações de nome-de-usuário-e-senha e meio bilhão de endereços de e-mail roubados em 2014 por uma gangue russa.[73] Isto diminui a confiança dos usuário nos serviços online. Se a cibersegurança geral melhora apenas lentamente (e de forma despadronizada), é provável que o setor empresarial estimule desenvolvimentos mais rápidos na cibersegurança. Isto poderá levar a maiores desafios referente ao princípio da neutralidade da rede e do desenvolvimento da "nova Internet", que facilitaria, entre outras coisas, uma comunicação mais segura via Internet.

Vigilância e espionagem

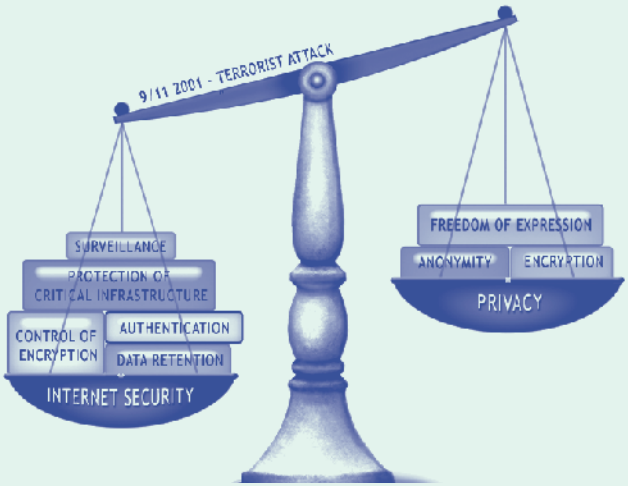
As revelações feitas em 2013 pelo funcionário da NSA, Edward Snowden, confirmaram que os países – inclusive os Estados Unidos – exploraram as vulnerabilidades da Internet para seus próprios interesses. O projeto PRISM da NSA baseou suas capacidades de vigilância na capacidade de acessar os cabos, roteadores e servidores em nuvens de grandes empresas de Internet (telecoms baseadas nos EUA, serviços e provedores de conteúdo). Em resposta, outros países – especialmente a UE e os BRICS – começaram a considerar táticas de mitigação, inclusive instalar suas próprias conexões de cabo submarino intercontinental para evitar passar pelos nodos dos EUA,[74] exigindo que as empresas de Internet armazenem dados pessoais de seus cidadãos em centros de dados dentro de suas jurisdições e incentivando o desenvolvimento dos serviços e conteúdo locais.

Em 2013, a Mandiant, empresa de segurança baseada nos Estados Unidos, divulgou um relatório sobre uma campanha de ciberespionagem

73 Perlroth N e Gellese D (2014) Russian gang said to amass more than a billion stolen Internet credentials. New York Times. Disponível em <https://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0> [acessado em 10 de agosto de 2014].

74 Brazil and the EU have pushed forward their dialogue on developing a direct submarine link. Acessível em <http://rt.com/news/brazil-eu-cable-spying-504/> [acessado em 10 de agosto de 2014].

Figura 6



contra empresas dos EUA realizada pela China.[75] Após os EUA acusarem cinco "hackers militares" chineses, a China, por sua vez, acusou os EUA de ciberespionagem, resultando na suspensão das atividades do Grupo de Trabalho Cibernético Chinês-Americano.[76]

A crescente militarização do ciberespaço por meio de ferramentas de exploração e hacking pelos países resulta em crescente tensão política. Essa tensão pode acelerar a necessidade de envidar esforços globais para evitar a proliferação de armas cibernéticas.

Cibersegurança e direitos humanos

A ligação entre cibersegurança e direitos humanos é altamente relevante para o futuro da Internet. Até o momento, esses dois campos estão sendo tratados de forma separada em seus respectivos silos. No entanto, experiências recentes (SOPA, ACTA, PRISM/NSA) mostram que a proteção dos direitos humanos não é apenas uma prioridade baseada em valores, mas também uma ferramenta bastante prática para garantir que a Internet permaneça aberta e segura. Os direitos humanos são uma questão de realpolitik cibernética.

75 Keck Z (2014) China expands cyber spying. Acessível em <http://thediplomat.com/2014/04/china-expands-cyber-spying/> [acessado em 10 de agosto de 2014].

76 Ranger S (2014) We're the real hacking victims, says China. Acessível em <http://www.zdnet.com/were-the-real-hacking-victims-says-china-7000029666/> [acessado em 10 de agosto de 2014].

Os usuários individuais da Internet são os pilares da cibersegurança. Mesmo assim, costumam ser o "elo mais fraco" quando de se trata da proteção contra ataques cibernéticos. Nossos computadores pessoais são usados para realizar ataques cibernéticos (como parte dos botnets) e espalhar vírus e malware. O acesso desprotegido a computadores e dispositivos móveis oferece um backdoor para o acesso dos conjuntos de dados das empresas ou instituições, e prejudica muitos outros computadores.

As preocupações dos usuários finais, no entanto, geralmente não são sobre possíveis danos maiores (frequentemente devido à ignorância) como resultado de seus computadores infectados, e sim sobre a proteção de seus dados, e dessa forma sua integridade e privacidade e seus direitos em geral. As discussões pós-PRISM enfatizam aumentar a segurança dos PCs em termos de vigilância, inclusive discutindo de que forma aplicar a criptografia, patches e atualizações regulares, protocolos IPSec e VPN[77] – medidas de conscientização que iriam, de fato, também evitar o acesso desprotegido e contribuir para melhorar a cibersegurança no geral.

A Cibersegurança Global – construída com base no importante papel dos usuários individuais da Internet – tem nos direitos humanos um de seus pilares. O reconhecimento desta ligação começou a aparecer nos documentos das políticas pertinentes. A estratégia de cibersegurança da União Europeia, por exemplo, considera a preservação do ciberespaço aberto, livre e seguro –inclusive apoia a promoção e a proteção de direitos fundamentais – como um dos seus cinco pilares estratégicos.[78] O principal desafio será superar a visão de ganho/perda que vem predominando após o 11 de setembro: mais segurança implica menos direitos humanos e vice-versa. No entanto, existem várias áreas onde há ganho/ganho ao fortalecer e proteger os indivíduos na qualidade de pilares do sistema de cibersegurança (acesso à informação, proteção da privacidade) que deveriam ser prioridade.

77 Schneier B (2013) NSA surveillance: A guide to staying secure. Acessível em <www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance> [acessado em 12 de agosto de 2014].

78 Comissão Europeia (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Acessível em <http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security> [acessado em 12 de agosto de 2014].

Criptografia

Hoje, a criptografia consiste em codificar documentos eletrônicos e a comunicação em um formato ilegível que só pode ser lido por meio de software de criptografia. Tradicionalmente, os governos eram os únicos atores que tinham poder e conhecimento para desenvolver e aplicar uma criptografia forte em suas comunicações militares e diplomáticas. Com pacotes como o Pretty Good Privacy, a criptografia se tornou acessível a quaisquer usuários da Internet, inclusive criminosos e terroristas, levantando muitas questões sobre governança referentes a como encontrar o equilíbrio certo entre a necessidade de respeitar a privacidade da comunicação dos usuários da Internet e a necessidade dos governos de monitorar alguns tipos de comunicação de relevância para a segurança nacional (a potencial atividade criminosa e terrorista continua sendo um problema).

Os aspectos internacionais da política de criptografia são relevantes para a discussão da governança da Internet na medida em que a regulação da criptografia deveria ser global ou, pelo menos, deveria envolver outros países capazes de produzir ferramentas de criptografia. Por exemplo, a política dos Estados Unidos de controle sobre exportações de software de criptografia não teve muito êxito porque não conseguiu controlar a distribuição internacional.

As empresas de software dos Estados Unidos iniciaram um forte lobby argumentando que os controles sobre a exportação não aumentam a segurança nacional, pelo contrário, enfraquecem os interesses comerciais dos EUA.

Regimes internacionais para ferramentas de criptografia

A criptografia foi tratada em dois contextos: o Acordo de Wassenaar e a OCDE. O Acordo de Wassenaar é um regime internacional adotado por 41 países para restringir a exportação de armas convencionais e das tecnologias de "duplo uso" a países em guerra ou considerados "Estados párias".[79] O acordo criou um secretariado em Viena. O lobby dos Estados Unidos junto ao Grupo de Wassenaar tinha como objetivo ampliar a Abordagem Clipper[80] internacionalmente, ao controlar software de

79 The Wassenaar Arrangement. Acessível em <http://www.wassenaar.org/> [acessado em 13 de fevereiro de 2014].

80 A abordagem Clipper foi proposta pelo governo dos Estados Unidos em 1993. A questão principal da proposta era o uso do chip Clipper que supostamente era usado em telefones e todas as outras ferramentas de comunicação de voz. O chip Clipper tinha uma "back door" que poderia ser usada pelos governos para vigilância nos termos da lei. Após forte oposição de ativistas de direitos humanos e do público em geral, o governo dos EUA abandonou esta proposta em 1995. Ver: Denning D (1995) The case

criptografia por meio da custódia de chaves. Muitos países resistiram a isso, principalmente o Japão e os países escandinavos.

Chegou-se a um acordo em 1998 com a introdução de diretrizes de criptografia, que incluía produtos de criptografia de hardware e software em lista de controle de duplo uso acima de 56 bits. Esta extensão incluía ferramentas de Internet, como navegadores Web e e-mail. É interessante observar que o tal acordo não inclui transferências "intangíveis", como downloads. O fato de não se ter conseguido introduzir uma versão internacional do Clipper contribuiu para a retirada da proposta internamente nos Estados Unidos. Neste exemplo da ligação entre cenários nacionais e internacionais, os acontecimentos internacionais tiveram impacto decisivo sobre os acontecimentos nacionais.

A OCDE é outro fórum para a cooperação internacional no campo da criptografia. Embora a OCDE não elabore documentos juridicamente vinculativos, as suas diretrizes sobre diversos assuntos são bastante respeitadas. Elas resultam de uma abordagem especializada e do processo de tomada de decisões que tem como base o consenso. A maioria das diretrizes é por fim incorporada em legislações nacionais. A questão da criptografia foi um tópico bastante polêmico nas atividades da OCDE, tendo iniciado em 1996 com uma proposta dos Estados Unidos para a adoção da custódia de chaves como padrão internacional. De forma similar a Wassenaar, as negociações sobre as propostas dos EUA de adotar a referida custódia de chaves como padrão internacional encontrou forte oposição no Japão e nos países escandinavos. O resultado foi a especificação adaptada dos principais elementos da política de criptografia.

Algumas tentativas de desenvolver um regime internacional para a criptografia, principalmente no contexto do Acordo de Wassenaar, não levaram ao desenvolvimento de um efetivo regime internacional. Ainda é possível obter software de criptografia forte na Internet.

Spam

Situação atual

O spam costuma ser definido como e-mail não solicitado, enviado a uma grande quantidade de usuários da Internet. O spam é principalmente usado para promoção comercial, sendo que seus outros usos incluem ativismo social, campanha política e a distribuição de materiais

for clipper. MIT Technology Review. MIT: Cambridge, MA, EUA. Acessível em <http://encryption_policies.tripod.com/us/denning_0795_clipper.htm> [acessado em 13 de fevereiro de 2014].

pornográficos. Ele foi incluído na cesta de infraestrutura porque afeta o funcionamento normal da Internet ao obstruir um dos principais aplicativos da internet, o e-mail. Trata-se de um dos problemas de governança da Internet que afeta quase todo mundo que se conecta à Internet. De acordo com estatísticas de 2014, 66% do tráfego de e-mail é spam.[81] Além do fato de ser irritante, o spam também causa prejuízo econômico considerável, tanto em termos da banda larga usada quanto em termos do tempo gasto o verificando e apagando.

O spam pode ser combatido por meio de métodos técnicos e jurídicos. Do ponto de vista técnico, muitos aplicativos para filtrar mensagens e detectar spams estão disponíveis. O principal problema com os sistemas de filtragem é que eles são conhecidos por apagar mensagens não spam também. O setor antispam está em expansão, com aplicativos cada vez mais sofisticados capazes de distinguir o spam das mensagens comuns. Os métodos técnicos tem efeito limitado e requerem medidas jurídicas complementares.

Do ponto de vista jurídico, muitos países reagiram a isso ao introduzir novas leis antispam. Nos Estado Unidos, a lei Can-Spam Act envolve o equilíbrio delicado entre a permissão de promoções via e-mail e prevenção de e-mails spam.[82] Apesar de a lei prever penalidades severas para a distribuição de spam, inclusive pena de prisão de até cinco anos, algumas de suas provisões, de acordo com os críticos, toleram ou até incentivam a atividade de envio de spam. A posição inicial da lei é de que o spam é permitido até o destinatário das mensagens spam falar "pare" (ao usar uma cláusula de autoexclusão).

Em julho de 2003, a UE introduziu sua própria lei antispam como parte de sua diretiva sobre privacidade e comunicações eletrônicas. A lei da UE incentiva a autoregulação e iniciativas do setor privado que levariam à redução do spam.[83]

---

81 Spam stops here (2014) Global Spam Threat Report. Acessível em <http://www.spamstopshere.com/global-report/spam-threats-february-2014.php> [acessado em 11 de agosto de 2014].

82 Mais referências à lei Can-Spam estão disponíveis no Bureau of Consumer Protection (2009). The CAN-SPAM Act: A Compliance Guide for Business. Acessível em <http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business> [acessado em 13 de fevereiro de 2014].

83 A Contact Network of Spam Enforcement Authorities (CNSA) foi estabelecida em fevereiro de 2005 por 13 países da UE (França, Áustria, Bélgica, Chipre, República Tcheca, Dinamarca, Grécia, Irlanda, Itália, Lituânia, Malta, Reino Unido e Espanha). O seu objetivo é promover tanto a cooperação entre os Estados quanto a coordenação com empresas fora da EU, como a OCDE e a UIT.

84 Conforme citação em Johnsson O (2007) Methods to combat SPAM. Acessível em <http://home.swipnet.se/Johnson_Consulting/images/spam1.htm> [acessado em 13 de fevereiro de 2014].

SPAM COMO FOCO DE POLÍTICAS

O spam é um exemplo ilustrativo das tendências e às vezes, da moda nas políticas globais. Em 2005, o spam era uma questão importante de governança da Internet, listado como uma questão de governança da Internet relevante no relatório do GTGI. O spam foi discutido na CMSI em Túnis e em várias reuniões internacionais. O spam também era frequentemente coberto pela mídia.

Desde 2005, o volume do spam triplicou, de acordo com estimativas conservadoras (2005: 30 bilhões de mensagens por dia; 2008: 100 bilhões de mensagens por dia; 2010: 200 bilhões de mensagens por dia). A relevância da política do spam não acompanha esta tendência. O spam atualmente tem muito pouca visibilidade nos processos das políticas globais.

Em novembro de 2006, a Comissão Europeia adotou a Comunicação de Combate ao Spam, Spyware e Software Malicioso. A Comunicação identifica uma série de ações para promover a implementação e o cumprimento da legislação existente esboçada acima, uma vez que a falta de cumprimento é entendida como o principal problema.

Resposta internacional

Ambas as leis antispam adotadas nos Estados Unidos e na União Europeia têm uma falha: a falta de disposições para evitar spams transnacionais. A Ministra da Indústria do Canadá, Lucienne Robillard, afirmou que o problema não pode ser resolvido "país por país".[84] Conclusão similar foi obtida em um estudo sobre as leis antispam da UE realizada pelo Instituto para a Lei da Informação na Universidade de Amsterdã: "O simples fato de que a maior parte dos spams é originada fora da UE limita de forma considerável a eficiência da Diretiva da União Europeia".[85] É necessário haver uma solução global, implementada por meio de um tratado internacional ou algum mecanismo similar.

Um Memorando assinado pela Austrália, pela Coreia e pelo Reino Unido é um dos primeiros exemplos de cooperação internacional da campanha antispam.

A OCDE constituiu uma força tarefa contra o spam e preparou um conjunto de ferramentas antispam. A UIT também mostrou proati-

85 BBC NEWS (2004) European anti-spam laws lack bite. 28 de abril. Disponível em <http://news.bbc.co.uk/2/hi/technology/3666585.stm> [acessado em13 de fevereiro de 2014]

vidade ao organizar a Reunião Temática de Combate ao Spam (2004) para considerar várias possibilidades de elaboração de um Memorando de Entendimento de Combate ao Spam global.[86] No nível regional, a UE estabeleceu a Network of Anti-Spam Enforcement Agencies (Rede de Agências de Aplicação Antispam) e a APEC elaborou um conjunto de diretrizes para o consumidor.

Outra possível abordagem antispam foi realizada pelas empresas de Internet mais importantes que hospedam contas de e-mail: America Online, British Telecom, Comcast, EarthLink, Microsoft e Yahoo!. Elas estabeleceram em 2003 a Aliança Técnica Antispam (ASTA), tendo como tarefa principal coordenar atividades antispam na esfera técnica e de políticas.

Questões

Definições diferentes de spam

Diferentes entendimentos do que é spam afetam a campanha antispam. Nos Estados Unidos, a preocupação geral sobre a proteção à liberdade de expressão e à Primeira Emenda do país também afeta a campanha antispam. Os legisladores norte-americanos consideram que o spam nada mais é que "e-mail comercial não solicitado", deixando de fora outros tipos de spam, inclusive ativismo político e pornografia. A maioria dos outros países considera o spam "e-mail em massa não solicitado" independentemente de seu conteúdo. Como a maior parte dos spams é gerada nos EUA, tal diferença de definições limita seriamente qualquer possibilidade de implementação de mecanismos antispam internacionais efetivos.

Spam e autenticação de e-mail

Um dos facilitadores estruturais do spam é a possibilidade de enviar mensagens de e-mail com endereço falso do remetente. Há uma solução técnica possível para esse problema, que exigiria mudanças nos padrões existentes para e-mails de Internet. A IETF tem considerado alterar o protocolo de e-mail, garantindo a autenticação de e-mail. Este é um exemplo de como as questões técnicas (padrões) podem afetar as políticas. Tal implementação da autenticação de e-mail possivelmente implicaria na restrição da anonimidade na Internet.

86 Para mais informações sobre as atividades da UIT relacionadas ao combate ao spam, ver UIT (sem data) ITU Activities on Countering Spam. Disponível em <http://www.itu.int/osg/spu/spam/> [acessado em 13 de fevereiro de 2014].

Necessidade de ação global

A maior parte dos spams é originada fora de determinado país. Trata-se de um problema global que requer uma solução global. Existem várias iniciativas que poderiam melhorar a cooperação global. Algumas delas, como memorandos de entendimento bilaterais, já foram mencionadas. Outras incluem ações como a construção de capacidades e a troca de informações. Uma solução mais abrangente seria implementar algum tipo de instrumento antispam global. Até o momento, os países desenvolvidos preferem fortalecer suas legislações nacionais em conjunto com campanhas antispam bilaterais ou regionais. Dada sua posição de desvantagem no recebimento do "mal público global" originado em muitos países desenvolvidos, a maioria dos países em desenvolvimento tem interesse em definir uma resposta global ao problema do spam.

Cesta jurídica

Quase todo aspecto da governança da Internet inclui um componente jurídico, porém a definição do arcabouço jurídico para moldar o desenvolvimento rápido da Internet está em sua fase inicial. As duas abordagens predominantes são:

1 Abordagem real às questões legais na qual a Internet é essencialmente tratada da mesma forma que outras tecnologias de telecomunicação, na extensa linha evolutiva dos sinais de fumaça até o telefone. Com uma comunicação mais rápida e abrangente, a Internet apresenta mudanças quantitativas, mas não qualitativas, na sociedade moderna. Consequentemente, quaisquer regras jurídicas existentes também podem ser aplicadas à Internet[1].

2 Abordagem ciber às questões legais, com base na premissa de que a Internet introduz novos tipos de relacionamentos sociais no ciberespaço. Consequentemente, existe a necessidade de formular novas leis cibernéticas para regular o referido ciberespaço. Um argumento para tal abordagem é de que a mera velocidade e volume da comunicação transnacional facilitada pela Internet prejudica o cumprimento das regras jurídicas existentes.

A abordagem real às questões legais está se tornando predominante. Parte considerável da legislação existente pode ser aplicada à Internet. Para algumas questões como o crime cibernético, as mesmas regras reais teriam que ser adaptados para serem aplicáveis ao mundo cibernético.

1 Um dos maiores defensores da abordagem real às questões legais é o Juiz Frank Easterbrook, que é citado com a seguinte afirmação: "Vá para casa; não existe o ciberdireito". Neste artigo, Cyberspace and the law of the horse, ele argumenta que embora os cavalos fossem muito importantes nunca houve a "Lei do Cavalo". O Juiz Easterbrook argumenta que existe a necessidade de priorizar os principais instrumentos jurídicos, como contratos, responsabilidade, etc. Acessível em: <http://www.law.upenn.edu/ law619/f2001/week15/easterbrook.pdf> [acessado em 9 de agosto de 2014]. O argumento do Juiz Frank Easterbrook causou diversas reações, e resultou no livro de Lawrence Lessig, The Law of the Horse: What Cyberlaw Might Teach. Acessível em http://cyber.law.harvard.edu/works/lessig/LNC_Q_D2.PDF [acessado em 13 de fevereiro de 2014]. Nota do Tradutor: o primeiro endereço foi substituído por <http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2147&context=journal_articles> [acessado em 7 de março de 2017].

Instrumentos jurídicos

Existe uma grande variedade de instrumentos jurídicos já aplicada ou que poderia ser aplicada à governança da Internet.

NOTA

Um argumento frequente para uma nova regulação do ciberespaço é de que a regulação tradicional (ex., crime, tributação) não é suficientemente eficiente. É importante lembrar que as leis não impossibilitam comportamentos proibidos, apenas os tornam puníveis.

Instrumentos jurídicos nacionais e comunitários

Legislação

As atividades legislativas se intensificaram progressivamente no campo da Internet, principalmente no âmbito dos países da UE e da OCDE, onde a Internet é amplamente usada e tem alto grau de impacto nas relações econômicas e sociais. Até o momento, as áreas prioritárias para a atividade legislativa em torno da Internet têm sido a privacidade, a proteção de dados, a propriedade intelectual, tributos e crimes cibernéticos. Porém, as relações sociais são complexas demais para serem reguladas somente por legisladores. A sociedade é dinâmica e a legislação sempre fica defasada com relação às mudanças sociais. Pode-se observar isso mais especificamente nos dias atuais, com o desenvolvimento tecnológico remodelando a realidade social a uma rapidez para além do que os legisladores conseguem acompanhar. Às vezes, as regras se tornam obsoletas mesmo antes de entrarem em vigor. O risco da obsolescência jurídica é um aspecto importante a ser considerado na regulação da Internet.

Normas sociais (costumes)

Assim como a legislação, as normas sociais prescrevem determinados comportamentos. Elas são cumpridas pela comunidade por meio da pressão entre pares. Nos primórdios da Internet, o seu uso foi regido por um conjunto de normas sociais classificadas como "netiqueta", no qual a pressão entre colegas e a exclusão eram as principais sanções. Durante esse período, no qual a Internet era basicamente usada por comunidades relativamente pequenas e na sua maioria acadêmicas, as regras sociais eram largamente observadas. O crescimento da Internet tornou essas regras ineficazes. Tal tipo de regulação pode ainda ser aplicado, no entanto em grupos restritos com fortes laços

comunitários. Por exemplo, a comunidade da Wikipédia é regida por normas sociais que regulam a forma como seus artigos são editados e a forma com que os conflitos referentes a tais artigos são resolvidos. Por meio da adoção de códigos de conduta, as regras da Wikipédia foram gradualmente evoluindo para a autorregulação.

Auto-regulação

O *White Paper* on *Internet Governance*[2] (Livro Branco sobre Governança da Internet), de 1998 elaborado pelo governo dos Estados Unidos, que abriu caminho para a fundação da ICANN, sugeria a autorregulação como mecanismo regulatório preferido da Internet. A autorregulação possui elementos em comum com as normas sociais anteriormente descritas. A principal distinção é que, diferentemente das normas sociais, que tipicamente envolve regras tácitas e difusas, a autorregulação tem como base um conjunto de regras explícitas e bem organizadas. As regras da autorregulação costumam codificar o conjunto de regras em forma de boa conduta. A tendência no sentido da autorregulação é particularmente evidente entre os ISPs. Em muitos países, os ISPs estão sob pressão crescente das autoridades governamentais para cumprir as regras relacionadas às políticas de conteúdo. Os ISPs tentam responder a tal pressão por meio da autorregulação ao impor determinados padrões de comportamento para seus clientes.

Embora a autorregulação possa ser uma técnica regulatória útil, alguns riscos permanecem ao aplicá-la para regular áreas de grande interesse público, como as políticas de conteúdo, a liberdade de expressão e a proteção da privacidade. Eles conseguem tomar decisões no lugar das autoridades judiciais? Os ISPs são capazes de julgar o que é um conteúdo aceitável?

Jurisprudência

Jurisprudência (o conjunto de precendentes judiciais) são o pilar do sistema jurídico dos EUA, o primeiro a abordar as questões jurídicas da Internet. Nesse sistema, os precedentes criam leis, principalmente nos casos que envolvem a regulação de novas questões, como a Internet. Os juízes têm que decidir casos mesmo que não tenham as ferramentas necessárias, isto é, as regras jurídicas. A primeira ferramenta jurídica que os juízes usam é a analogia jurídica, na qual algo novo é relacionado a algo conhecido. A maior

2 NTIA (1988) Statement of Policy on the Management of Internet Names and Addresses. Acessível em <http://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses> [acessado em 13 de fevereiro de 2014].

parte das ações judiciais referentes à Internet são resolvidas por meio de analogias.

Instrumentos jurídicos internacionais

A diferença entre direito internacional privado e direito internacional público

A natureza transnacional das atividades da Internet implica a necessidade do uso de ferramentas jurídicas internacionais. Em discussões sobre o direito internacional há uma confusão terminológica que poderia levar a consequências significativas. O termo direito internacional é principalmente usado como sinônimo de direito internacional público , estabelecido por estados nacionais, geralmente por meio da adoção de tratados e convenções. O direito internacional público é aplicável a muitas áreas da Internet, entre as quais as telecomunicações, os direitos humanos e crimes cibernéticos, entre outros. No entanto, o direito internacional privado é igualmente ou até mais importante no tratamento das questões referentes à Internet, uma vez que a maior parte dos processos judiciais envolvendo a Internet tratam de contratos, atos ilícitos e responsabilidades comerciais. As regras do direito internacional privado especificam os critérios para o estabelecimento da jurisdição e da lei aplicáveis em processos judiciais com elementos externos (ex., relações jurídicas envolvendo duas ou mais empresas de diferentes países). Por exemplo, quem tem jurisdição em possíveis casos jurídicos entre empresas da Internet (ex., Facebook, Twitter) e seus usuários espalhados em todo o mundo. Os critérios de jurisdição incluem a ligação entre o indivíduo e a jurisdição nacional (ex., nacionalidade, domicílio) ou a ligação entre uma transação particular e a jurisdição nacional (ex., no qual o contrato tenha sido concluído, tendo ocorrido a troca de bens).

Direito internacional privado

Dada a natureza global da Internet, as controvérsias jurídicas envolvendo pessoas e instituições de diferentes jurisdições nacionais são frequentes. Contudo, somente em raras situações o direito internacional privado foi utilizado para resolver questões relacionadas à Internet, possivelmente porque seus procedimentos geralmente são complexos, lentos e caros. Os principais mecanismos do direito internacional privado foram desenvolvidos em uma época em que a interação transnacional era menos frequente e intensa, e proporcionalmente menos processos envolviam pessoas e empresas de diferentes jurisdições.

Direito internacional público

O direito internacional público regula as relações entre estados nações. Alguns instrumentos do direito internacional público já tratam de algumas áreas de relevância para a governança da Internet (ex. regulações de telecomunicações, direitos humanos, convenções, tratados do comércio internacional). Nesta seção, a análise irá priorizar os elementos do direito internacional público que poderiam ser utilizados no campo da governança da Internet, entre os quais tratados e convenções, costumes, legislações não vinculativas e as normas premptórias de direito internacional (ius cogens).

Convenções internacionais

O principal conjunto de convenções de questões relacionadas à Internet foi adotado pela UIT, sendo as ITRs as mais importantes na elaboração de um quadro de políticas para as telecomunicações para subsequentes avanços da Internet. A versão atual das ITRs (1998) foi alterada na CMTI-12. Além das convenções da UIT, a única convenção que trata diretamente de questões relacionadas à Internet é a Convenção sobre Crime Cibernético do Conselho da Europa. No entanto, muitos outros instrumentos jurídicos internacionais abordam aspectos mais amplos da governança da Internet, como direitos humanos, comércio e direitos de propriedade intelectual.

Direito internacional consuetudinário

O desenvolvimento de regras consuetudinárias incluem dois elementos: a prática geral (consuetudo) e o reconhecimento de que tal prática é vinculativa juridicamente (opinio juris). Geralmente requer um longo período de tempo para a consolidação da prática geral.

Alguns elementos do direito consuetudinário aparecem na forma como o governo dos EUA realiza a supervisão da raiz da Internet, por meio da prática corrente de não intervenção na questão do gerenciamento dos domínios de países (ex., .ch, .uk., .ge). A prática geral é o primeiro elemento para a identificação do direito consuetudinário. Ainda é necessário saber se tal prática geral teve como base a percepção do governo dos EUA de que o gerenciamento dos domínios de país que realiza está em linha com as regras jurídicas internacionais (existência de opinio iuris). Se este for o caso, existe a possibilidade de identificar o direito consuetudinário internacional nas partes gerenciais do sistema de servidor-raiz da Internet que trata dos domínios de país. Seria difícil estender tal raciocínio ao status jurídico dos gTLDs (.com, .org, .edu, .net) que não envolvem outros países.

Soft Law

A Soft Law tem se tornado um termo frequentemente utilizado no debate sobre a governança da Internet. A maior parte das definições da legislação não vinculativa foca naquilo que ela não é: não é um instrumento juridicamente vinculante. Normalmente, os instrumentos da legislação não vinculativa contêm princípios e normas em vez de regras específicas que geralmente são encontradas em documentos internacionais como declarações e resoluções. Como não é juridicamente vinculativo, não pode ser executada por meio dos tribunais internacionais ou de outros mecanismos de resolução de disputas.

Os principais documentos da CMSI, inclusive a Declaração Final, o Plano de Ação e as Declarações Regionais, têm potencial para desenvolver determinadas normas da legislação não vinculativa. Não são juridicamente vinculativas, mas costumam ser o resultado de negociações prolongadas e aceitação por parte dos estados nacionais. O compromisso assumido pelos estados nacionais e outras partes interessadas na negociação dos instrumentos da legislação não vinculativa e na obtenção de um consenso necessário forma o primeiro elemento para considerar que tais documentos são mais que simples declarações políticas.

A Soft Law oferece algumas vantagens no seu tratamento das questões de governança da Internet. Primeiramente, é uma abordagem menos formal, não exigindo a ratificação por parte dos países e, consequentemente, não exigindo negociações prolongadas. Em segundo lugar, é flexível o suficiente para facilitar o teste de novas experiências e adaptações a avanços rápidos no campo da governança da Internet. Em terceiro lugar, a legislação não vinculativa aumenta a possibilidade de aplicação da abordagem multissetorial quando comparada à abordagem jurídica internacional restrita a países e organizações internacionais.

Ius cogens

O *ius cogens* é descrito pela Convenção de Viena sobre o Direito dos Tratados[3] no artigo 53 como "uma norma, aceita e reconhecida pela comunidade internacional dos países como um todo, com base na qual nenhuma derrogação é permitida e que pode ser modificada somente por uma norma subsequente do direito

3 Vienna Convention on the Law of Treaties. Acessível em <http://www.ilsa.org/jessup/jessup11/basicmats/VCLT.pdf> [acessado em 13 de fevereiro de 2014].

internacional geral de mesma natureza". O Professor Brownlie relaciona os seguintes exemplos das regras do ius cogens:

- A proibição do uso da força.
- As normas relativas a prevenção e a punição do crime de genocídio.
- O princípio da não discriminação racial.
- As normas relativas a prevenção e a punição de crimes contra a humanidade.
- As normas que proíbem o comércio de escravos e a pirataria[4].

No âmbito da governança da Internet, o ius cogens poderia ser usado para atividades que incentivem algumas destas regras (ex., genocídio, discriminação racial, escravidão).

Jurisdição

A jurisdição é a autoridade do tribunal e dos órgãos governamentais para decidir processos judiciais. A relação entre jurisdição e a Internet tem sido ambígua, uma vez que a jurisdição é definida predominantemente na divisão geográfica de territórios nacionais. Cada país tem o direito soberano de exercer jurisdição sobre seu território. Contudo, a Internet facilita intercâmbios internacionais consideráveis que são difíceis (mas não impossíveis) de monitorar por meio de mecanismos governamentais tradicionais. A questão da jurisdição na Internet enfatiza um dos dilemas centrais associados a sua governança: como delimitar a Internet com base na geografia jurídica e política existente?[5]

Jurisdição – técnicas básicas

Três principais considerações são importantes na decisão sobre determinada jurisdição:

- Qual tribunal ou autoridade governamental tem autoridade competente (jurisdição processual)?
- Quais regras deveriam ser aplicadas (jurisdição substantiva)?
- De que forma implementar decisões judiciais (jurisdição de execução)?

4 Brownlie I (1999) Principles of Public International Law, 5th Ed. Oxford: Oxford University Press, p. 513.

5 Salis RP (2001) A Summary of the American Bar Association's (ABA) Jurisdiction in Cyberspace Project: Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet. Acessível em <http://www.jstor.org/discover/10.2307/40687955?uid=3738216&uid=2&uid=4&sid=21103388060741> [acessado em 13 de fevereiro de 2014].

Os critérios a seguir estabelecem jurisdição em casos específicos:

- **Princípio Territorial** – o direito do país de decidir sobre pessoas e propriedades dentro de seu território.
- **Princípio da Personalidade** – o direito do país de decidir sobre seus cidadãos onde quer que eles estejam (princípio da nacionalidade).
- **Princípio dos Efeitos** – o direito do país de decidir sobre os efeitos econômicos e jurídicos em seu território, resultante de atividades realizadas no exterior.

Outro princípio importante apresentado pelo direito internacional moderno é o princípio da jurisdição universal[6]. "O conceito de jurisdição universal em seu sentido mais amplo (é) o poder do país de punir determinados crimes, independentemente de onde tal crime tenha sido cometido e por quem, sem que haja necessidade de haver conexão com o território, a nacionalidade ou o interesse específico do país[7]". A jurisdição universal abrange crimes como pirataria, crimes de guerra e genocídio.

Conflito de jurisdição

O conflito de jurisdição surge quando mais de um país reivindica jurisdição sobre um processo jurídico específico. Geralmente, ocorre quando um processo jurídico envolve um componente extraterritorial (ex., envolve pessoas de diferentes países ou transações internacionais). A jurisdição competente é estabelecida por um dos seguintes elementos: territorialidade, nacionalidade ou efeito da ação/fato). Ao publicar conteúdo ou interagir na Internet, é difícil saber qual lei nacional, se houver, poderá ser violada. Neste contexto, quase qualquer atividade da Internet tem um aspecto internacional que poderia levar a múltiplas jurisdições ou ao chamado *spillover effect* (efeito de transbordamento)[8].

Um dos primeiros e frequentemente citados casos que exemplificam o problema das jurisdições múltiplas é o processo do Yahoo! de 2001

6 Uma das principais fontes neste campo é Princeton Principles on Universal Jurisdiction (2001). Acessível em <http://www1.umn.edu/humanrts/instree/princeton.html> [acessado em 13 de fevereiro de 2014].

7 Malanczuk P (1997) Akehurst's Modern Introduction to International Law. Londres: Routledge, p. 113.

8 Para um panorama geral dos casos envolvendo jurisdição extraterritorial relacionada ao conteúdo da Internet, ver Timofeeva YA (2005) Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis. Connecticut Journal of International Law, 20, 199. Acessível em <http://ssrn.com/abstract=637961> [acessado em 13 de fevereiro de 2014].

na França[9]. Foi provocado por uma infração segundo a lei francesa, que proíbe a exibição e venda de objetos nazistas, mesmo que o sítio web que tenha disponibilizado tais itens – o sítio web de leilão Yahoo.com – seja hospedado nos Estados Unidos, e a exibição de tais materiais esteja dentro da lei, à epoca e ainda hoje. O processo judicial foi resolvido por meio de solução técnica (software de geolocalização e filtragem do acesso). O Yahoo! foi obrigado a identificar os usuários que acessaram o site da França e bloquear seu acesso às paginas do sítio web que estavam mostrando tais materiais nazistas[10].

Além das soluções técnicas (geolocalização e filtragem), outras abordagens para a resolução do conflito de jurisdição incluem a harmonização das leis nacionais e a utilização da arbitragem.

Harmonização das leis nacionais

VER A SEÇÃO 2 PARA UMA DISCUSSÃO MAIS APROFUNDADA SOBRE CIBERSEGURANÇA E SPAM

A harmonização das leis nacionais poderia resultar no estabelecimento de um conjunto de regras equivalentes no nível global. Com regras idênticas sendo aplicadas, a questão da jurisdição seria menos relevante. A harmonização seria alcançada em áreas nas quais um alto nível de consenso global já exista, como por exemplo, a pornografia infantil, a pirataria, a escravidão e o terrorismo. Os pontos de vista são convergentes em outras questões também, como os crimes cibernéticos. No entanto, em alguns campos, entre os quais a política de conteúdo, não é provável que haja consenso global sobre as regras básicas, uma vez que as diferenças culturais continuam a entrar em choque no ambiente online de forma mais marcante do que no ambiente offline[11]. Outra possível consequência da falta de harmonização é a migração dos materiais da Web para países com níveis mais baixos de regulação da Internet. Fazendo uma analogia com o Direito do Mar, alguns países talvez se tornem "bandeiras de conveniência" ou centros "offshore" do mundo da Internet.

9 EDRI-gram (2006) French anti-hate groups win case against Yahoo! Acessível em <http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html> [acessado em 17 de fevereiro de 2014].

10 Outras ações judiciais incluem o processo do Tribunal de Justiça da Alemanha contra Fredrick Toben, ex-cidadão alemão com nacionalidade australiana que publicou em um sítio web com base na Austrália materiais questionando a existência do holocausto. Acessível em <http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html> [acessado em 13 de fevereiro de 2014].

11 Conteúdo racista e pornografia (nos casos apresentados acima) não são as únicas questões polêmicas – outros exemplos incluem jogos ilegais, publicidade de cigarro e venda de drogas.

Arbitragem

A arbitragem é um mecanismo de resolução de controvérsias acessível, substituindo os tribunais tradicionais. Nas arbitragens, as decisões são tomadas por uma ou mais pessoas independentes escolhidas pelos contendedores. A arbitragem internacional no âmbito do setor empresarial tem longa tradição. O mecanismo de arbitragem geralmente é estabelecido por meio de um contrato privado entre as partes que concordam em resolver quaisquer disputas futuras por meio da arbitragem. Uma grande quantidade de contratos de arbitragem está disponível, definindo questões como o local da arbitragem, procedimentos e a eleição do foro.

A **tabela 2** apresenta um breve panorama das principais diferenças entre os sistemas do tribunal tradicional e da arbitragem.

Quando comparada à justiça tradicional, a arbitragem oferece muitas vantagens, entre as quais mais flexibilidade, menos despesas, velocidade, eleição do foro e facilitação do cumprimento das sentenças de

TABELA 2

Elementos	*Competência jurídica*	*Arbitragem*
Organização	Resolução por leis/tratados – permanente.	Resolução pelas partes envolvidas (temporária, ad hoc). Resolução por convenções (permanente).
Lei aplicável	A lei do tribunal (o juiz decide sobre a lei aplicável).	As partes podem escolher a lei; caso não a escolham, devem optar pela lei indicada no contrato; se não houver indicação, pela lei do órgão de arbitragem.
Procedimento	Procedimentos judiciais definidos em lei/ tratados.	Definido pelas partes envolvidas (temporário, ad hoc). Definido pelo regulamento do órgão de arbitragem (permanente).
Competência/ Objeto da controvérsia	Definido pelas leis/tratados com relação ao objeto da controvérsia	Definido pelas partes

arbitragem estrangeira. Uma das principais vantagens da arbitragem é que ela supera o possível conflito de jurisdição. A arbitragem apresenta vantagens específicas com relação a uma das mais difíceis tarefas nos processos judiciais relacionados à Internet, o cumprimento de decisões (sentenças arbitrais). A Convenção de Nova York sobre Reconhecimento e Execução de Sentenças Arbitrais Estrangeiras[12] regula o cumprimento de sentenças arbitrais. De acordo com esta convenção, os tribunais nacionais são obrigados a executar as sentenças arbitrais. Paradoxalmente, costuma ser mais fácil executar sentenças arbitrais em outros países com base no regime da Convenção de Nova York em vez de fazer cumprir uma sentença judicial estrangeira.

A principal limitação da arbitragem é que ela não consegue tratar das questões de maior interesse público, como a proteção dos direitos humanos; tais questões requerem a intervenção dos tribunais estabelecidos pelo poder público.

A arbitragem tem sido usada extensivamente em disputas judiciais. Existe um sistema de regras e instituições bem desenvolvido que trata de tais disputas comerciais. O principal instrumento internacional é a Lei Modelo sobre Arbitragem Comercial Internacional[13] de 1985 da Comissão das Nações Unidas sobre Direito do Comércio Internacional (CNUDCI). As principais arbitragens tradicionais são geralmente anexadas a câmaras de comércio.

Arbitragem e a Internet

A arbitragem e outros sistemas alternativos de resolução de disputas são usados extensivamente para preencher uma lacuna resultante da incapacidade do atual direito internacional privado para tratar de casos internacionais. Um exemplo específico de um método de resolução de disputas alternativo em casos relacionados à Internet é a Política para Resolução Uniforme de Litígios sobre Nomes de Domínio (UDRP), desenvolvida pela OMPI e implementada pela ICANN como principal procedimento de resolução de disputas. Desde o início de seus trabalhos nos termos da UDPR em dezembro de 1999, o Centro de Arbitragem e Mediação da OMPI já administrou mais de 22.500 casos, sendo que com a introdução

12 CNUDCI(1958) The New York Convention. Disponível em <http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/1985Model_arbitration.html>[acessado em 13 de fevereiro de 2014].

13 CNUDCI (1985) Model Law in International Commercial Arbitration. Disponível em <http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/1985Model_arbitration.html>[acessado em 13 de fevereiro de 2014].

de novos gTLDs, espera-se que surjam novas contestações.[14]

A UDRP é estipulada com antecedência como mecanismo de resolução de disputas em todos os contratos envolvendo o registro de gTLDs (ex., .com, .edu, .org, .net) e para alguns ccTLDs também. O que a torna singular é que as sentenças arbitrais são aplicadas diretamente por meio de mudanças no DNS, sem recorrer à aplicação da lei por meio de tribunais nacionais.

A arbitragem é um meio de resolução de disputas mais rápido, mais simples e mais barato. No entanto, a utilização da arbitragem como principal mecanismo de resolução de disputas relacionadas à Internet tem algumas sérias limitações.

- Em primeiro lugar, como a arbitragem geralmente é estabelecida por um contrato prévio, ela não cobre diversas áreas nas quais existem questões em que nenhum contrato entre as partes foi estabelecido com antecedência (difamação, vários tipos de responsabilidades, crimes cibernéticos).
- Em segundo lugar, muitos enxergam a atual prática de anexar a cláusula de arbitragem a contratos regulares como uma desvantagem para a parte mais vulnerável do contrato (geralmente um usuário da Internet ou um cliente do comércio eletrônico).
- Em terceiro lugar, algumas pessoas receiam que a arbitragem amplie a lei baseada em precedentes (sistema jurídico dos Estados Unidos/Reino Unido) globalmente e gradualmente elimine outros sistemas jurídicos nacionais. No caso do comércio eletrônico, talvez isso acabe sendo mais aceitável, dado o alto grau de unificação das regras substantivas do direito comercial. Contudo, a ampliação da jurisprudência se tornou mais delicada em questões socioculturais como o conteúdo da Internet, no qual um sistema jurídico nacional reflete contextos culturais específicos.

VER A SEÇÃO 1
PARA UMA DISCUSSÃO MAIS APROFUNDADA SOBRE DNS

Direitos de propriedade intelectual (DPI)

O conhecimento e as ideias são recursos fundamentais na economia global, sendo que protegê-los, por meio dos DPI, tornou-se uma das questões predominantes no debate sobre a governança da Internet, além de conter um componente fortemente orientado para desenvolvimento. Os DPI foram afetados pelo desenvolvimento da Internet, principalmente por meio da digitalização do conhecimen-

14 OMPI (2012) WIPO Prepares for Launch of New gTLDs while Cybersquatting Cases Continued to Rise. Disponível em <http://www.wipo.int/pressroom/en/articles/2012/article_0002.html> [acessado em 13 de fevereiro de 2014].

to e de informações, bem como por meio de novas possibilidades de manipulá-los. Os DPI relacionados à Internet inclui direitos autorais, marcas registradas e patentes. Outros DPI incluem projetos, modelos de utilidade, segredos comerciais, indicações geográficas e variedades de plantas.

Direitos autorais

Os direitos autorais somente protegem a expressão de uma ideia quando esta é materializada em várias formas, como livros, CDs ou arquivos de computador. A ideia em si não é protegida pelos direitos autorais. Na prática, às vezes é difícil fazer uma clara distinção entre a ideia e a expressão.

O regime de direitos autorais acompanhou de perto a evolução tecnológica. Toda nova invenção, como a imprensa escrita, o rádio, a televisão e o VCR, foi afetada tanto pela forma quanto pela aplicação das regras dos direitos autorais. A Internet não foge à regra. O conceito tradicional dos direitos autorais foi contestado de diversas formas, desde os textos mais simples de "copia e cola" da Web até atividades mais complexas, como a distribuição em massa de materiais de música e vídeo via Internet.

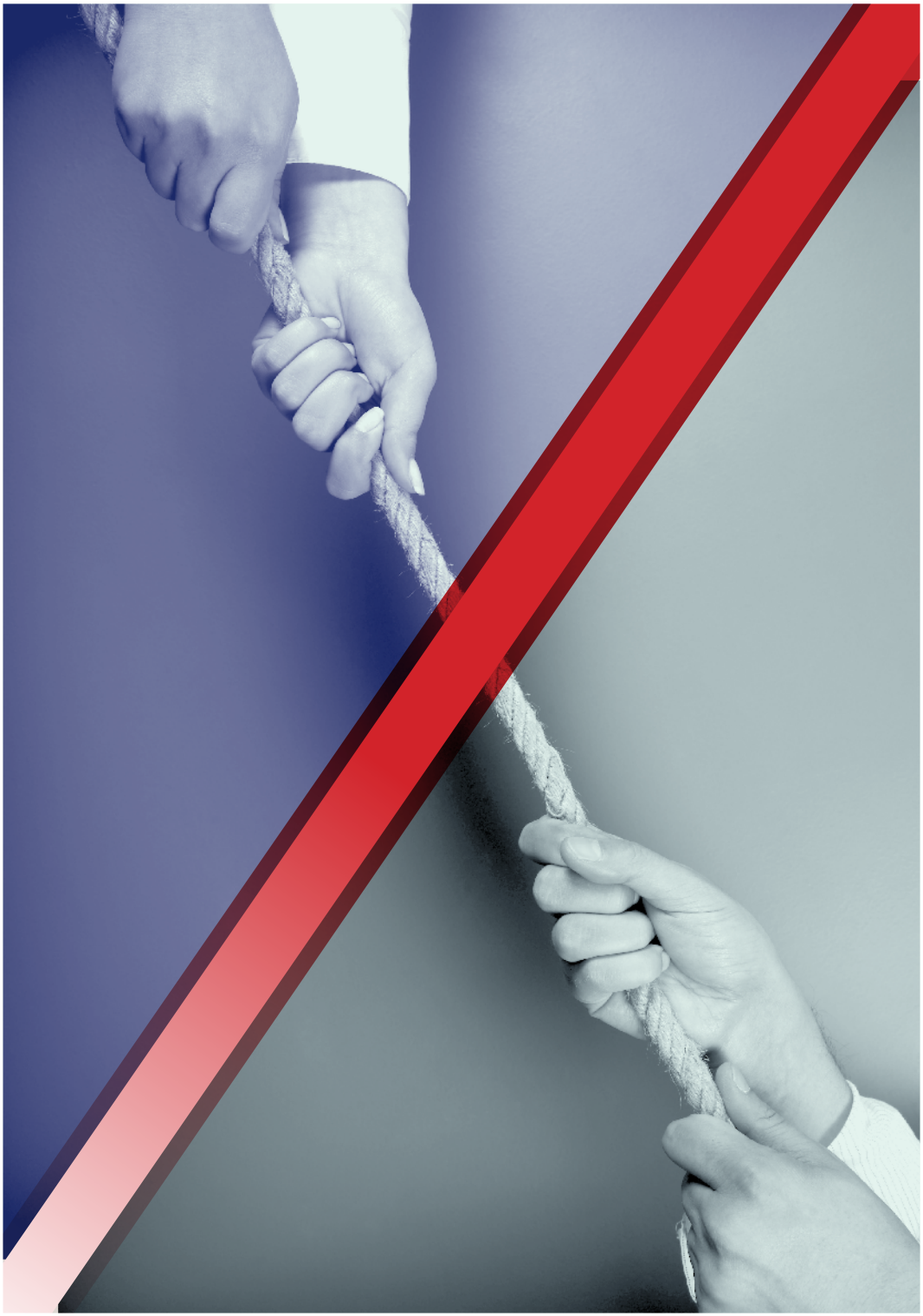
A Internet também fortalece os detentores dos direitos autorais, ao conceder a eles ferramentas técnicas mais poderosas para proteger e monitorar a utilização de material protegido por direitos autorais. Estes avanços colocam em risco o equilíbrio delicado entre os direitos do autor e o interesse público, que é a base dos direitos autorais.

Até o momento, os detentores de direitos autorais representados por grandes gravadoras e empresas de multimídia têm sido muito ativos na proteção de seus DPIs. A percepção do interesse público tem sido vaga e sua proteção tem sido baixa. Isto, contudo, vem mudando gradualmente, principalmente com inúmeras iniciativas globais que priorizam o acesso aberto ao conhecimento e à informação (ex. *Creative Commons*).

Situação atual

Proteção de direitos autorais mais rígida nos níveis nacional e internacional

As indústrias fonográfica e de entretenimento têm feito lobby intenso nos âmbitos nacional e internacional para fortalecer a proteção aos direitos autorais. Nos Estados Unidos, a proteção mais rígida aos direitos autorais foi introduzida pela Lei dos Direitos Auto-



rais do Milênio Digital dos Estados Unidos (DMCA), de 1998. No nível internacional, a proteção de artefatos digitais foi introduzida no Tratado de Direitos Autorais da OMPI (1996). Este tratado inclui disposições para fortalecer o regime de proteção de direitos autorais, como disposições mais rígidas de limitações dos direitos exclusivos de autor, a proibição de contornar a proteção tecnológica de direitos autorais e outras medidas relacionadas.

Diversas regulações foram promulgadas nos níveis nacional e internacional, buscando executar um controle mais rígido ao obrigar os intermediários da Internet a filtrar ou monitorar a disseminação de conteúdo com copyright. Elas despertaram forte reação pública, que impediu a adoção destas regulações. Em 2011, nos Estados Unidos, dois projetos de lei foram promovidos – o *Stop Online Piracy Act* (SOPA)[15] e o *PROTECT IP Act* (PIPA)[16] – fornecendo novos meios de combater a pirataria online, inclusive bloqueando o acesso a sítios web que infringem a lei e proibindo os motores de busca a incluírem links a tais sítios web. No nível internacional, o Acordo Comercial Anticontrafação (ACTA)[17] buscou tratar das infrações aos DPI pensando em viabilizar a execução privada e ações de policiamento. Após fortes protestos na Europa, o Parlamento Europeu votou contra o ACTA. Estas ações regulatórias foram duramente criticadas por acadêmicos e grupos a favor das liberdades civis com base em fundamentos relacionados aos direitos humanos e à liberdade. Os usuários individuais da Internet aderiram aos protestos online e offline.[18]

Software contra a infração de direitos autorais

As ferramentas utilizadas por criminosos podem também ser utilizadas pelos defensores dos direitos autorais. Normalmente, as autoridades públicas e as empresas executam suas responsabilidades por meio de mecanismos jurídicos. No entanto, a utilização de ferramentas de

15 Mashable (sem data) Stop Online Piracy Act. Acessível em <http://mashable.com./category/stop-online-piracy-act/>[acessado em 17 de fevereiro de 2014].

16 Senado dos EUA (sem data) Protect IP Act. Disponível em <http://www.leahy.senate.gov/imo/media/doc/BillText-PROTECTIPAct.pdf> [acessado em 17 de fevereiro de 2014].

17 Anti-Counterfeiting Trade Agreement. Acessível em <http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147937.pdf> [acessado em 10 de abril de 2014].

18 La Quadrature du Net, grupo de defesa dos direitos civis, acompanhou atentamente os desenvolvimentos da lei HADOPI e elaborou um arquivo abrangente sobre a ACTA. Acessível em <http://www.laquadrature.net/en/ACTA> [acessado em 13 de fevereiro de 2014]. Para informações sobre os protestos contra os projetos de lei dos EUA, ver Vijayan J (2012) Protests against SOPA, PIPA go viral, Computerworld. Disponível em <http://www.computerworld.com/s/article/9223496/Protests_against_SOPA_PIPA_go_viral> [acessado em13 de fevereiro de 2014].

software "alternativas" pelo setor empresarial contra violadores de direitos autorais está aumentando.

Um artigo no *New York Times* listou as seguintes táticas baseadas em software, utilizadas por gravadoras e empresas de entretenimento para proteger seus direitos autorais:

- Um programa *Trojan Horse* redireciona os usuários para sítios web onde eles podem comprar de forma legítima a música que eles tentaram baixar.
- Um software de bloqueio que inviabiliza os computadores por determinado período e exibe um aviso sobre baixar música pirateada.
- Silêncio, quando os discos rígidos são escaneados e tenta-se remover quaisquer arquivos pirateados encontrados.
- A interdição evita o acesso à Internet daqueles que tentarem baixar música pirateada.

O Professor Lawrence Lessig, agora na faculdade de Direito Harvard alertou que tais medidas talvez sejam ilegais.[19] As empresas que adotaram tais medidas em causa própria teriam violado a lei?

Tecnologias para a gestão de direitos digitais

Com uma abordagem de longo prazo e mais estrutural, o setor empresarial introduziu várias tecnologias para gerir o acesso a materiais protegidos por direitos autorais. A Microsoft implementou um software de gestão de direitos digitais para gerir o download de arquivos de som, filmes e outros materiais protegidos por direitos autorais. Sistemas similares foram desenvolvidos pela Xerox (*ContentGuard)*, Philips e Sony (*InterTrust*).

A utilização de ferramentas tecnológicas para a proteção de direitos autorais tem fundamento jurídico no Tratado dos Direitos Autorais da OMPI e na DMCA. Ademais, a DMCA penaliza a atividade cujo objetivo é contornar a proteção tecnológica dos materiais protegidos por direitos autorais.

Questões

Alterar mecanismos de direitos autorais existentes ou criar novos?

De que forma os mecanismos de direitos autorais deveriam ser adaptados para refletir as profundas mudanças realizadas pelos avanços

19 Sorkin AR (2003) Software bullet is sought to kill musical piracy. New York Times 4 de maio. Acessível em <http://www.nytimes.com/2003/05/04/business/04MUSI.html> [acessado em 13 de fevereiro de 2014].

das TIC e da Internet? Uma resposta sugerida pelo White Paper on Intellectual Property and the National Information Infrastructure (Livro Branco sobre Propriedade Intelectual e a Infraestrutura de Informação Nacional)[20] elaborado pelo governo dos EUA é que somente pequenas mudanças são necessárias na regulação existente, principalmente por meio da "desmaterialização" dos conceitos do direito autoral de "fixação", "distribuição", "transmissão" e "publicação". Esta abordagem foi adotada nos principais tratados internacionais sobre direitos autorais, entre os quais o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio (TRIPS) e o Tratado de Direitos Autorais da OMPI.

Contudo, visões contrárias argumentam que as mudanças no sistema jurídico devem ser profundas, uma vez que os direitos autorais na era digital não estão somente relacionados ao "direito de evitar a cópia", mas também ao "direito de evitar o acesso". Por fim, com cada vez mais possibilidades técnicas de restrição do acesso a materiais digitais, pode-se questionar se a proteção aos direitos autorais é no fim necessária. Falta saber de que forma o interesse público, a segunda parte da equação dos direitos autorais, será protegido.

Proteção do interesse público – o "uso justo" dos materiais protegidos por direitos autorais

Os direitos autorais foram inicialmente concebidos para estimular a criatividade e a inventividade, e é por isso que combinaram dois elementos: a proteção dos direitos do autor e a proteção do interesse público. O principal desafio era estipular de que forma o público poderia acessar os materiais protegidos por direitos autorais para aumentar a criatividade, o conhecimento e o bem estar global. Em termos operacionais, a proteção do interesse público é garantida por meio do conceito do "uso justo" dos materiais protegidos.[21]

Direitos autorais e desenvolvimento

Qualquer restrição ao uso justo poderia enfraquecer a posição dos países em desenvolvimento. A Internet oferece a pesquisadores, estudantes e outras pessoas destes países em desenvolvimento uma ferramenta poderosa de participação em intercâmbios científicos

20 Escritório de Patentes e Marcas Registradas dos Estados Unidos (sem data) Intellectual Property and the National Information Infrastructure. Acessível em <https://www.uspto.gov/web/offices/com/doc/ipnii/>[acessado em 13 de fevereiro de 2014].

21 Para uma explicação do conceito de"uso justo" e exemplos ver The UK Copyright Service (sem data) Copyright Law fact sheet P-09: Understanding Fair Use. Acessível em <http://www.copyrightservice.co.uk/copyright/p09_fair_use> [acessado em 13 de fevereiro de 2014].

e acadêmicos globais. Um regime de direitos autorais restritivo poderia causar um impacto negativo no desenvolvimento de capacidades em países em desenvolvimento. Outro aspecto é a digitalização crescente das obras culturais e artísticas dos países em desenvolvimento. Paradoxalmente, os países em desenvolvimento talvez tenham que pagar por seu patrimônio cultural e artístico quando este for digitalizado, reembalado e tornado propriedade de empresas estrangeiras de entretenimento e mídia.

OMPI e TRIPS

Existem dois importantes regimes para os direitos de propriedade intelectual. A OMPI administra o regime de DPI com base nas convenções de Paris e Berna. Outro regime emergente é executado pela OMC e toma como base a TRIPS. Transferiu-se a coordenação dos DPI internacional da OMPI para a OMC para fortalecer a proteção dos mesmos, principalmente com relação a seu cumprimento. Este foi um dos grandes ganhos dos países desenvolvidos durante a Rodada do Uruguai das negociações da OMC.

Muitos países em desenvolvimento estão preocupados com este fato. Os rígidos mecanismos de cumprimento da OMC poderiam reduzir o espaço de manobra dos países em desenvolvimento, bem como a possibilidade de equilibrar as necessidades de desenvolvimento com a proteção de direitos de propriedade intelectual internacionais. Até o momento, o principal foco da OMC e do TRIPS tem sido as várias interpretações do DPI para produtos farmacêuticos. É bem provável que as futuras discussões sejam estendidas ao DPI e à Internet.

A responsabilidade dos ISPs na violação dos direitos autorais

Os mecanismos internacionais de cumprimento no campo da propriedade intelectual fortaleceram-se ainda mais ao fazer com que os ISPs fossem responsabilizados por hospedar materiais que violam os direitos autorais, caso tais materiais não sejam removidos após notificação de violação. Isto tornou o regime do DPI, vago até então, diretamente aplicável no campo da Internet.

A abordagem escolhida pela DMCA dos Estados Unidos e pelas diretivas da União Europeia[22] é de eximir o provedor de serviços de respon-

22 União Europeia [UE] (2000) Diretiva 2000/31/EC do Parlamento Europeu e do Conselho de 8 junho de 2000 sobre determinados aspectos jurídicos dos serviços da sociedade da informação, mais especificamente o comércio eletrônico, no Mercado Interno (Directive on electronic commerce) e Diretiva 2001/29/EC do Parlamento Europeu e do Conselho de 22 de maio de 2001 sobre a harmonização de determinados aspectos dos direitos autorais e direitos relacionados na sociedade de informação. Mais informações disponíveis em <http://europa.eu/legislation_summaries/consumers/

sabilidade pela informação transmitida ou armazenada conforme direção dos usuários, exigindo que o provedor de serviços atue com base no procedimento de "Notificação e Retirada".[23] Esta solução alivia um pouco os ISPs porque os exime de sanções jurídicas, mas ao mesmo tempo os transforma em juízes de conteúdo[24] e resolve o problema apenas parcialmente, uma vez que o conteúdo contestado pode ser publicado em outro sítio web, hospedado por outro ISP. Um caso particularmente relevante para o futuro dos direitos autorais na Internet é o processo contra a *Grokster* e a *StreamCast*, duas empresas que produzem software de compartilhamento de arquivo P2P. Com base nas disposições da DMCA, a Associação da Indústria Fonográfica Americana (RIAA) solicitou que essas empresas desistissem de desenvolver tecnologias de compartilhamento de arquivos que contribuíssem para a violação dos direitos autorais. Em princípio, a justiça dos EUA decidiu não responsabilizar empresas de software como a *Grokster* e a *StreamCast* por possíveis violações dos direitos autorais, em circunstâncias razoáveis. No entanto, em junho de 2005, a Suprema Corte dos Estados Unidos decidiu que os desenvolvedores de software eram responsáveis por quaisquer utilizações indevidas de software. A *Electronic Frontier Foundation* (EFF) entendeu o caso como um prelúdio de uma onda de ações judiciais interpostas nos anos seguintes contra pessoas e ISPs, totalizando 30.000 processos em 2008.[25] Apesar de a RIAA ter abandonado sua campanha pelo litígio, as ações judiciais referentes à violação de direitos autorais continuam em destaque e aumentam em diversidade no mesmo ritmo que os avanços tecnológicos.[26]

protection_of_consumers/l24204_en.htm> [acessado em 13 de fevereiro de 2014].

23 O procedimento de "Notificação e Retirada" se refere à obrigação dos provedores de serviços de remover conteúdo dos sítios web por eles administrados caso recebam notificação ou reclamação referente à legalidade de um conteúdo específico.

24 Por medo de enfrentar possíveis sanções jurídicas, alguns ISPs preferem restringir o acesso a conteúdo indicado mesmo quando não há infração. Para mais informações, consultar os seguintes estudos de caso: Europa (Países Baixos): Nas S (2004) The Multatuli Project ISP Notice & Take Down, Bits of Freedom. Acessível em <https://www-old.bof.nl/docs/researchpaperSANE.pdf> [acessado em 13 de fevereiro de 2014]. EUA: Urban J e Quilter L (2006), Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act. Acessível em <http://static.chillingeffects.org/Urban-Quilter-512-summary.pdf> [acessado em 13 de fevereiro de 2013].

25 EFF (2008) RIAA v. The People: Five Years Later. Acessível em <https://www.eff.org/wp/riaa-v-people-five-years-later> [acessado em 13 de fevereiro de 2014].

26 Ver exemplo da última tendência nos EUA – a "trollagem" dos direitos autorais: Kravets D (2012) Judge Orders Failed Copyright Troll to Forfeit 'All' Copyrights. Wired.com. Acessível em <http://www.wired.com/threatlevel/2012/03/troll-forfeits-copyrights> [acessado em 13 de fevereiro de 2014].

Marcas registradas

As marcas registradas são relevantes para a Internet devido ao registro dos nomes de domínio. No início do desenvolvimento da Internet, o registro dos nomes de domínio tinha como base o princípio "quem chegar primeiro é atendido primeiro". Isto levou à especulação com a prátca de registro de nomes (ciberespeculação), que é a prática de registrar nomes de empresas e vendê-los depois por um preço mais alto. Esta situação obrigou o setor empresarial a colocar a questão da proteção de marcas registradas no centro da reforma da governança da Internet, levando à criação da ICANN em 1998. No *White Paper* sobre a criação da ICANN, o governo dos Estados Unidos exigiu que a ICANN desenvolvesse e implementasse um mecanismo de proteção de marcas registradas no campo dos nomes de domínio. Logo após sua constituição, a ICANN implementou o Política para Resolução Uniforme de Litígios sobre Nomes de Domínio (UDRP)[27] elaborado pela OMPI.

Patentes

Normalmente, a patente protege um novo processo ou produto de natureza predominantemente técnica ou produtiva. Faz pouco tempo que as patentes começaram a ser concedidas para software. Mais registros de patente resultam em mais ações judiciais entre empresas de software dos Estados Unidos, envolvendo quantias expressivas de dinheiro. Algumas patentes foram concedidas para processos comerciais, resultando em algumas polêmicas, como o pedido da British Telecom por taxas de licença pela patente de links de hipertexto, registrado pela empresa nos anos 80. Em agosto de 2002, o processo foi indeferido.[28] Se a British Telecom tivesse ganhado o processo, os usuários da Internet teriam que pagar uma taxa por cada link de hipertexto criado ou usado. É importante enfatizar que a prática de conceder patentes a procedimentos relacionados a software e à Internet não foi aceita na Europa e em outras regiões.[29]

---

27 Para um estudo abrangente das principais questões envolvendo UDRP, consultar a OMPI (2011) WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Second Edition (WIPO Overview 2.0) Acessível em <http://www.wipo.int/amc/en/index.html> [acessado em 13 de fevereiro de 2014].

28 Loney M (2002) Hyperlink patent case fails to click. CNET News.com. Acessível em <http://news.cnet.com/2100-1033-955001.html> [acessado em 13 de fevereiro de 2014].

29 Para mais informações sobre o debate na Europa sobre a patenteabilidade de software, consultar <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>[acessado em 13 de fevereiro de 2014].

Crimes cibernéticos

A dicotomia entre a abordagem real e a abordagem ciber às questões legais faz parte da discussão sobre o crime cibernético. A abordagem do direito real enfatiza que o crime cibernético é o mesmo que um crime offline, mas é praticado utilizando um computador que provavelmente está conectado à Internet. O crime é o mesmo, somente as ferramentas são diferentes. A abordagem do ciberdireito enfatiza que elementos específicos do crime cibernético justificam o tratamento especial, principalmente com relação à aplicação da lei e à prevenção. Os relatores da Convenção sobre Crime Cibernético do Conselho da Europa[30] pendiam para a abordagem do direito real, enfatizando que o único aspecto específico do crime cibernético era a utilização das TIC como meio de cometer o crime. A convenção, que entrou em vigor em 1o de julho de 2004, é o principal instrumento internacional na área. Contudo, a relevância do tópico crime cibernético o colocou na agenda de diversas organizações internacionais, regionais e locais, devido a sua recorrência e à diversificação dos crimes cometidos em sistemas de rede eletrônicos.[31] Uma das iniciativas mais recentes que vale a pena mencionar é a Iniciativa da Comunidade de Nações Contra Crimes Cibernéticos[32] que foi gerada dentro do Fórum de Governança da Internet da Commonwealth (CIGF). O setor empresarial também reconheceu a importância de combater o crime cibernético e começou iniciativas privadas para apoiar campanhas de conscientização e a melhoria de disposições jurídicas.[33]

Questões

Definição de crime cibernético

A definição de crime cibernético tem relevância prática e implicações jurídicas. Se o foco forem os atos ilícitos cometidos contra sistemas

30 Convenção sobre Crime Cibernético do Conselho da Europa (2001) Acessível em <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> [acessado em 13 de fevereiro de 2014]

31 Para ver a relação de redes, organizações e iniciativas de combate ao crime cibernético no mundo, ver as fontes nas páginas online do Conselho da Europa, acessível em <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/networks/Networks_en.asp> [acessado em 13 de fevereiro de 2014].

32 Fórum de Governança da Internet da Commonwealth (2012) Commonwealth Cybercrime Initiative. Acessível em <http://www.commonwealthigf.org/cigf/cybercrime> [acessado em 13 de fevereiro de 2014].

33 A título de exemplo, ver McAfee Initiative to Fight Cybercrime site and its Multipoint Strategy. Acessível em <http://www.mcafee.com/us/campaigns/fight_cybercrime/strategy.html> [acessado em 13 de fevereiro de 2014].

de computador, o crime cibernético incluiria acesso não autorizado; dano a dados ou programas do computador; sabotagem para prejudicar o funcionamento do sistema do computador ou da rede; interceptação não autorizada de dados para um sistema ou rede, de tal sistema ou rede ou dentro de tal sistema ou rede; bem como espionagem via computador. A definição de crime cibernético como sendo todos os crimes cometidos pela Internet e sistemas de computador incluiria uma ampla gama de crimes, inclusive aqueles especificados na Convenção do Crime Cibernético: fraudes envolvendo computador, violações de direitos autorais, pornografia infantil e segurança de rede.

Crimes cibernéticos e a proteção dos direitos humanos

A Convenção sobre Crime Cibernético reforçou a discussão sobre o equilíbrio entre segurança e direitos humanos. Muitas preocupações vieram à tona, articuladas principalmente pela sociedade civil, referentes a se a convenção confere às autoridades públicas poder demasiadamente amplo, inclusive o direito de verificar os computadores de hackers, vigiar a comunicação, entre outros. Esses amplos poderes poderiam potencialmente colocar em risco alguns direitos humanos, mais especificamente a privacidade e a liberdade de expressão.[34] A Convenção sobre Crime Cibernético foi adotada pelo Conselho da Europa, um dos promotores mais ativos dos direitos humanos. Isto talvez ajude no estabelecimento do equilíbrio necessário entre o combate ao crime cibernético e a proteção dos direitos humanos.

Coleta e preservação de provas

Um dos principais desafios no combate ao crime cibernético é a coleta de provas para ações judiciais. A velocidade da comunicação atualmente requer uma resposta rápida dos órgãos de aplicação da lei. Uma das possibilidades de preservação de provas são os logs de acesso a rede, que oferecem informação sobre quem acessou determinados recursos da Internet, e quando eles foram acessados. A Convenção sobre Crime Cibernético especifica a obrigação de providenciar procedimentos para preservar dados de tráfego da Internet. Sob a crescente pressão de ameaças cibernéticas e ataques terroristas, a UE deu um passo adiante e adotou a Diretiva de Retenção de Dados[35] que

34 Para uma opinião crítica da Convenção contra o Crime Cibernético expressando a preocupação da sociedade civil e dos ativistas de direitos humanos, consultar: The Association for Progressive Communication Report on the Cybercrime Convention. Acessível em <http://rights.apc.org/privacy/treaties_icc_bailey.shtml> [acessado em 13 de fevereiro de 2014]

35 Parlamento Europeu (2006) Data Retention Directive. Acessível em <http://eur-lexeuropa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF> [acessado em 13 de fevereiro de 2014].

requer que as ISPs retenham tráfego e dados da localização "com o objetivo de investigar, detectar e processar crimes graves, conforme definido por cada estado membro nos termos de sua legislação nacional" (Artigo 1). Esta disposição foi duramente criticada com fundamentos relacionados à privacidade e muitos países não promulgaram sua legislação nacional para cumprir com a diretiva ou anularam tal legislação, declarando-a inconstitucional.[36]

Em dezembro de 2013, o Advogado Geral do Tribunal Europeu de Justiça declarou que a Diretiva da Retenção de Dados é incompatível com a Carta dos Direitos Fundamentais.

Direito trabalhista

Menciona-se com frequência que a Internet está mudando a nossa forma de trabalhar. Enquanto tal fenômeno requer elaboração mais ampla, os aspectos a seguir tem relevância direta à governança da Internet:

- A Internet incorporou um grande volume de trabalhadores temporários. O termo *permtemp* foi cunhado para funcionários que são retidos por longos períodos por meio de contratos temporários reavaliados regularmente. Isto leva a um menor nível de proteção social para a mão de obra.
- O trabalho à distância está se tornando cada vez mais relevante com o maior desenvolvimento das telecomunicações, principalmente com o acesso à banda larga da Internet.
- A terceirização a outros países no setor de serviços de TIC, como centrais de atendimento e unidades de processamento de dados está aumentando. Uma quantidade considerável destas atividades já foi transferida a países de baixo custo, principalmente na Ásia e na América Latina.

As TIC confundiram a rotina normal de trabalho, lazer e sono (8+8+8 horas), principalmente em ambientes de trabalho de empresas multinacionais. Está cada vez mais difícil distinguir onde começa e onde termina o trabalho. Estas mudanças nos padrões de trabalho talvez demandem novas legislações trabalhistas, abordando questões como as horas de trabalho, a proteção de interesses trabalhistas e a remuneração.

36 Para obter um panorama mais detalhado das questões de retenção de dados na UE, consultar Comissão Europeia (2011) Evaluation report on the Data Retention Directive (Directive 2006/24/EC). Acessível em <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmeuleg/428-xxix/42816.htm> [acessado em 13 de fevereiro de 2014].

No campo do direito trabalhista, uma questão importante diz respeito à privacidade no local de trabalho. O empregador tem permissão para monitorar o uso da Internet por parte do empregado (por exemplo, conteúdo das mensagens de e-mail ou acesso a sítios web)? Precedentes estão gradualmente avançando nesta área, com a oferta de diferentes soluções.

Na França, em Portugal e na Grã-Bretanha, as diretrizes jurídicas e alguns casos tendem a restringir a vigilância sobre e-mails de funcionários.[37] O empregador deve enviar aviso prévio de quaisquer atividades de monitoramento. Na Dinamarca, os tribunais consideraram uma ação judicial envolvendo a demissão de um funcionário por enviar e-mails privados e acessar chats de encontros sexuais na Web. A justiça decidiu que a demissão era ilegal porque o empregador não tinha uma política de uso da Internet para proibir a utilização não oficial da Internet. Outro raciocínio adotado pela justiça dinamarquesa foi o fato de que o uso da Internet por parte do funcionário não afetou seu desempenho no trabalho.

Outra preocupação oriunda do crescente uso das redes sociais é a delimitação entre a vida privada e a vida profissional. Casos recentes[38] mostram que o comportamento e os comentários dos funcionários nas redes sociais podem abordar vários tópicos, desde o ambiente de trabalho e colegas até estratégias e produtos do empregador, considerados opiniões pessoais (e privadas), mas que podem afetar consideravelmente a imagem e a reputação de empresas e colegas.

O direito trabalhista tradicionalmente é uma questão nacional. No entanto, a globalização em geral e a Internet em particular resultaram na internacionalização das leis trabalhistas. Com um número cada vez maior de pessoas trabalhando para empresas estrangeiras e interagindo com equipes de trabalho ao redor do mundo, há a necessidade crescente de mecanismos regulatórios internacionais adequados. Este aspecto foi reconhecido na declaração da CMSI, que no pará-

37 The Register (2007) EU court rules monitoring of employee breached human rights. 5 de abril. Acessível em <http://www.theregister.co.uk/2007/04/05/monitoring_breached_human_rights> [acessado em 13 de fevereiro de 2014].

38 Ver os seguintes artigos como exemplos: Holding R (2011) Can You Be Fired for Bad- Mouthing Your Boss on Facebook? Time U.S. Acessível em <http://content.time.com/time/nation/article/0,8599,2055927,00.html> [acessado em 13 de fevereiro de 2014]. Broughton A et al. (2009) Workplaces and Social Networking. The Implications for Employment Relations, Acas. Acessível em <http://www.acas.org.uk/media/pdf/d/6/1111_Workplaces_and_Social_Networking.pdf> [acessado em 13 de fevereiro de 2014].

grafo 47 solicita o cumprimento de todas as normas internacionais relevantes no mercado de trabalho das TIC.

Privacidade e proteção de dados[39]

A privacidade e a proteção de dados são duas questões de governança da Internet interligadas. A proteção de dados é um mecanismo jurídico que garante a privacidade. Porém, o que é privacidade? Costuma ser definida como o direito do cidadão de controlar suas próprias informações pessoais e decidir sobre elas (divulgar informações ou não). A privacidade é um direito humano fundamental. É reconhecida na Declaração Universal dos Direitos Humanos,[40] e no Pacto Internacional sobre Direitos Civis e Políticos[41] e em muitas outras convenções de direitos humanos internacionais e regionais.

Culturas nacionais e o estilo de vida influenciam a prática da privacidade. Embora esta questão seja importante nas sociedades ocidentais, talvez tenha menos importância em outras culturas. As práticas modernas de privacidade concentram-se na privacidade da comunicação (para que não haja vigilância da comunicação) e na privacidade da informação (para que não haja tratamento da informação sobre pessoas). As questões sobre privacidade, que costumavam focar em atividades governamentais, foram ampliadas e agora incluem o setor empresarial.[42]

Questões

As principais questões de privacidade são analisadas em triangulação entre pessoas, Estados e empresas, conforme apresentado na próxima figura.

Pessoas e Estados

A informação sempre foi uma ferramenta essencial para os Estados exercerem sua autoridade sobre territórios e populações. Os governos coletam grandes quantidades de informações pessoais (certidões de nascimento e casamento, números de previdência social, título de eleitor, antecedentes criminais, informações sobre impostos,

39 Comentários e contribuições valiosos foram dados por Katitza Rodriguez.

40 ONU (sem data) Universal Declaration of Human Rights. Acessível em <http://www.un.org/en/universal-declaration-human-rights/index.html> [acessado em 13 de fevereiro de 2014].

41 ACNUR (sem data) International Covenant on Civil and Political Rights. Acessível em <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> [acessado em 27 de março de 2014].

42 Relatório da União Americana Pelas Liberdades Civis (American Civil Liberties Union): Stanley J (2004). The surveillance-industrial complex: How the American government is conscripting businesses and individuals in the construction of a surveillance society. Este relatório explica o problema da privatização da vigilância e os novos desafios ligados à proteção da privacidade. Acessível em <https://www.aclu.org/files/FilesPDFs/surveillance_report.pdf> [acessado em 13 de fevereiro de 2014].

documentos referentes a imóveis, carro, patrimônio etc). A pessoa não pode escolher não apresentar dados pessoais antes de imigrar para outro país, no qual enfrentaria o mesmo problema. A tecnologia da informação, como a usada em prospecção de dados,[43] auxilia na agregação e correlação de dados de muitos sistemas especializados (ex., tributação, documentos referentes à imóveis, propriedade de veículos etc.) para realizar análises elaboradas, buscando por padrões comuns e incomuns e inconsistências. Um dos principais desafios das iniciativas do governo eletrônico é garantir o equilíbrio adequado entre a modernização das funções do governo e a garantia dos direitos privados dos cidadãos, incluindo limitar a coleta de informações ao que é estritamente necessário para o desempenho das funções do governo ou do serviço público. No entanto, os anos recentes testemunharam o apetite crescente do governo por coleta de informações e a associação de mais dados pessoais para identificação obrigatória (como dados biométricos).

Após os acontecimentos de 11 de setembro de 2001 nos Estados Unidos, a Lei Patriota (Patriot Act) dos Estados Unidos[44] e legislações comparáveis em outros países ampliaram a autoridade dos governos para coletar informações, inclusive a disposição para a intercepção legal de informações. O conceito de intercepção legal para coletar provas também é contemplado pela Convenção sobre Crime Cibernético[45] (Artigos 20 e 21). Ademais, a UE solicitou a adoção de legislação nacional permitindo a retenção de dados necessários para identificar o usuário durante um período de seis a 24 meses.

Proteção da privacidade: pessoas e empresas

Conforme ilustrado na imagem da triangulação da privacidade, a segunda e cada vez mais importante relação é aquela entre indivíduos e o setor empresarial. Determinada pessoa divulga dados pessoais ao abrir uma conta no banco, reservar um voo ou um quarto de hotel, realizar pagamentos online com o cartão de crédito ou até mesmo navegando e pesquisando na Internet. Inúmeros rastros de dados costumam ser deixados nestas atividades.

43 UCLA (sem data) What is data mining? Acessível em <http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm> [acessado em 17 de fevereiro de 2014].

44 Epic.org (sem data) US Patriot Act. Acessível em <http://epic.org/privacy/terrorism/hr3162.html> [acessado em 13 de fevereiro de 2014].

45 Conselho da Europa (2001) Convention on Cybercrime. Acessível em <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> [acessado em 13 de fevereiro de 2014].

O êxito e a sustentabilidade do comércio eletrônico, tanto no relacionamento empresa-cliente quanto no relacionamento empresa-empresa, depende do estabelecimento da ampla confiança tanto nas políticas de privacidade empresarial e das medidas de segurança que estabelecem para proteger as informações confidenciais dos clientes de roubos e desvios.[46] Com a expansão das plataformas de redes sociais (ex., Facebook, Twitter), surgem preocupações sobre o possível uso indevido de dados pessoais – não somente pelo proprietário ou administrador da plataforma de rede social, mas também por outras pessoas participando delas.[47]

Na economia da informação, os dados sobre clientes, inclusive suas preferências e perfis de compra, se tornam um importante bem de mercado. Para algumas empresas, como o Facebook, o Google e a Amazon, informações sobre as preferências dos clientes constituem um dos pilares do seu modelo de negócios. Basicamente, os dados pessoais dos indivíduos constituem a moeda com a qual "pagam" serviços gratuitos tanto na forma de um navegador cookie indicando o comportamento específico do cliente quanto uma informação específica solicitada no preenchimento de um formulário na Web ou na realização de um pagamento. E com o valor crescente de informações que os usuários revelam sobre si mesmos, as violações da privacidade são frequentes e proporcionalmente sofisticadas.[48]

Proteção da privacidade: Estados e empresas

O terceiro lado da triangulação da privacidade é o menos divulgado,

46 TRUSTe, a organização que desenvolveu um selo de privacidade para garantir o cumprimento de sítios web com as exigências de privacidade, também monitora a confiança do consumidor online: TRUSTe Launches New Privacy Index Measuring Consumer Privacy Insights and Trends. São Francisco, Califórnia, 13 de fevereiro de 2012. Acessível em <http://www.truste.com/about-TRUSTe/press-room/news_truste_launches_new_trend_privacy_index> [acessado em 13 de fevereiro de 2013].

47 O foco na privacidade e a preocupação relacionada a sítio webde redes sociais são muito bem exemplificados no monitoramento atento e na pressão exercida pelos defensores dos direitos civis da mídia no Facebook. Para obter um panorama da diversidade das questões sobre privacidade levantadas com relação à utilização desta plataforma, ver: Wikipedia (2012) Criticism of Facebook. Acessível em <http://en.wikipedia.org/wiki/Criticism_of_Facebook> [acessado em 13 Facebook 2013].

48 Para obter um panorama das maiores violações à privacidade ao longo do tempo (mas com foco nos EUA) ver Marsan C (2012) 15 worst Internet privacy scandals of all time. Network World 26 de janeiro. Acessível em <http://www.networkworld.com/news/2012/012612-privacy- scandals-255357.html?page=1> [acessado em 13 de fevereiro de 2014]. Nota do Tradutor: o primeiro endereço foi substituído por <http://www.networkworld.com/article/2185187/security/15-worst-internet-privacy-scandals-of-all-time.html> [acessado em 7 de março de 2017].

mas talvez a questão de privacidade mais significativa. Tanto Estados quanto empresas coletam quantidades consideráveis de dados sobre pessoas. Alguns destes dados são compartilhados com outros Estados e empresas para impedir atividades terroristas. No entanto, em algumas situações, como as aplicadas pela Diretiva Europeia sobre Proteção de Dados, o Estado supervisiona e protege os dados de pessoas detidos por empresas.

Proteção da privacidade: pessoas e pessoas

O último aspecto da proteção da privacidade, não representado na triangulação da privacidade, é o possível risco à privacidade por parte das pessoas. Atualmente, qualquer pessoa com recursos suficientes pode ter poderosas ferramentas de vigilância. Até mesmo um celular simples equipado com câmera pode ser tal ferramenta. A tecnologia "democratizou a vigilância", em citação ao *The Economist*.[49] Muitos níveis da invasão da privacidade surgiram, do simples voyeurismo até a utilização sofisticada de câmaras para gravar números de cartões em bancos e para a espionagem econômica.

O principal problema para este tipo de violação da privacidade é que a maioria das legislações priorizam os riscos da privacidade advindos do Estado. Frente a esta nova realidade, alguns governos tomaram algumas medidas iniciais. O Congresso dos EUA adotou a Lei de Prevenção do Voyeurismo de Vídeo,[50] proibindo tirar fotos de pessoas sem roupas sem a sua permissão. A Alemanha e alguns outros países adotaram leis de privacidade similares, evitando a vigilância individual.

A regulação internacional da privacidade e proteção de dados

Um dos principais instrumentos internacionais de privacidade e proteção de dados é a Convenção do Conselho da Europa para a Proteção dos Indivíduos com respeito ao Processamento Automático de Dados Pessoais[51] de 1981. Apesar de ter sido adotada pela organização regional (CoE), pode ser aderida por países não europeus. Como a convenção é neutra em termos tecnológicos, ela resistiu ao tempo.

49 The Economist (2004) Move over, Big Brother. 2 de dezembro. Acessível em <http://www.economist.com/node/3422918> [acessado em 13 de fevereiro de 2014].

50 Gov.track.us (sem data) Video Voyeurism Prevention Act. Acessível em <http://www.govtrack.us/congress/bills/108/s1301> [acessado em 13 de fevereiro de 2014].

51 Conselho da Europa (sem data) Convention for the protection of individual with regard to automatic processing of personal data. Acessível em <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> [acessado em 13 de fevereiro de 2014].

A Diretiva de Proteção de Dados da UE[52] (Diretiva 45/46/EC) também elaborou um quadro legislativo importante para o processamento de dados pessoais na UE e tem amplo impacto no desenvolvimento de legislação nacional não somente na Europa mas também em nível global. Esta regulação também implementou um processo de reforma para lidar com os novos desenvolvimentos e garantir a efetiva proteção de dados no atual ambiente tecnológico.[53]

Outro documento internacional fundamental – não vinculativo – sobre privacidade e proteção de dados é o documento da OCDE, Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais[54] de 1980. Estas diretrizes e o trabalho subsequente da OCDE serviram de inspiração para inúmeros documentos internacionais, regionais e nacionais sobre privacidade e proteção de dados. Hoje, praticamente todos os países da OCDE promulgaram leis e concederam competência a autoridades para executar estas leis.

Embora os princípios das diretrizes da OCDE tenham sido amplamente aceitos, a principal diferença está na forma de implementação, notavelmente entre as abordagens da Europa e dos Estados Unidos. Enquanto na Europa existe uma legislação abrangente para a proteção de dados, nos Estados Unidos a regulação da privacidade é elaborada de acordo com cada setor da economia, entre as quais a privacidade nas finanças (o *Graham- Leach-Bliley Act*),[55] privacidade das crianças (o *Children's Online Privacy Protection Act*)[56] e privacidade nos serviços médicos (de acordo com o *Health Insurance Portability and Accountability Act*).[57]

52 Europa (sem data) Protection of personal data. Acessível em <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l14012 > [acessado em 11 de abril de 2012]

53 Mais informações sobre o processo de reforma podem ser acessadas em <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l14012> [acessado em 13 de fevereiro de 2014].

54 OCDE (1980) Guidelines on the Protection of Privacy and TransborderFlow Flows of Personal Data. Acessível em <http://www.oecd.org/internet/ieconomypoecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> [acessado em 13 de fevereiro de 2014]. Nota do Tradutor: o primeiro endereço foi substituído por <http://www.oecd.org/sti/ieconomy/uidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> [acessado em 7 de março de 2017].

55 Graham-Keach-Bliley Act. Acessível em <http://www.ftc.gov/privacy/glbact/glbsub1.htm> [acessado em 13 de fevereiro de 2014].

56 Children's Online Privacy Protection Act. Acessível em <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule> [acessado em 13 de fevereiro de 2014].

57 Health Information Privacy. Acessível em <http://www.hhs.gov/ocr/privacy/> [acessado em 13 de fevereiro de 2014].

Outra diferença significativa é que, na Europa, a legislação da privacidade é executada pelas autoridades públicas, ao passo que nos Estados Unidos sua execução é realizada principalmente pelo setor privado e pela autorregulação. As empresas estabelecem políticas de privacidade, sendo que cabe a elas e aos indivíduos decidir por contra própria sobre as políticas de privacidade. A principal crítica à abordagem dos EUA é que as pessoas são colocadas em uma posição relativamente vulnerável, uma vez que raramente sabem da importância das opções oferecidas pelas políticas de privacidade e geralmente concordam com tais políticas sem se informarem a seu respeito.

Acordo Safe Harbor entre os EUA e a UE

Estas duas abordagens – a dos EUA e a da UE – da proteção de privacidade começaram a entrar em conflito. O principal problema advém da utilização de dados pessoais pelas empresas comerciais. De que forma a UE pode garantir que dados sobre os cidadãos estejam protegidos de acordo com as regras especificadas em sua Diretiva para Proteção de Dados? De acordo com quais regras (a da UE ou a dos EUA) os dados são transferidos através de uma rede da empresa da UE para os EUA? A UE ameaçou bloquear a transferência dos dados a qualquer país que não fosse capaz de garantir o mesmo nível de proteção de privacidade conforme disposto em sua diretiva. Este requisito inevitavelmente confrontou com a abordagem dos EUA de autorregulação da proteção da privacidade.

Esta profunda diferença fez com que qualquer acordo possível se tornasse mais difícil de alcançar. Ademais, a adaptação da lei dos EUA à lei de proteção de dados da UE não seria possível porque exigiria a alteração de alguns princípios importantes do sistema jurídico dos EUA. A solução para o impasse ocorreu quando o Embaixador Aaron sugeriu em 1998 a fórmula safe harbour (porto seguro). Isto reestruturou toda a questão e ofereceu uma solução para o impasse nas negociações.

Na solução apresentada, as regulações da UE podiam ser aplicadas às empresas dos EUA dentro de um safe harbour jurídico. As empresas norte-americanas que administravam os dados de cidadãos da UE poderiam voluntariamente se cadastrar para observar as exigências de proteção da privacidade da UE. Ao fazerem isso, as empresas deveriam observar os mecanismos de cumprimento formais acordados entre a UE e os EUA.

Quando foi assinado em 2000, o Acordo Safe Harbor foi recebido

com grande esperança como o instrumento jurídico que conseguiria solucionar problemas similares com outros países. No entanto, o histórico não é muito promissor. Ele foi criticada pelo Parlamento Europeu por não proteger de forma suficiente a privacidade dos cidadãos europeus. As empresas dos EUA não ficaram particularmente entusiasmadas com a utilização desta abordagem. De acordo com um estudo realizado pela Galexia, de 1597 empresas registradas no Acordo Safe Harbor, apenas 348 atendiam aos requisitos básicos (ex., política de privacidade).[58] Dada a alta relevância da privacidade e da proteção de dados nas relações entre os EUA e a UE após as revelações de Snowden, provavelmente é de se esperar forte pressão para que se encontre uma solução para o disfuncional Acordo Safe Harbour. Em seu discurso sobre políticas no Parlamento Europeu, Jean-Claude Juncker, presidente recém-eleito da Comissão Europeia, mencionou um acordo de "porto seguro" como uma possibilidade para solucionar os problemas de proteção de dados entre a União Europeia e os Estados Unidos.

58 Connolly C (2008) The US Safe Harbor – Fact or Fiction? Galexia. Acessível em <http://www.galexia.com/public/research/articles/research_articles-pa08.html> [acessado em 13 de fevereiro de 2014].

Cesta econômica

Sabemos rotear pacotes.
O que não sabemos é como rotear dólares.
David Clark

Esta citação de David Clark, arquiteto-chefe de protocolos da Internet, expressava o espírito do início da comunidade da Internet, no qual o projeto sem fins lucrativos da Internet era financiado principalmente pelas bolsas de pesquisa dos EUA. Mas nos anos 90 e início dos anos 2000, novos modelos de negócios para "rotear dólares" começaram a surgir no Vale do Silício, priorizando a receita advinda de publicidade.

As questões econômicas da governança da Internet estão principalmente relacionadas a esta evolução da Internet como projeto sem fins lucrativos para um dos principais negócios e motores do crescimento econômico da sociedade moderna. O fluxo de ideias e criatividade dos primórdios da Internet foi complementado pelo fluxo de dinheiro, sendo que cada vez mais a Internet se encontra competindo por dinheiro. Mais dinheiro resultou em negócios mais tangíveis e interesses em políticas. A criativa abordagem "o céu é o limite" da incipiente comunidade da Internet começou a convergir com a lógica da "lucratividade" da comunidade de negócios.

A prática econômica da Internet é, atualmente, considerada eficiente, devido ao seu bom funcionamento e, no geral, a seu custo acessível. A principal crítica à atual economia da Internet é o risco do monopólio das principais empresas de Internet e telecoms que poderia levar à distorção do mercado.

Nguyen and Armitrage argumentam que a Internet deveria equilibrar de forma ótima e ideal três elementos: eficiência técnica, eficiência econômica e efeitos sociais.[1] Outros autores apontam os desafios de substituir a estrutura existente fixa e de preços simples por uma mais complexa, como a contabilidade baseada no tráfego de pacotes.[2] Com relação às mudanças práticas, alguns acreditam que mudar as atuais

1 Thuy T, Nguyen T, Armitage GJ (2005) Evaluating Internet Pricing Schemes: A Three Dimensional Visual Model. ETRI Journal 27(1) pp. 64-74. Acessível em <http://etrij.etri.re.kr/etrij/journal/article/article.do?volume=27&issue=&page=64?> [acessado em 13 de fevereiro de 2014].

2 Hayel Y, Maille P, Tuffin B (2005) Modelling and analysis of Internet Pricing: introduction and challenges in Proceedings of the International Symposium on Applied Models and Data Analysis (ASMDA), Brest, França. Acessível em <http://conferences.telecom-bretagne.eu/asmda2005/IMG/pdf/proceedings/1389.pdf> [acessado em 13 de fevereiro de 2014].

políticas econômicas da Internet poderia abrir uma caixa de Pandora. A questão principal da análise da governança é que ela costuma ser uma análise sobre o fluxo do dinheiro. [3] A resposta a esta simples questão de quem paga pela Internet é complexa. Uma série de transações monetárias e não monetárias acontecem entre várias partes envolvidas com a Internet. Iremos abordá-las no âmbito de quatro domínios:

- Comércio eletrônico: atividades econômicas tradicionais conduzidas via Internet.
- Economia de CONTEÚDO da Internet: novo modelo de negócios baseado na publicidade.
-Economia de ACESSO da Internet: a indústria das telecomunicações na era da Internet.
- Pagamentos eletrônicos e moedas cibernéticas.

Além disso, iremos abordar as seguintes questões no âmbito das políticas de relevância econômica: proteção ao consumidor, tributação e assinaturas digitais.

Comércio eletrônico

O comércio eletrônico tem sido um dos principais motores de promoção do crescimento da Internet nos últimos 15 anos. A importância do comércio eletrônico é exemplificada pelo título do documento que iniciou a reforma da governança da Internet e estabeleceu a ICANN: O Framework for Global Electronic Commerce[4] de 1997, que estabelece que o "setor privado deveria liderar" o processo de governança da Internet e que a principal função desta governança será "implementar um ambiente jurídico para os negócios que seja previsível, minimalista, consistente e simples". Estes princípios são a fundação do regime de governança da Internet que tem como princípio a ICANN.

3 Andrew Odlyzko entende a questão dos preços e da arquitetura da Internet do ponto de vista histórico. Ao identificar a linha das políticas de preço a partir dos sistemas de transporte no mundo antigo, ele faz uma conexão com a atual política de preços da Internet. Para mais informações, consultar: Odlyzko A (2004) Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation. Acessível em <http://www.dtc.umn.edu/~odlyzko/doc/pricing.architecture.pdf> [acessado em 13 de fevereiro de 2014].

4 The White House (1997) Framework for Global Electronic Commerce. Acessível em <http://clinton4.nara.gov/WH/New/Commerce/> [acessado em 17 de fevereiro de 2014].

Definição

A escolha de uma definição para o comércio eletrônico tem muitas implicações práticas e jurídicas. Regras específicas são aplicadas dependendo da possibilidade de uma transação específica ser classificada como comércio eletrônico, como as que regulam a tributação e a alfândega.

Para o governo dos EUA, o principal elemento de distinção entre o comércio tradicional e o comércio eletrônico é o compromisso online de venda de bens e serviços. Isto significa que qualquer negociação comercial concluída online deveria ser considerada uma transação de comércio eletrônico, mesmo que a realização da negociação envolva a entrega física. Por exemplo, comprar um livro pela Amazon.com é considerado uma transação de comércio eletrônico, mesmo com o livro sendo frequentemente entregue via correio tradicional. A OMC define o comércio eletrônico com maior precisão: "a produção, distribuição, o marketing, a venda ou entrega de bens e serviços por meios eletrônicos".[5] A abordagem da UE para o comércio eletrônico trata dos "serviços da sociedade de informação" que cobrem "qualquer serviço normalmente prestado para obter remuneração, à distância, por meio de equipamento eletrônico para o processamento (inclusive a compressão digital) e armazenamento de dados, e mediante solicitação específica feita pelo beneficiário do serviço".[6]

O comércio eletrônico assume muitas formas:

- Venda para consumidores privados (Business-to-consumer - B2C) – o tipo mais comum de comércio eletrônico (ex., Amazon.com).
- Venda para outras empresas (Business-to-business - B2B) – economicamente o mais intenso, respondendo por mais de 90% de todas as transações de comércio eletrônico.[7]
- Venda para o governo (Business-to-government - B2G) – muito importante na área da política de compras.
- Venda entre consumidores privados (Consumer-to-consumer - C2C) – por exemplo, leilões do eBay.

5 OMC (1998) Work programme on electronic commerce. Acessível em <http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm> [acessado em 17 de fevereiro de 2014].

6 União Europeia [EU] (2000) Diretiva 2000/31/EC do Parlamento Europeu e do Conselho da Europa de 8 de junho de 2000 sobre determinados aspectos jurídicos dos serviços da sociedade de informação, mais especificamente o comércio eletrônico no Mercado Interno (Diretiva sobre comércio eletrônico). Acessível em <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031> [acessado em 17 de fevereiro de 2014].

7 Global Web Index. GlobalWebIndex e-Commerce Report: Online Plays a Role in 90% of Transactions. Acessível em <http://blog.globalwebindex.net/globalwebindex-e-commerce-report-online-plays-a-role-in-90-of-transactions/> [acessado em 10 de agosto de 2014].

Muitos países estão desenvolvendo um ambiente regulatório para o comércio eletrônico. Leis têm sido adotadas nos campos de assinatura digital, resolução de disputas, crimes cibernéticos, proteção ao consumidor e tributação. No nível internacional, há uma quantidade cada vez maior de iniciativas e regimes relacionados ao comércio eletrônico.

A OMC e o comércio eletrônico

Na qualidade de principal ator no âmbito das políticas referentes ao comércio global moderno, a OMC estabeleceu um sistema de acordos regulando o comércio internacional. Os principais tratados são o Acordo Geral sobre Pautas Aduaneiras e Comércio (GATT),[8] que lida com o comércio de bens, o Acordo Geral sobre o Comércio de Serviços (GATS) e o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio (TRIPS).[9] Dentro deste quadro, a OMC regula muitas questões importantes relacionadas ao comércio eletrônico, entre as quais a liberalização das telecomunicações, DPI e alguns aspectos do desenvolvimento das TIC. O comércio eletrônico está presente nas seguintes atividades e iniciativas da OMC:

- A moratória temporária sobre direitos aduaneiros de transações eletrônicas, implementada em 1998, fez com que todas as transações eletrônicas fosses globalmente isentas de tais direitos aduaneiros.
- A criação do Programa de Trabalho para o Comércio Eletrônico da OMC promove a discussão sobre o comércio eletrônico.[10]
- O mecanismo de resolução de disputas; o comércio eletrônico foi particularmente relevante no processo do Jogo Online Estados Unidos/Antígua.[11]

Embora o comércio eletrônico tenha ficado em segundo plano na esfera da diplomacia da OMC, várias iniciativas surgiram e uma série de questões importantes foram identificadas. Mencionaremos aqui duas destas questões.

8 OMC (sem data) GATT and the Goods Council. Acessível em <https://www.wto.org/english/tratop_e/gatt_e/gatt_e.htm> [acessado em 17 de fevereiro de 2014].

9 OMC (1994) Agreement on Trade-related Aspects of Intellectual Property Rights. Acessível em <http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm> [acessado em 17 de fevereiro de 2014].

10 Esta seção do sítio web da OMC foca o comércio eletrônico. Acessível em <https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm> [acessado em 17 de fevereiro de 2014].

11 Para mais informações sobre o Processo de Jogos Online envolvendo Estados Unidos Antígua, consultar <http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm> [acessado em 17 de fevereiro de 2014].

As transações do comércio eletrônico deveriam ser categorizadas em serviços (regulados pelo GATS) ou em bens (regulados pelo GATT)?

A categorização da música como um bem ou serviço muda de acordo com a forma que ela é entregue, CD (tangível) ou via Internet (intangível)? Por fim, uma mesma música poderia ter diferentes condições de negociação (e estar sujeita a diferentes direitos aduaneiros e impostos) dependendo da mídia de entrega. A questão da categorização apresenta implicações consideráveis, devido aos diferentes mecanismos regulatórios para bens e serviços.

Qual deveria ser a ligação entre o TRIPS e a proteção do DPI na Internet?

Como o acordo TRIPS da OMC oferece mecanismos de cumprimento muito mais fortes para o DPI, os países desenvolvidos vêm tentando estender a abrangência do TRIPS para o comércio eletrônico e para a Internet por meio de duas abordagens. Primeiramente, ao citar o princípio da "neutralidade tecnológica", eles argumentam que o TRIPS, assim como outras regras da OMC, deveria ser estendido a qualquer mídia de telecomunicações, inclusive a Internet. Em segundo lugar, alguns países desenvolvidos requisitaram uma integração mais estreita entre "tratados digitais" da OMPI e o sistema do TRIPS. O TRIPS oferece mecanismos de cumprimento mais fortes que as convenções da OMPI. Ambas as questões continuam abertas e se tornarão cada vez mais importantes em futuras negociações da OMPI. Durante a fase atual das negociações comerciais, é provável que o comércio eletrônico receba destaque na agenda da OMC. A ausência de acordos referentes ao comércio eletrônico global será parcialmente compensada por algumas iniciativas específicas (ex., relacionadas a contratos e assinaturas) e vários acordos regionais, principalmente na União Europeia e na região da Ásia-Pacífico.

Outras iniciativas do comércio eletrônico internacional

Uma das iniciativas internacionais mais bem sucedidas e amplamente apoiadas no campo do comércio eletrônico é a Lei Modelo sobre Arbitragem Comercial Internacional da Comissão das Nações Unidas[12] sobre Direito do Comércio Internacional[13] (CNUDCI). A prioridade

12 Sítio web da CNUDCI. Acessível em <http://www.uncitral.org/uncitral/index.html> [acessado em 17 de fevereiro de 2014

13 CNUDCI (1996) Model Law on Electronic Commerce. Acessível em <http://www.uncitralorg/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html> [acessado em 17 de fevereiro de 2014].

da Lei Modelo são os mecanismos para integração entre o comércio eletrônico e o direito comercial tradicional (ex., reconhecimento da validade dos documentos eletrônicos). A Lei Modelo tem sido utilizada como base para a regulação do comércio eletrônico em diversos países. Outra iniciativa concebida para desenvolver o comércio eletrônico é a implementação do e-business XML (ebXML)[14] pelo Centro para Facilitação do Comércio e Negócios Eletrônicos das Nações Unidas (ONU/CEFACT), que é um conjunto de padrões baseados na tecnologia XML. Embora tais padrões ainda estejam desenvolvendo novas versões e o conjunto anterior – o Intercâmbio Eletrônico de Dados (Electronic Data Interchange - EDI) ainda seja largamente utilizado, resta saber se eles serão ajustados e de que forma isso será feito para lidar com novas tendências e desenvolvimentos tecnológicos.[15]

As atividades da OCDE tratam de diversos aspectos relacionados ao comércio eletrônico, entre os quais a proteção ao consumidor e as assinaturas digitais. A OCDE enfatiza a promoção e a pesquisa relacionadas ao comércio eletrônico por meio de suas recomendações e diretrizes. A UNCTAD é especialmente ativa nos campos de pesquisa e construção de capacidades, com foco na relevância do comércio eletrônico para o desenvolvimento. Todo ano ela monitora a evolução da economia da informação em um relatório que avalia o papel das novas tecnologias na esfera do comércio e desenvolvimento.[16] No setor de negócios, as organizações internacionais mais ativas são a Câmara Internacional do Comércio,[17] que formula diversas recomendações e análises no campo do comércio eletrônico; e o Global Business Dialogue,[18] que promove o comércio eletrônico tanto no contexto internacional quanto no nacional.

14 Sítio web da ebXML. Acessível em <http://www.ebxml.org/> [acessado em 17 de fevereiro de 2014].

15 Ver por exemplo a discussão sobre a relevância do padrão ebXML hoje. Acessível em <http://www.infoq.com/news/2012/01/ebxml> [acessado em 17 de fevereiro de 2014].

16 UNCTAD (sem data) Economic reports. Acessível em <http://unctad.org/en/Pages/Publications/InformationEconomyReportSeries.aspx> [acessado em 17 de fevereiro de 2014].

17 Sítio web da Câmara de Comércio Internacional. Acessível em <http://www.iccwbo.org/> [acessado em 17 de fevereiro de 2014].

18 Sítio web do The Global Business Dialogue. Acessível em <http://www.gbdinc.org/> [acessado em 17 de fevereiro de 2014].

Iniciativas regionais

A UE desenvolveu uma estratégia para o comércio eletrônico na chamada Cúpula Dot Com em Lisboa (março de 2000). Apesar de ter adotado uma abordagem voltada para o segmento privado e para o mercado do comércio eletrônico, UE também implementou algumas medidas corretivas para proteger interesses públicos e sociais (a promoção do acesso universal, políticas de concorrência que consideram o interesse público, e a restrição da distribuição de conteúdo nocivo). A EU adotou a Diretiva sobre Comércio Eletrônico,[19] bem como um conjunto de outras diretivas relacionadas a assinaturas eletrônicas, proteção de dados e transações financeiras eletrônicas.

Na região da Ásia-Pacífico, o ponto focal da cooperação do comércio eletrônico é a Cooperação Econômica Ásia-Pacífico (APEC). A APEC formou o Comitê Diretor para o Comércio Eletrônico, que trata de várias questões referentes ao comércio eletrônico, entre as quais a proteção ao consumidor, a proteção de dados, spam e cibersegurança. A iniciativa mais proeminente é a Ação Individual para o Comércio Sem Papel (Paperless Trading Individual Action)[20] da APEC, cujo objetivo é criar sistemas sem papel para o comércio transnacional.

Economia do CONTEÚDO da Internet

O novo modelo de negócios da indústria da Internet, desenvolvido principalmente pelas empresas localizadas no Vale do Silício, começou a surgir no final dos anos 90 e tomou forma completa na década iniciada em 2010. O crescimento da Internet nos anos 90 não podia ser sustentado pelo financiamento público da mesma forma que antes; necessitava de um modelo de negócios mais robusto. Algumas tentativas de cobrar pelo acesso aos serviços e conteúdo da Internet fracassaram. O novo modelo de negócios da Internet não cobra seus usuários pela utilização dos serviços da Internet; ele gera receitas a partir da publicidade sofisticada.

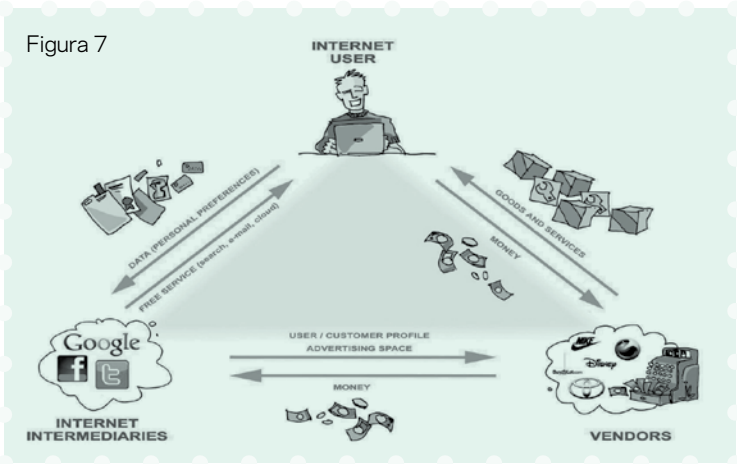
Os usuários "pagam" pelos serviços prestados com seus dados, inclusive informações que geram – suas "pegadas eletrônicas" – ao fazerem buscas e interagir na Internet. As empresas de Internet analisam os dados do usuário para extrair informações sobre suas preferências,

19 Comissão Europeia (sem data) E-commerce directive. Acessível em <http://ec.europa.euinternal_market/e-commerce/directive_en.htm> [acessado em 17 de fevereiro de 2014].

20 APEC (sem data) Paperless Trading Individual Action Plan. Acessível em <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Paperless-Trading-Individual-Action-Plan.aspx> [acessado em 17 de fevereiro de 2014].

gostos e hábitos. Elas também exploram os dados para extrair informações sobre determinado grupo; por exemplo, o comportamento de adolescentes em uma cidade ou região específica. Estas empresas de Internet conseguem prever com alto grau de certeza o que uma pessoa com determinado tipo de perfil irá comprar ou fazer. Este valioso bloco de dados sobre os usuários da Internet tem diversos usos comerciais, sendo que um dos principais usos é sua compra por parte de fornecedores que os utilizam para suas atividades de marketing. Por exemplo, em 2013, 90% da receita anual do Google no valor de US$ 55,5 bilhões veio da publicidade e serviços correspondentes.[21]

Figura 7



Questões

Proteção aos usuários e transparência

Formalmente, ao clicar em "Concordo" em contratos normalmente longos e de letra pequena, o usuário aceita as condições dos serviços. Permanece a questão de saber se os usuários decidem de forma esclarecida, principalmente diante da possível utilização de seus dados para fins comerciais. É bem provável que, em muitos casos, os usuários aceitem a "oferta" de trocar seus dados por valiosos serviços de Internet. Quanto mais transparente e fácil de compreender forem os acordos da Internet, mais benefícios existirão tanto para os usuários quanto para as empresas de Internet que poderão garantir um modelo de negócios mais sustentável.

21 Google (sem data) Investor relations. Acessível em <http://investor.google.com/financialtables.html> [acessado em 10 de agosto de 2014].

Risco de monopólios de mercado

A natureza da indústria da Internet tende a criar monopólios de mercado (ex., a participação do Google nas buscas da Internet supera 80% na Europa). Ademais, não existem regimes globais antimonopólio que poderão lidar com o potencial monopólio do mercado global da indústria da Internet. Huston argumenta que a criação de monopólios e a perda de um mercado diversificado de recursos da Internet inevitavelmente afetaria o preço e a qualidade dos serviços da Internet.[22] Atualmente, a União Europeia é quem mais fortemente atua a favor do antimonopólio globalmente. Com um mercado de 500 milhões de pessoas, a UE pode obrigar as empresas de Internet a seguirem suas regulações de mercado e prevenir práticas monopolísticas. A União Europeia iniciou uma ação antimonopólio contra o Google, priorizando – entre outras questões – o posicionamento de publicidade paga na lista dos resultados de busca. Outros países com mercados de Internet menores e menos alavancagem de políticas provavelmente seguirão o acordo negociado entre a UE e as empresas de Internet.

Economia do ACESSO à Internet

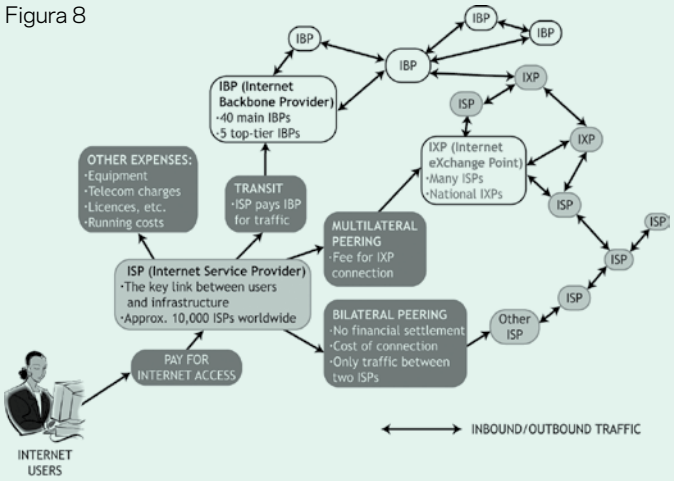
Os usuários e as empresas de Internet pagam os ISPs pelo acesso e serviços da Internet Normalmente, os ISPs têm que cobrir as seguintes despesas com as taxas recolhidas:

- Custo de despesas de telecomunicação e de largura de banda de Internet ao principal hub de Internet mais próximo.
- Custo do endereço IP obtido de registros regionais da Internet (RIRs) ou de registros locais da Internet (LIRs). O endereço IP é necessário para o dispositivo de acesso à Internet.
- Custo de equipamentos, software e manutenção de suas instalações.

Cada vez mais, o negócio de ACESSO da Internet é dificultado pelas exigências regulatórias dos governos, como a retenção de dados. Mais regulação demanda mais despesas, que poderiam ser repassadas aos usuários da Internet por meio de assinatura ou absorvidas reduzindo os lucros dos ISPs.

22 Huston G (2005) Where's the Money? – Internet Interconnection and Financial Settlements. The ISP Column. Acessível em <http://www.potaroo.net/ispcol/2005-01/interconn.pdf> [acessado em 13 de fevereiro de 2014].

Figura 8



Questões

Redistribuição de receitas entre empresas de telecomunicação e de Internet

As operadoras de telecomunicações estão levantando a questão da redistribuição das receitas geradas pela Internet. Elas buscam aumentar sua participação no "bolo das receitas" geradas pela rápida expansão da Internet. Até o momento, os principais beneficiários desta rápida expansão da Internet são as empresas de conteúdo da rede, devido ao seu modelo de negócios inovador baseado na publicidade online. O principal argumento das empresas de telecomunicações é que elas facilitam o acesso à Internet por meio de seus cabos e infraestrutura de telecomunicações.

A indústria de telecomunicações costuma justificar a exigência por maiores receitas advindas da Internet argumentando sobre a necessidade de investir na atualização da infraestrutura de telecomunicações. As empresas de conteúdo, por outro lado, argumentam que os provedores de acesso já cobram o usuário final pelo acesso à Internet, e que o principal motivo de seus alegados baixos rendimentos são seus modelos obsoletos de negócios (taxas "de uso ilimitado", como os preços fixos). As operadoras europeias de telecomunicações, organizadas na Associação das Operadoras de Redes de Telecomunicações Europeias (European Telecommunications Network Operators - ETNO), criou muitas polêmicas durante os

preparativos para a CMTI-12 em Dubai, ao fazer uma proposta concreta que alteraria o atual modelo de receitas, propondo que os provedores de conteúdo (ex., Facebook, Google) pagassem pelo acesso a seus serviços.

A proposta não obteve apoio nos preparativos para a CMTI-12, mas esta questão provavelmente continuará aberta nas futuras negociações sobre a governança da Internet. Esta discussão sobre a redistribuição das receitas de Internet constitui uma base sólida para o debate da neutralidade da rede – por exemplo, o tráfego da Internet deveria estar todo numa mesma categoria, como é hoje, ou deveria ser segregado em diferente(s) Internet(s) dependendo da qualidade dos serviços, do pagamento, e da confiabilidade (ex., ter uma variedade de Internets, desde a Internet VIP até a Internet para os pobres).

Compartilhamento de telecomunicações com países em desenvolvimento

Muitos países em desenvolvimento reclamam das condições econômicas desfavoráveis da economia da Internet. Comparado ao tradicional sistema de telefonia, no qual o preço de cada chamada internacional é compartilhado entre dois países, o modelo da Internet atribui todo o ônus a somente um dos lados – países em desenvolvimento que têm que financiar a conexão aos backbones da Internet principalmente nos países desenvolvidos. Como resultado, paradoxalmente, os países pequenos e pobres talvez no fim acabem subsidiando a Internet nos países desenvolvidos.

O problema do acordo financeiro é especialmente relevante para os países mais pobres, que dependem das receitas advindas das telecomunicações internacionais como importante fonte orçamentária. A situação se complicou ainda mais com a introdução do protocolo de voz (VoIP) – a telefonia da Internet – que transfere o tráfego de telefones dos operadores nacionais de telecomunicações para a Internet. Os países em desenvolvimento levantaram a questão sobre modelos de negócios mais justos para acessar a Internet durante a CMSI, os grupos de trabalho da UIT e, mais recentemente, na CMTI-12 em Dubai.

Banco eletrônico, dinheiro eletrônico e moedas virtuais

O dinheiro digital é uma ameaça para todos os governos deste planeta que queiram administrar sua própria moeda.
David Saxton[23]

O banco eletrônico envolve a utilização da Internet para conduzir operações bancárias convencionais, como o pagamento de cartão e a transferência de recursos. A novidade está somente no meio utilizado; o serviço bancário é essencialmente o mesmo. O banco eletrônico oferece vantagens ao cliente ao implementar novos serviços e reduzir os custos das transações. Por exemplo, estima-se que as transações do cliente, que custam US$ 4,00 no banco tradicional, custa somente US$ 0,17 no banco eletrônico.[24]

O dinheiro eletrônico é definido pelo Banco de Compensações Internacionais (Bank for International Settlements - BIS) como "valor armazenado ou mecanismos de pagamento pré-pago para a execução de pagamentos via terminais de ponto de venda, transferências diretas entre dois dispositivos ou até mesmo por meio de redes de computadores abertas como a Internet".[25] O dinheiro eletrônico costuma ser associado aos chamados smart cards emitidos por empresas como a Mondex e a Visa Cash e é ancorado no sistema monetário e bancário existente (com valor de moeda corrente).

Diferentemente do dinheiro eletrônico, as moedas virtuais não fazem parte do sistema financeiro nacional. A emissão de moedas virtuais seria equivalente a imprimir dinheiro sem o controle de uma instituição bancária central. O Bitcoin é a moeda virtual mais conhecida, também descrita como criptomoeda, pois é criada por um processo específico que tem como base a criptografia.[26]

---

23 Conforme citação em Holland K e Cortese A (1995) The future of money: e-cash could transform the world's financial life. Acessível em <http://www.businessweek.com/1995/24/ b3428001.htm> [acessado em 17 de fevereiro de 2014]. Nota do Tradutor: o endereço foi substituído por <https://www.bloomberg.com/news/articles/1995-06-11/the-future-of-money> [acessado em 6 de março de 2017].

24 Conforme citação em Olson T (2012) Higher costs, new laws mean no more free rides on some bank services, accounts. Pittsburgh Tribune-Review, 1o de abril. Acessível em <http://www. pittsburghlive.com/x/pittsburghtrib/business/s_789300.html> [acessado em 17 de fevereiro de 2014].

25 Comitê da Basiléia de Supervisão Bancária (1998) Risk Management for Electronic Banking and Electronic Money Activities. Basileia, março de 1998. Acessível em <http://www.bis.org/publ/ bcbs35.pdf> [acessado em 17 de fevereiro de 2014]. Versão final publicada em 2003 e acessível em <http://www.bis.org/publ/bcbs98.htm> [acessado em 17 de fevereiro de 2014]

26 Kamberi A (2014) Cryptocurrencies and bitcoin. Acessível em <http://www.diplomacy.edu/blog/cryptocurrencies-and-bitcoin> [acessado em 10 de agosto de 2014]

Questões

Mudanças no sistema bancário mundial

A utilização mais intensa tanto do banco eletrônico quanto do dinheiro eletrônico poderia resultar em mudanças no sistema bancário mundial, oferecendo ao cliente mais possibilidades e simultaneamente reduzindo os encargos bancários. Os métodos bancários tradicionais serão seriamente desafiados pelos bancos eletrônicos mais eficientes.[27] É importante observar que muitos bancos tradicionais já adotam o banco eletrônico. Em 2002, havia apenas 30 bancos eletrônicos nos Estados Unidos. Hoje em dia, é difícil encontrar um banco sem serviços eletrônicos.

COMÉRCIO LETRÔNICO POR MEIO DE PLATAFORMA MÓVEL

Os pagamentos eletrônicos e o dinheiro eletrônico passam por mudanças rápidas, no mesmo ritmo com que a tecnologia e os dispositivos evoluem e são desenvolvidos. Os pagamentos móveis já superaram os comandos inseridos via SMS do início, na medida em que o celular se tornou mais sofisticado e "inteligente" (ex., smartphones e iPhones) possibilitando a diversidade de aplicativos, entre os quais o comércio móvel.[28]

VER A SEÇÃO 2 PARA UMA DISCUSSÃO MAIS APROFUNDADA SOBRE CIBERSEGURANÇA

Cibersegurança

A cibersegurança é um dos principais desafios à utilização mais ampla dos pagamentos eletrônicos. De que forma a segurança das transações financeiras via Internet pode ser garantida? A cibersegurança já foi discutida. Neste ponto, é importante enfatizar a responsabilidade dos bancos e de outras instituições financeiras pela segurança das transações online. O principal desenvolvimento neste sentido foi a Sarbanes-Oxley Act (SOXA),[29] adotado pelo Congresso dos EUA como uma resposta aos escândalos financeiros envolvendo a Enron, a Arthur Andersen e a WorldCom.

27 Este artigo apresenta uma introdução ao banco online e uma pesquisa das suas vantagens e desvantagens em comparação ao banco tradicional. Acessível em <http://www.bankrate.com/brm/olbstep2.asp> [acessado em 17 de fevereiro de 2014].

28 appsworldblog (2011) 5 Reasons why you need to be ready for Mobile Payments. 10 de Agosto. Acessível em <http://www.apps-world.net/blog/2011/08/10/5-reasons-why-you-need- to-be-ready-for-mobile-payments/> [acessado em 17 de fevereiro de 2014.

29 Soxlaw (sem data) A guide to the Sarbanes Oxley Act. Acessível em <http://www.soxlaw.com/> [acessado em 17 de fevereiro de 2014]

Esta ação aumenta o controle financeiro e também a responsabilidade das instituições financeiras pela segurança das transações online. Ela também divide o ônus da responsabilidade pela segurança entre os clientes – que devem adotar certa cautela – e as instituições financeiras.[30]

Falta de meios de pagamento

A ausência de meios de pagamento frequentemente é vista como um dos principais impedimentos para o desenvolvimento mais rápido do comércio eletrônico. Atualmente, o comércio eletrônico é conduzido principalmente via cartão de crédito. Isto é um obstáculo relevante para os países em desenvolvimento que não possuem um mercado de cartão de crédito desenvolvido. Os governos nestes países teriam que fazer mudanças necessárias no âmbito jurídico para viabilizar a implementação mais rápida do pagamento via cartões.

Iniciativas nacionais

Para incentivar o desenvolvimento do comércio eletrônico, os governos mundiais precisam estimular todas as formas de pagamento sem dinheiro, inclusive cartão de crédito e dinheiro eletrônico. A implementação mais rápida do dinheiro eletrônico demandará que haja mais atividades regulatórias governamentais. Depois de Hong Kong, o primeiro a aplicar uma legislação abrangente para o dinheiro eletrônico, a UE adotou a Diretiva do Dinheiro Eletrônico[31] em 2000 (revisada em 2009). Diferentemente do dinheiro eletrônico, não existe regulação para a moeda virtual na UE. Atualmente, cabe aos estados-membros regular as moedas virtuais como o Bitcoin. A Alemanha considera o Bitcoin "dinheiro privado" trocado entre duas pessoas ou empresas. No Reino Unido, é considerado um meio de troca, mas não dinheiro. A maior parte dos países escolheu a abordagem de "esperar para ver". Atualmente, o Bitcoin não oferece risco relevante para o sistema monetário na forma de seus vários usos indevidos (lavagem de dinheiro, roubo, etc). No entanto, alguns países, como a Rússia e a Tailândia, tomaram medidas mais radicais, banindo o Bitcoin.

30 Para mais informações, consultar: Jacobs E (sem data), Security as a Legal Obligation: About EU Legislation Related to Security and Sarbanes-Oxley in the European Union. Acessível em <http://www.arraydev.com/commerce/JIBC/2005-08/security.htm> [acessado em 17 de fevereiro de 2014].

31 Comissão Europeia (sem data) E-money. Acessível em <http://ec.europa.eu/internalmarket/payments/emoney/index_en.htm> [acessado em 17 de fevereiro de 2014] Nota do Tradutor: o endereço foi substituído por <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF> [acessado em 7 de março de 2017].

A abordagem da questão no nível internacional

Devido à natureza da Internet, é provável que o dinheiro eletrônico e as moedas virtuais se tornem um fenômeno global, dessa forma oferecendo motivo para abordar a questão no nível internacional. Um ator potencial no campo do banco eletrônico é o Grupo de Banco Eletrônico do Comitê da Basiléia. Este grupo já começou a tratar das questões de autorização, padrões prudenciais, transparência, privacidade, lavagem de dinheiro e supervisão transnacional, questões cruciais para a adoção do dinheiro eletrônico.[32]

Com relação à moeda virtual, a principal iniciativa internacional foi tomada pela Força-Tarefa de Ação Financeira (Financial Action Task Force - FATF), que trata das questões envolvendo a lavagem de dinheiro e o financiamento do terrorismo.[33] Os EUA iniciaram discussões na FATF sobre a forma de aplicar as regras contra a lavagem de dinheiro e o financiamento do terrorismo no campo das moedas virtuais.

Conexão com o cumprimento da lei

A requisição feita em 2002 pelo Procurador Geral do Estado de Nova York ao PayPal e ao Citibank para que estes não realizassem pagamentos a cassinos da Internet estabelece uma conexão direta entre o pagamento eletrônico e o cumprimento da lei.[34] Aquilo que os órgãos de execução da lei não conseguiram alcançar por meio de instrumentos jurídicos, conseguiram atingir por meio do controle de pagamentos eletrônicos.

Privacidade

O uso dos sistemas de pagamentos eletrônicos deixa um rastro de cada transação realizada que é registrada pelos emissores do instrumento de pagamento eletrônico (empresas de cartão de crédito, bancos). Embora a manutenção de tais registros seja necessária e justificável para fins de compensação, a agregação destes dados pode ser uma grave ameaça à privacidade dos usuários se a exploração dos dados for utilizada para rastrear hábitos de compra

32 O Grupo da Basileia está baseado no Banco de Compensações Internacionais. Apresenta o documento Survey of Developments in Electronic Money and Internet and Mobile Payments. Acessível em <http://www.bis.org/publ/cpss62.pdf> [acessado em 17 de fevereiro de 2014].

33 Sítio web FATF. Acessível em <http://www.fatf-gafi.org/pages/aboutus/> [acessado em 10 de agosto de 2014].

34 Richtel M (2002) PayPal and New York in Accord on Gambling. The New York Times, 22 de agosto. Acessível em <http://www.nytimes.com/2002/08/22/business/technology- paypal-and-new-york-in-accord-on-gambling.html?src=pm> [acessado em 17 de fevereiro de 2014]

e gasto ou atribuir pontos aos clientes para a provisão de futuros serviços financeiros.[35]

Riscos e uso indevido das moedas virtuais

Os riscos da moeda virtual ficaram claros após o fechamento da Mt Gox, uma das maiores empresas de Bitcoin, em fevereiro de 2014.[36] Diversos investidores perderam aproximadamente US$500 milhões. Existem vários sinais de que as moedas virtuais podem ser utilizadas indevidamente para bens e serviços ilegais, fraude e lavagem de dinheiro. O anonimato das transações com Bitcoin aumenta a possibilidade de uso indevido. Até o momento, houve apenas alguns casos de uso indevido relatado. O FBI fechou o sítio web Silk Road, que era usado para comercializar dados de cartões roubados, drogas e outros produtos ilegais; o sítio web usou o Bitcoin como meio de pagamento.

Proteção ao consumidor

A confiança do cliente é uma das principais pré-condições para o êxito do comércio eletrônico. O comércio eletrônico ainda é relativamente novo e os clientes ainda não se sentem seguros com ele em comparação às compras no mundo real. A proteção ao consumidor é um importante instrumento jurídico para desenvolver a confiança no comércio eletrônico e sua regulação deveria proteger os consumidores em diversas áreas:

- Utilização online das informações de cartão de crédito.
- Propaganda enganosa.
- Entrega de produtos defeituosos.

A nova idiossincrasia do comércio eletrônico é a internacionalização da proteção ao consumidor, que não é uma questão vital no comércio tradicional. No passado, os clientes raramente precisavam de proteção internacional, compravam localmente e, portanto, precisavam de proteção ao consumidor no âmbito local. Com o comércio eletrônico, um número maior de transações acontecem no nível transnacional. A jurisdição é uma questão importante referente à proteção ao consumidor. Ela envolve duas principais abordagens. A primeira favorece o vendedor (essencialmente o negócio eletrônico) e é uma abordagem

35 Prater C (2009) What you buy, where you shop may affect your credit. Acessível em <http://www.creditcards.com/credit-card-news/how-shopping-can-affect-credit-1282.php> [acessado em 17 de fevereiro de 2014].

36 Villar R, Knight S, Wolf B (2014) Bitcoin exchange Mt. Gox goes dark in blow to virtual currency. Acessível em <http://www.reuters.com/article/2014/02/25/us-mtgox-sítioweb- idUSBREA1O07920140225> [acessado em 10 de agosto de 2014].

baseada no país de origem/prescrição do vendedor. Neste contexto, as empresas de comércio eletrônico têm a vantagem de confiar em um ambiente jurídico previsível e conhecido. A outra abordagem, que favorece o cliente, é uma abordagem baseada no país de destino. A principal desvantagem para as empresas de comércio eletrônico é a potencial exposição a inúmeras jurisdições judiciais. Uma possível solução para este dilema é fortalecer a harmonização das regras de proteção ao consumidor, diminuindo assim a relevância desta questão. Assim como outras questões do comércio eletrônico, a OCDE assumiu a liderança ao adotar em 1999 as Diretrizes para Proteção do Consumidor no Contexto do Comércio Eletrônico[37] e em 2003 as Diretrizes para Proteção do Consumidor contra Práticas Comerciais Fraudulentas e Enganosas Transfronteiriças.[38] Os principais princípios estabelecidos pela OCDE ainda são válidos e foram adotados por outras associações comerciais, entre as quais a Câmara Internacional do Comércio e o Council of Better Business Bureaus.[39]

A UE oferece um alto nível de proteção ao consumidor do comércio eletrônico e promove campanhas de conscientização sobre questões referentes às compras online. O problema da jurisdição foi resolvido por meio do Regulamento de Bruxelas I,[40] que estipula que os clientes sempre poderão contar com os recursos da proteção jurídica local. A versão reformulada do Regulamento de Bruxelas I[41] aplicável desde janeiro de 2015, harmoniza ainda mais as regras de

37 OCDE (1999) Guidelines for Consumer Protection in the Context of Economic Commerce. Acessível em <http://www.oecd.org/internet/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm> [acessado em 17 de fevereiro de 2014].

38 OCDE (2003) Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices. Acessível em <http://www.oecd.org/sti/consumer/oecdguidelinesforprotectingconsumersfromfraudulentanddeceptivecommercialpracticesacrossborders2003.htm> [acessado em 17 de fevereiro de 2014]. Nota do Tradutor: o endereço foi substituído por <http://www.oecd-ilibrary.org/industry-and-services/oecd-guidelines-for-protecting-consumers-from-fraudulent-and-deceptive-commercial-practices-across-borders_9789264103573-en-fr> [acessado em 7 de março de 2017].

39 Sítio web do Better Business Bureaus. Acessível em <http://www.bbb.org/us/cbbb/> [acessado em 17 de fevereiro de 2014]

40 União Europeia (sem data) Regulação (EC) No 44/2001 (Regulamento Bruxelas I). Acessível em <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001R0044> [acessado em 11 de agosto de 2014].

41 União Europeia (sem data) Regulação (EU) No 1215/2012 (Regulamento Bruxelas I Reformulada). Acessível em <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:en:PDF> [acessado em 11 de agosto de 2014].

jurisdição ao ampliar as situações nas quais pessoas não domiciliadas na UE podem ser processadas pelos consumidores nos tribunais dos estados-membros da UE.

Mais da metade dos consumidores da UE (53%) fizeram pelo menos uma compra online nos 12 meses anteriores a setembro de 2012, quase o dobro do volume desde 2006. Porém, apenas 15% dos consumidores compraram online de vendedores fora de seus países. Isto se reflete no nível de confiança: embora 53% se sintam confortáveis para comprar online de lojistas nacionais, apenas 36% se sente confortável para comprar de outro país da UE.[42]

No nível global, nenhum instrumento jurídico internacional pertinente foi estabelecido. Um dos mais apropriados, a Convenção das Nações Unidas sobre Contratos de Compra e Venda Internacional de Mercadorias[43] de 1980, não abrange os contratos com consumidores e a proteção ao consumidor.

Uma série de associações privadas e organizações não governamentais também prioriza a proteção ao consumidor no âmbito do comércio eletrônico, entre as quais a Consumers International, a International Consumer Protection and Enforcement Network e a Consumer Reports WebWatch.

O futuro desenvolvimento do comércio eletrônico irá exigir a harmonização das leis nacionais ou um regime internacional novo para a proteção ao consumidor no comércio eletrônico.

Tributação

Após Faraday descobrir o princípio básico da eletricidade em 1831 (indução eletromagnética), um político cético lhe perguntou sobre o propósito de sua invenção. Faraday respondeu: "Senhor, não sei para que serve. Mas de uma coisa tenho quase certeza, um dia o senhor cobrará imposto sobre ela". [44]

Com a Internet entrando no mainstream da sociedade contemporânea, a questão da tributação ganhou mais destaque. Ela se tornou ainda mais importante desde a crise financeira de 2008. Muitos governos têm tentado aumentar a receita fiscal para reduzir a crescente dívida

42 The Gallup Organisation (2013) Consumer attitudes towards cross-border trade and consumer protection. Analytical Report. Flash Eurobarometer. Acessível em <http://ec.europa.eu/public_opinion/flash/fl_358_sum_en.pdf> [acessado em 14 de agosto de 2014]

43 CNUDCI (1980) CISG ONU. Acessível em <http://www.uncitral.org/uncitral/uncitraltexts/sale_goods/1980CISG.htm> [acessado em 17 de fevereiro de 2014].

44 Maastricht Economic Research Institute on Innovation and Technology (MERIT) (1999). Cybertax. Acessível em <www.merit.unu.edu/publications/rmpdf/1998/rm1998-020.pdf> [acessado em 17 de fevereiro de 2014]

pública. O relatório mais abrangente sobre a tributação da Internet foi apresentado pelo Ministério da Economia e Finanças da França em janeiro de 2013.[45] A tributação de atividades econômicas na Internet se tornou uma das primeiras possibilidades de aumentar a receita fiscal. O dilema da governança da Internet referente a se as questões cibernéticas deveriam ser tratadas de forma diferente das questões da vida real se encontra claramente refletida na questão da tributação.[46] Desde o início, os EUA buscam declarar a Internet uma zona franca. Em 1998, o Congresso dos EUA adotou a lei Internet Tax Freedom Act,[47] que foi prorrogada mais outros três anos em dezembro de 2004. Em outubro de 2007, a lei foi prorrogada até 2014, apesar de alguns receios sobre isto resultar em perdas significativas de receitas.[48]

A OCDE e a UE defenderam opinião contrária, isto é, de que a Internet não deveria receber tributação especial. Os Princípios de Ottawa da OCDE especificam que a tributação do comércio eletrônico não deveria ter como base os mesmos princípios que a tributação sobre as atividades comerciais tradicionais.[49] Ao aplicar este princípio, a UE implementou uma regulação em 2003 solicitando que empresas de comércio eletrônico que não são da UE paguem imposto sobre o valor agregado (IVA) ao vender dentro da UE. A principal motivação para a decisão da UE foi que as empresas de comércio eletrônico que não são da UE (principalmente dos EUA) detinham vantagem sobre as empresas europeias, obrigadas a pagar IVA sobre todas as transações, inclusive as eletrônicas.

Outra questão sobre a tributação eletrônica que ainda não foi resolvida entre a UE e os EUA é a questão do local da tributação. Os Princípios

45 Collin P, Colin N (2013) Mission d'expertise sur la fiscalité de l'économie numérique. Acessível em <http://www.redressement-productif.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf> [acessado em 10 de agosto de 2014]

46 Para uma discussão sobre vários aspectos da política de tributação e a Internet, consultar:Cockfield AJ (2001) Transforming the Internet into a Taxable Forum: A Case Study in E-Commerce Taxation, 85 Minn. L. Rev. 1171, 1235-1236; Morse EA (1997) State Taxation of Internet Commerce: Something New under the Sun? 30 Creighton L. Rev. 1113, 1124-1227; Williams WR (2001) The Role of Caesar in the Next Millennium? Taxation of E-Commerce: An Overview and Analysis, 27 Wm Mitchell L. Rev. 1703, 1707

47 Internet Tax Freedom Act. Acessível em <http://legacy.gseis.ucla.edu/iclp/itfa.htm> acessado em 17 de fevereiro de 2014].

48 Mazerov M (2007) Making the 'Internet Tax Freedom Act' permanent could lead to a substantial revenue loss for states and localities. Acessível em <http://www.cbpp.org/7-11-07sfp.htm> [acessado em 17 de fevereiro de 2014].

49 Os Princípios de Ottawa da Tributação são: Neutralidade, Eficiência e Certeza e simplicidade, Efectividade e equidade, Flexibilidade. Ver OCDE (2003) Implementation of the Ottawa Taxation Framework Conditions. The 2003 Report. Acessível em <http://www.oecd.org/tax/administration/20499630.pdf> [acessado em 17 de fevereiro de 2014].

de Ottawa aplicaram o princípio do "destino" em lugar do princípio de "origem" da tributação. O governo dos EUA tem forte interesse em fazer com que a tributação permaneça na origem das transações, uma vez que a maioria das empresas de comércio eletrônico estão baseadas nos EUA. Em contraposição, o interesse da UE na "tributação do destino" é amplamente influenciado pelo fato de que a UE tem mais consumidores do que vendedores no âmbito do comércio eletrônico.

Assinaturas digitais

Em termos gerais, as assinaturas digitais estão conectadas à autenticação de pessoas na Internet, o que afeta muitos aspectos, inclusive jurisdição, crimes cibernéticos e comércio eletrônico. A utilização das assinaturas digitais deveria contribuir para estabelecer confiança na Internet. A autenticação digital em geral faz parte da estrutura do comércio eletrônico. Deveria facilitar as transações do comércio eletrônico por meio da conclusão de contratos eletrônicos. Por exemplo, o contrato é válido e vinculativo quando preenchido via e-mail ou sítio web? Em muitos países, a lei exige que os contratos sejam celebrados "por escrito" ou "assinados". O que isto significa em termos de Internet? Diante destes dilemas e pressionados a estabelecer um ambiente facilitador do comércio eletrônico, muitos governos começaram a adotar legislações para assinatura digital.

Com relação às assinaturas digitais, o principal dilema é que os governos não estão adotando uma regulação sobre um problema existente, como o crime cibernético ou a violação aos direitos autorais; em vez disso estão criando um novo ambiente regulatório no qual eles não possuem nenhuma experiência prática. Isto levou a diversas soluções e à indefinição geral das disposições das assinaturas digitais. Surgiram três grandes abordagens da regulação das assinaturas digitais.[50]

A primeira é uma abordagem minimalista, especificando que as assinaturas eletrônicas não podem ser negadas porque estão em formato eletrônico. Esta abordagem determina uma utilização bem ampla das assinaturas digitais e foi adotada em países com o sistema da common law: os Estados Unidos, o Canadá, a Nova Zelândia e a Austrália.

50 Para uma explicação mais detalhada destas três abordagens, consultar: ILPF (sem data Survey of International Electronic and Digital Signature Initiatives. Acessível em <http://www.ilpf.org/groups/survey.htm#IB> [acessado em 17 de fevereiro de 2014].

A segunda abordagem é maximalista, especificando o quadro e os procedimentos das assinaturas digitais, entre as quais a criptografia e o uso dos principais identificadores públicos. Esta abordagem geralmente determina o estabelecimento de autoridades certificadas específicas, que poderão certificar futuros usuários das assinaturas digitais, tendo prevalecido nas leis dos países europeus, como a Alemanha e a Itália.

A terceira abordagem, adotada dentro da Diretiva de Assinaturas Eletrônicas da UE,[51] combina estas duas abordagens. As suas disposições são minimalistas com relação ao reconhecimento de assinaturas digitais feitas através de um meio eletrônico. A abordagem maximalista também é reconhecida por meio da concessão de "assinaturas eletrônicas avançadas" que terá efeitos jurídicos mais sólidos (ex., maior facilidade de comprovar tais assinaturas em ações judiciais). A regulação da UE referente às assinaturas digitais era uma das respostas no nível multilateral. Embora esta regulação tenha sido adotada em todos os estados-membros da UE, a diferença na situação jurídica das assinaturas digitais continua existindo.[52]

No nível global, em 2001, a CNUDCI adotou a Lei Modelo sobre Assinaturas Eletrônicas,[53] que confere o mesmo status às assinaturas digitais das assinaturas escritas a mão, desde que algumas exigências técnicas sejam atendidas. A Câmara Internacional do Comércio (ICC) emitiu o General Usage in International Digitally Ensured Commerce (GUIDEC), que fornece uma pesquisa das melhores práticas, regulações e questões sobre certificação.[54]

As iniciativas referentes à infraestrutura de chaves públicas (PKI) estão diretamente relacionadas às assinaturas digitais. Duas organizações, a UIT e a IETF, estão envolvidas com a padronização da PKI.

51 Comissão Europeia (1999) Directive on Electronic Signatures. Acessível em <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML> [acessado em 17 de fevereiro de 2014].

52 Comissão Europeia (2006) Relatório da Operação da Diretiva 1999/93/EC sobre Quadro da Comunidade para Assinaturas Eletrônicas. Acessível em <http://eur-lex.europa.eu/LexUriServ/%20LexUriServ.do?uri=COM:2006:0120:FIN:EN:PDF> [acessado em 17 de fevereiro de 2014]

53 CNUDCI (2001) Model Law on Electronic Signatures. Acessível em <http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2001Model_signatures.html> [acessado em 17 de fevereiro de 2014].

54 Mais informações sobre a elaboração do GUIDEC podem ser encontradas no sítio web dedicado a ICC. Acessível em <http://www.iccwbo.org/policy/ebitt/id2340/index.html> [acessado em 17 de fevereiro de 2014]

Questões

Privacidade e assinaturas digitais

As assinaturas digitais fazem parte da consideração mais ampla do relacionamento entre privacidade e autenticação na Internet, sendo apenas uma das importantes técnicas utilizadas para identificar pessoas na Internet.[55]

Por exemplo, em alguns países nos quais a legislação ou os padrões e procedimentos das assinaturas digitais ainda não foram implementados, a autenticação de SMS via celular é utilizada por bancos para aprovar as transações online dos clientes.

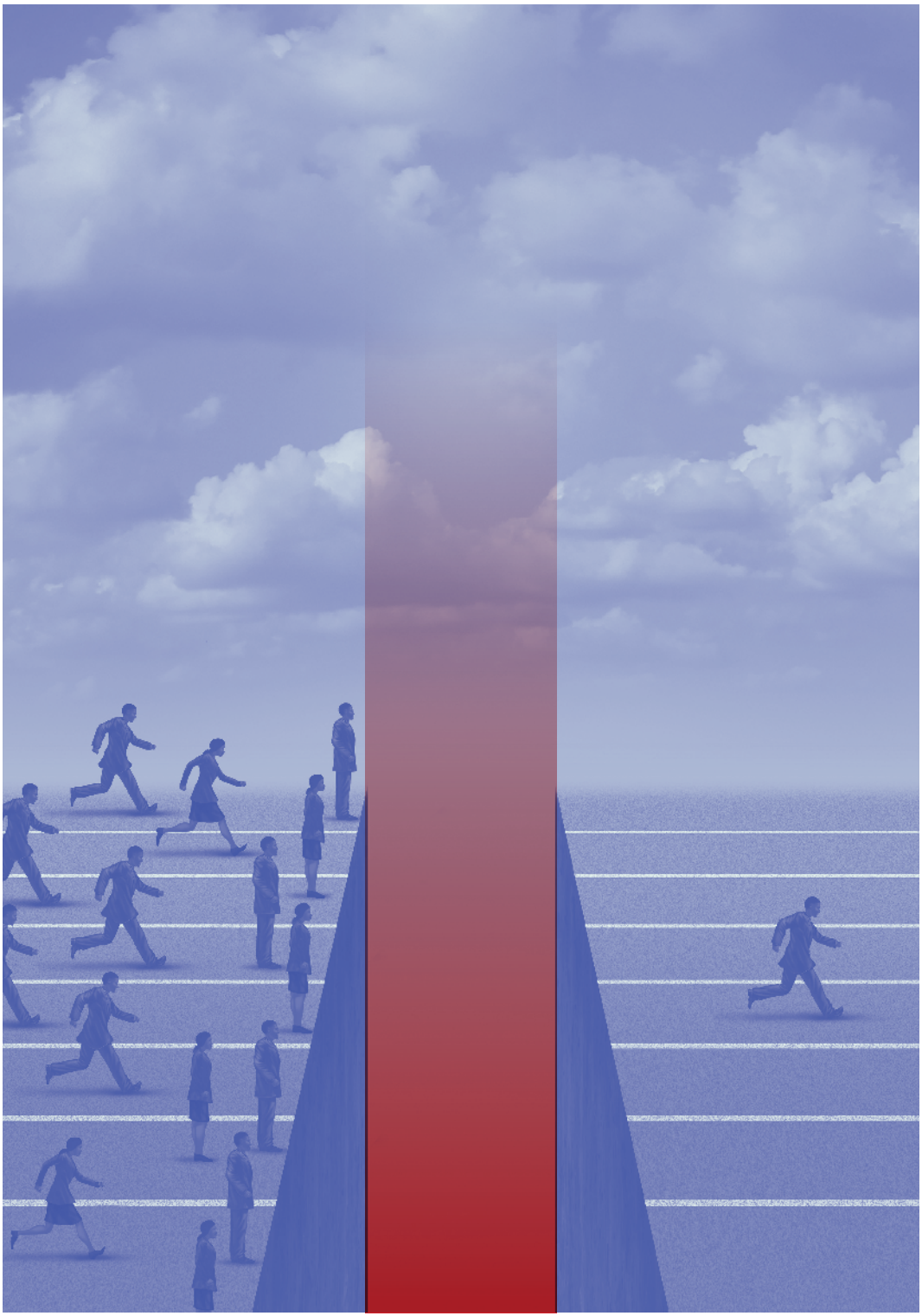
A necessidade de padrões de implementação detalhados

Apesar de muitos países desenvolvidos terem adotado uma ampla legislação para assinaturas digitais, os seus padrões e procedimentos de implementação costumam ser ausentes de detalhes. Dada a novidade das questões envolvidas, muitos países estão aguardando para saber em qual direção os reais padrões irão se desenvolver. As iniciativas de padronização ocorrem em diversos níveis, entre os quais em organizações internacionais (a UIT), órgão regionais (Comitê Europeu para Padronização – CEN) e associações profissionais (a IETF).

O risco da incompatibilidade

A variedade de abordagens e padrões no campo das assinaturas digitais poderia levar à incompatibilidade entre diferentes sistemas nacionais. Soluções remendadas poderiam limitar o desenvolvimento do comércio eletrônico no nível global. A harmonização necessária deveria ser realizada por meio de organizações regionais e globais.

55 Longmuir G (2000) Privacy and Digital Authentication. Acessível em <http://caligula.anuedu.au/~gavin/ResearchPaper.htm> [acessado em 17 de fevereiro de 2014]. Este artigo se concentra nos aspectos pessoal, comunitário e governamental da necessidade da autenticação no mundo digital. Nota do Tradutor: o endereço foi substituído por <www.longmuir.net/papers/Research%20Paper.doc> [acessado em 9 de março de 2017].



Cesta de desenvolvimento

A tecnologia nunca é neutra. A história da sociedade apresenta muitos exemplos nos quais a tecnologia confere poder a alguns indivíduos, grupos ou nações e exclui outros. A Internet não é diferente neste sentido. Do nível individual até o nível global, uma mudança profunda ocorreu na distribuição de riqueza e poder. O impacto da Internet na distribuição de poder e desenvolvimento levantou muitas questões, entre as quais:

- A Internet irá reduzir ou expandir a exclusão digital existente entre os países desenvolvidos e em desenvolvimento?
- De que forma e quando os países em desenvolvimento conseguirão atingir os níveis digitais dos países desenvolvidos?

As respostas a estas e outras perguntas exigem a análise da relevância do desenvolvimento no contexto da governança Internet. Quase toda questão sobre governança da Internet tem um aspecto referente ao desenvolvimento:

- A existência de certa infraestrutura de comunicação facilita o acesso, a primeira pré-condição para superar o fosso digital.
- O atual modelo econômico para o acesso da Internet, que impõe um ônus desproporcional aos países em desenvolvimento, os obrigando a financiar o acesso a backbones localizados nos países desenvolvidos.
- A regulação global dos direitos de propriedade intelectual, que afeta diretamente o desenvolvimento, devido à oportunidade reduzida dos países em desenvolvimento para acessar conhecimento e informação online.

O aspecto de desenvolvimento da CMSI tem sido frequentemente repetido, a começar pela primeira Resolução da Assembleia Geral da ONU sobre a CMSI, enfatizando que a CMSI deveria estar "promovendo o desenvolvimento, mais especificamente com relação ao acesso à tecnologia, bem como a sua transferência".[1] A Declaração de Genebra e o Plano de Ação da CMSI destacou o desenvolvimento como prioridade e o relacionou a Declaração do Milênio das Nações Unidas[2] e sua promoção de acesso de todos os países à informação, ao conhecimento e às tecnologias da comunicação para o desenvolvimento.

Com esta ligação com as metas de desenvolvimento do milênio (mille-

1 Assembleia Geral das Nações Unidas [UNGA] (2002) Resolução 56/183. World Summit on the Information Society (A/RES/56/183). Acessível em <http://www.itu.int/wsis/docs/background/resolutions/56_183_unga_2002.pdf> [acessado em 24 de fevereiro de 2014].

2 Nações Unidas (2000) Millennium Declaration. Acessível em <http://www.un.org/millennium/declaration/ares552e.htm> [acessado em 24 de fevereiro de 2014

nium development goals – MDGs),[3] a CMSI se encontra em uma posição sólida no contexto do desenvolvimento.

Esta linha de preocupação continuou presente no IGF, no qual o tema do desenvolvimento foi destaque, a começar pela primeira reunião em Atenas (2006), passando por oficinas específicas e até mesmo uma sessão principal em Vílnius (2010). As preocupações relacionadas ao desenvolvimento estavam entre as cinco mais frequentemente abordadas no contexto do debate sobre a continuação do IGF, notavelmente melhorando a participação dos países em desenvolvimento e aumentando a prioridade dada ao desenvolvimento.[4]

De que forma as TIC afetam o desenvolvimento da sociedade?

Os principais dilemas sobre as TIC e o desenvolvimento foram resumidos em um artigo na revista *The Economist*,[5] que lança argumentos a favor e contra a teoria de que as TIC é um incentivo específico para o desenvolvimento.

A exclusão digital

A exclusão digital pode ser definida como uma fissura entre aqueles que, por motivos técnicos, políticos, sociais ou econômicos, têm acesso e capacidades para usar as TIC/Internet e aqueles que não têm. Diversos pontos de vista foram apresentados sobre o tamanho e a relevância da exclusão digital. A(s) exlusão(s) digital(is) existe(m) em diferentes níveis: dentro de países e entre países, entre populações rural e urbana, entre os idosos e os jovens, bem como entre homens e mulheres. A OCDE se refere à exclusão digital como "a lacuna entre pessoas, residências, empresas e áreas geográficas em diferentes níveis socioeconômicos com relação tanto a oportunidades de acesso às tecnologias de informação e comunicação (TIC) e quanto ao seu uso da Internet para uma ampla variedade de atividades".[6]

3 Nações Unidas (sem data) Millennium Development Goals. Acessível em <http://www.un.org/millenniumgoals/> [acessado em 24 de fevereiro de 2014]

4 auDA (sem data) Continuation of the Internet Governance Forum. Analysis of the Note of the Secretary-General. Acessível em <http://www.intgovforum.org/cms/2010/contributions/Open%20Consultation%20on%20Enhanced%20Cooperation%20-%20auDA%20submission.pdf> [acessado em 24 de fevereiro de 2014]

5 The Economist (2000) A survey of the new economy: Falling through the Net? For the developing world, IT is more of an opportunity than a threat. Acessível em <http://www.economist.com/node/375645> [acessado em 24 de fevereiro de 2014]

6 OCDE (2001) Understanding the Digital Divide. p. 5. Acessível em <http://www.oecd.orginternet/ieconomy/1888451.pdf> [acessado em 24 de fevereiro de 2014].

TABELA 3

AS TIC não facilitam o desenvolvimento	*AS TIC facilitam o desenvolvimento*
As "externalidades da rede" ajudam os pioneiros a estabelecerem uma posição dominante. Isto favorece as gigantes norte-americanas, e dessa forma as empresas dos países emergentes seriam excluídas.	As TIC diminuiem os custos trabalhistas; é mais barato investir em países em desenvolvimento.
A mudança de poder do vendedor para o comprador (a Internet inevitavelmente faz surgir o cenário no qual "uma outra alternativa de fornecedor está a um clique de distância") prejudicará países mais pobres. Prejudicará produtores de mercadorias principalmente dos países em desenvolvimento.	As TIC se expandem rapidamente para além das fronteiras em comparação a tecnologias anteriores (ferrovias e a eletricidade) que levaram décadas até chegar a países em desenvolvimento. AsTIC estão avançando muito rapidamente.
A maior participação em ações de empresas de alta tecnologia em economias ricas reduzirá o interesse do investidor em países em desenvolvimento.	As TIC oferece a oportunidade de ultrapassar tecnologias antigas ao pular fases intermediárias, como fios de cobre e telefones analógicos, incentivando o desenvolvimento.
	A propensão das TIC em reduzir o tamanho ideal de uma empresa na maioria das indústrias está muito mais próxima das necessidades dos países em desenvolvimento.

A exclusão digital não é um fenômenos independente. Elareflete as grandes desigualdades socioeconômicas existentes na educação, saúde, capital, moradia, emprego, água limpa e comida. Esta definição é claramente expressa pela Opportunity Task Force (DOT Force) do G8: "Não existe dicotomia entre a 'exclusão digital' e as divisões sociais e econômicas mais profundas que o processo de desenvolvimento deveria abordar; a exclusão digital precisa ser compreendida e abordada no contexto destas divisões mais profundas."[7]

7 G8 (2001) Digital Opportunities for All: Meeting the Challenge. Report of the Digital Opportunity Task Force (DOT Force) including a proposal for a Genoa Plan of Action. Acessível em <http://www.g7.utoronto.ca/summit/2001genoa/dotforce1.html> [acessado em 24 de fevereiro de 2014

A exclusão digital está aumentando?

Os progressos da TIC/Internet deixam os países em desenvolvimento para trás em um ritmo muito mais rápido do que os avanços em outros campos (ex., técnicas agrícolas ou médicas); e como os países desenvolvidos possuem as ferramentas necessárias para utilizar com sucesso estes avanços tecnológicos, a exclusão digital parece estar aumentando de forma contínua e rápida. Esta é a visão frequentemente expressa em diversos documentos bem conceituados, como os Relatórios de Desenvolvimento Humano do Programa das Nações Unidas para o Desenvolvimento (PNUD) e os Relatórios Globais do Trabalho da OIT. Algumas visões contrárias argumentam que as estatísticas sobre a exclusão digital costumam ser enganosas e que a exclusão digital na verdade não está aumentando. De acordo com este ponto de vista, o foco tradicional sobre a quantidade de computadores, a quantidade de sítios web na Internet ou a largura de banda disponível deveria ser substituído pelo foco no impacto mais amplo da TIC/Internet na sociedade dos países em desenvolvimento. Os exemplos frequentemente citados são o êxito digital observado no Brasil, na Índia e na China. Contudo, os critérios para acessar as lacunas da exclusão digital também estão mudando e se tornando mais complexos para capturar melhor as realidades de desenvolvimento. As avaliações atuais levam em consideração aspectos como a prontidão das TIC e seu impacto geral na sociedade. O Fórum Econômico Mundial desenvolveu o Índice de Prontidão em Rede (Networked Readiness Index - NRI) como forma de propor uma nova abordagem para a mensuração do nível de Internet em países em todo o mundo.[8] Ele também oferece novos pontos de vista sobre a forma de lidar com a exclusão digital.

Acesso universal

Além da exclusão digital, outro conceito frequentemente mencionado no debate sobre o desenvolvimento é o acesso universal, isto é, o acesso para todos. Embora devesse ser o alicerce de qualquer política de desenvolvimento digital, percepções e concepções divergentes sobre a natureza e o escopo desta política de acesso ainda existem. A questão do acesso universal no nível global continua sendo em grande parte uma questão aberta, basicamente sujeita à disponibilidade dos países desenvolvidos em investir na realização deste objetivo.

8 Fórum Econômico Mundial (2013) Global Information Technology Report. Acessível em <http://www.weforum.org/reports/global-information-technology-report-2013> [acessado em 10 de agosto de 2014].

Diferentemente do acesso universal no nível global, em alguns países o acesso global é um conceito econômico e jurídico bem desenvolvido. Oferecer acesso às telecomunicações a todos os cidadãos tem sido a base das políticas de telecomunicação dos EUA. O resultado é um sistema bem desenvolvido com vários mecanismos políticos e financeiros, cujo objetivo é subsidiar os custos de acesso em áreas remotas e regiões com altos custos de conexão. O subsídio é financiado por regiões com baixos custos de conexão, principalmente em cidades grandes. A UE também tem adotado uma série de medidas concretas para alcançar o acesso universal, ao promover políticas que garantam a cada cidadão o acesso a serviços básicos de comunicação, inclusive conexão à Internet, e ao promulgar regulamentos específicos neste sentido.[9]

Estratégias para superar a exclusão digital

A teoria do desenvolvimento centrada na tecnologia, que tem dominado as políticas e os círculos acadêmicos nos últimos 50 anos, argumenta que o desenvolvimento depende da disponibilidade da tecnologia. Quanto mais tecnologia... mais desenvolvimento. No entanto, esta abordagem não funcionou em muitos países (principalmente antigos países socialistas) nos quais ficou evidente que o desenvolvimento da sociedade é um processo muito mais complexo. A tecnologia é necessária, mas não uma pré-condição autossuficiente para o desenvolvimento. Outros elementos incluem o quadro regulatório, apoio financeiro, recursos humanos disponíveis e outras condições socioculturais. Mesmo que todos estes ingredientes estejam presentes, o principal desafio continua sendo saber de que forma e quando eles devem ser utilizados, combinados e interagir.

O desenvolvimento das telecomunicações e as infraestruturas da Internet

O acesso à Internet é um dos principais desafios para superar o fosso digital. A taxa de penetração da Internet em 2012 na África era 16,6% comparada aos 78,6% na América o Norte ou 63,2% na Europa, mas registrou o maior crescimento na última década.[10] Existem dois principais aspectos relacionados ao acesso à Internet nos países em

9 União Europeia [EU] (sem data) Universal Service. Acessível em <http://ec.europa.eu/digital-agenda/en/universal-service> [acessado em 24 de fevereiro de 2014].

10 Internet World Stats (2012) Internet Usage Statistics. The Internet Big Picture.Acessível em <http://www.internetworldstats.com/stats.htm> [acessado em 24 de fev. de 2014]

desenvolvimento. Primeiramente, o acesso a backbones internacionais da Internet. Em segundo lugar, a conectividade nos países em desenvolvimento.

O acesso a backbones internacionais da Internet depende principalmente da disponibilidade dos cabos de fibra ótica submarina. Durante um bom tempo, somente a África Ocidental, estendendo até a África do Sul, recebia o cabo submarino SAT-3. A África Oriental tem acesso muito mais rápido com o East African Submarine Cable System (EASSy), que começou a operar em julho de 2010. Ele cria um anel digital ao redor da África que aumenta significativamente a largura de banda de Internet disponível para o continente africano. As ilhas pequenas e remotas enfrentam desafios similares no acesso à Internet, uma vez que muitas dependem da dispendiosa conectividade via satélite. Esforços estão sendo feitos para encontrar soluções mais eficientes para a conectividade em tais áreas.[11]

Outra solução para o acesso improvisado é a implementação dos Pontos de Troca de Tráfego (PTT), que mantém o tráfego local dentro do país e reduz tanto o uso quanto o custo da largura de banda internacional. Os PTTs são instalações técnicas por meio das quais diferentes ISPs trocam tráfego de Internet por meio de peering (sem pagar), sendo frequentemente estabelecidos para manter o tráfego da Internet dentro de comunidades menores (ex., cidade, região, país), evitando o roteamento desnecessário sobre locais geográficos remotos. Os PTTs também podem desempenhar um papel importante na redução da exclusão digital. Ainda assim, muitos países em desenvolvimento não tem PTTs, o que significa que uma parte considerável do tráfego entre clientes dentro de um país é roteado através de outro país. Isto aumenta o volume de tráfego de dados internacional de longa distância e o custo da prestação de serviços de Internet. Diversas iniciativas buscam estabelecer PTTs em países em desenvolvimento.[12] Uma que obteve considerável êxito foi a iniciativa da Associação Africana de Prestadores de Serviços de Internet, que estabeleceu diversos PTTs na África.

A conectividade dentro dos países em desenvolvimento é outro grande desafio. A maioria dos usuários da Internet estava concen-

11 Para mais informações sobre a situação das Ilhas do Pacífico,ver Economic and Social Commission for Asia and Pacific (2014). Acessível em <http://www.unescap.org/about> [acessado em 28 de março de 2014].

12 Para um estudo sobre o impacto da implementação dos PTTs no Quênia e na Nigéria, ver Internet Society (sem data) Internet exchange points (IXPs). Acessível em <http://internetsociety.org/what-we-do/issues/internet-exchange-points-ixps> [acessado em 24 de fevereiro de 2014]

trada nas cidades maiores. As áreas rurais geralmente não tinham acesso à Internet. A situação começou a mudar com o rápido crescimento da telefonia móvel e da comunicação sem fio. A comunicação sem fio talvez seja a solução para o problema de desenvolver uma infraestrutura de comunicações terrestre tradicional (a colocação de cabos em distâncias muito longas em muitos países asiáticos e africanos). Neste contexto, as políticas de espectro de rádio são de extrema importância para garantir a disponibilidade do espectro e criar as condições de uma Internet aberta sem fio que possa ser compartilhada entre os usuários. Desta forma, o problema da última milha ou da linha de assinantes, um dos principais obstáculos para o desenvolvimento de uma Internet mais rápida, poderá ser superado. Normalmente, o aspecto da infraestrutura da exclusão digital é o foco da UIT por meio de seu Setor de Desenvolvimento de Telecomunicações (UIT-D).

Quem deveria cobrir o custo dos das conexões entre países em desenvolvimento e desenvolvidos?

Quando um usuário final na África envia um e-mail a um correspondente na Europa ou nos EUA, é o ISP africano que arca com os custos da conectividade internacional da África para os EUA. Inversamente, quando um usuário final europeu envia um e-mail à África, ainda é o ISP africano que arca com os custos da conectividade internacional, e por fim é o usuário final africano que sofre as consequências de pagar assinaturas mais altas.

O principal argumento nas discussões sobre alterações no atual sistema de cobranças da Internet usa a analogia do sistema de pagamento financeiro do telefone, que divide os custos e as receitas entre pontos finais de comunicação. Contudo, Geoff Huston argumenta que esta analogia não é sustentável. No sistema de telefonia, apenas uma mercadoria claramente identificável[13] – um telefonema que estabelece uma conversa humana entre dois aparelhos telefônicos – tem um preço. A Internet não tem uma mercadoria equivalente; ela tem pacotes, que atravessam rotas diferentes na rede. Esta fundamental diferença faz com que a analogia seja inadequada. É também o principal motivo para o modelo do acordo financeiro da telefonia não ser aplicável à Internet.

13 Huston G (2005) Where's the Money? Internet Interconnection and Financial Settlement The ISP Column, janeiro de 2005, Internet Society, pp. 7-9. Acessível em <http://www.potaroo. net/ispcol/2005-01/interconn.pdf> [acessado em 24 de fevereiro de 2014].

A UIT iniciou discussões sobre possíveis melhorias ao sistema atual para o pagamento de despesas da Internet, com o principal objetivo de ter uma distribuição mais equilibrada dos custos para o acesso à Internet. Devido à oposição dos países desenvolvidos e telecoms, a Recomendação D. 50 da UIT adotada é praticamente ineficaz.[14] Tentativas fracassadas também foram feitas para apresentar esta questão durante as negociações da OMC. A necessidade de ajustes nos encargos de interconexão foi reiterada no documento final da CMSI e no relatório do GTGI.

Apoio financeiro

Durante o processo da CMSI, a importância do apoio financeiro para cobrir a exclusão digital foi claramente reconhecida. Uma ideia proposta na CMSI foi o estabelecimento do Digital Solidarity Fund, administrado pela ONU, para ajudar países defasados tecnologicamente a construir infraestruturas de telecomunicações. No entanto, a proposta de estabelecer o Digital Solidarity Fund não ganhou apoio mais amplo dos países desenvolvidos, que favoreceram o investimento direto em vez do estabelecimento de um fundo de desenvolvimento centralizado.

Os países em desenvolvimento recebem apoio financeiro por meio de vários canais, inclusive órgãos de desenvolvimento bilateral ou multilateral, como o PNUD ou o Banco Mundial, bem como iniciativas regionais de desenvolvimento e bancos. Com a maior liberalização do mercado de telecomunicações, a tendência para o desenvolvimento de infraestruturas de telecomunicações por meio do investimento direto estrangeiro cresceu. Como os mercados de telecomunicações dos países desenvolvidos estão supersaturados, muitas empresas internacionais de telecomunicações veem os mercados dos países em desenvolvimento como a área do crescimento futuro.

Aspectos socioculturais

O aspecto sociocultural da exclusão digital inclui uma série de questões, inclusive a alfabetização, habilidades de TIC, qualificação, educação e proteção de idiomas.

14 Uma das limitações em negociar esta questão entre governos é que a maior parte dos acordos de interconexão são celebrados entre operadoras privadas de telecomunicações. Costumam ser confidenciais. As recomendações da UIT podem ser acessadas em <http://www.itu.int/rec/T-REC-D.50/e> [acessado em 10 de agosto de 2014].

A existência de uma infraestrutura de comunicação é inútil, a menos que as pessoas possuam os meios (dispositivos) e o conhecimento (alfabetização de TIC) para acessar a Internet e se beneficiar dela. As iniciativas e organizações internacionais como o Um Laptop por Criança (One Laptop per Child) ou o Computer Aid International buscam fornecer equipamentos reciclados e de baixo custo para comunidades sem acesso em países em desenvolvimento. As iniciativas locais para fornecer dispositivos de computadores acessíveis também deslancharam, mas ainda há desafios com relação ao desempenho.[15]

Para os países em desenvolvimento, uma das principais questões tem sido a fuga de cérebros, descrita como a migração do trabalho altamente qualificado dos países em desenvolvimento para os países desenvolvidos. Por meio da fuga de cérebros, os países em desenvolvimento perdem de diversas formas. A principal perda é a de mão de obra qualificada. Os países em desenvolvimento também perdem investimento na qualificação e educação dos profissionais qualificados que migram.

É provável que a fuga de cérebros continue, devido aos diversos esquemas de emprego/emigração implementados nos EUA e em outros países desenvolvidos para atrair mão de obra especializada e qualificada, principalmente em TIC.

Um dos acontecimentos que pode frear ou, em alguns casos, reverter essa fuga de cérebros, é o aumento da terceirização de tarefas de TIC para os países em desenvolvimento. Os exemplos de maior sucesso são o desenvolvimento dos centros da indústria de software da Índia, como Bangalore e Hyderabad.

No âmbito global, a ONU iniciou as Redes Digitais de Diáspora (Digital Diaspora Networks) para promover o desenvolvimento por meio da mobilização da especialização tecnológica, empresarial e profissional e recursos das diásporas no campo das TIC.

Aspectos de políticas e institucionais

As questões sobre políticas das telecomunicações estão intimamente ligadas em muitos aspectos à superação da exclusão digital:

- Os investidores privados e, cada vez mais, os doadores públicos, não estão preparados para investir em países sem um

15 A Índia anunciou o lançamento de um tablet subsidiado pelo governo por apenas US$ 35,00, de acordo com a BBC News South Asia (2011) India launches Aakash tablet computer priced at $35. 5 de outubro. Acessível em <http://www.bbc.co.uk/news/world-south-asia-15180831> [acessado em 24 de fevereiro de 2014]

ambiente institucional e jurídico adequado para o desenvolvimento da Internet.

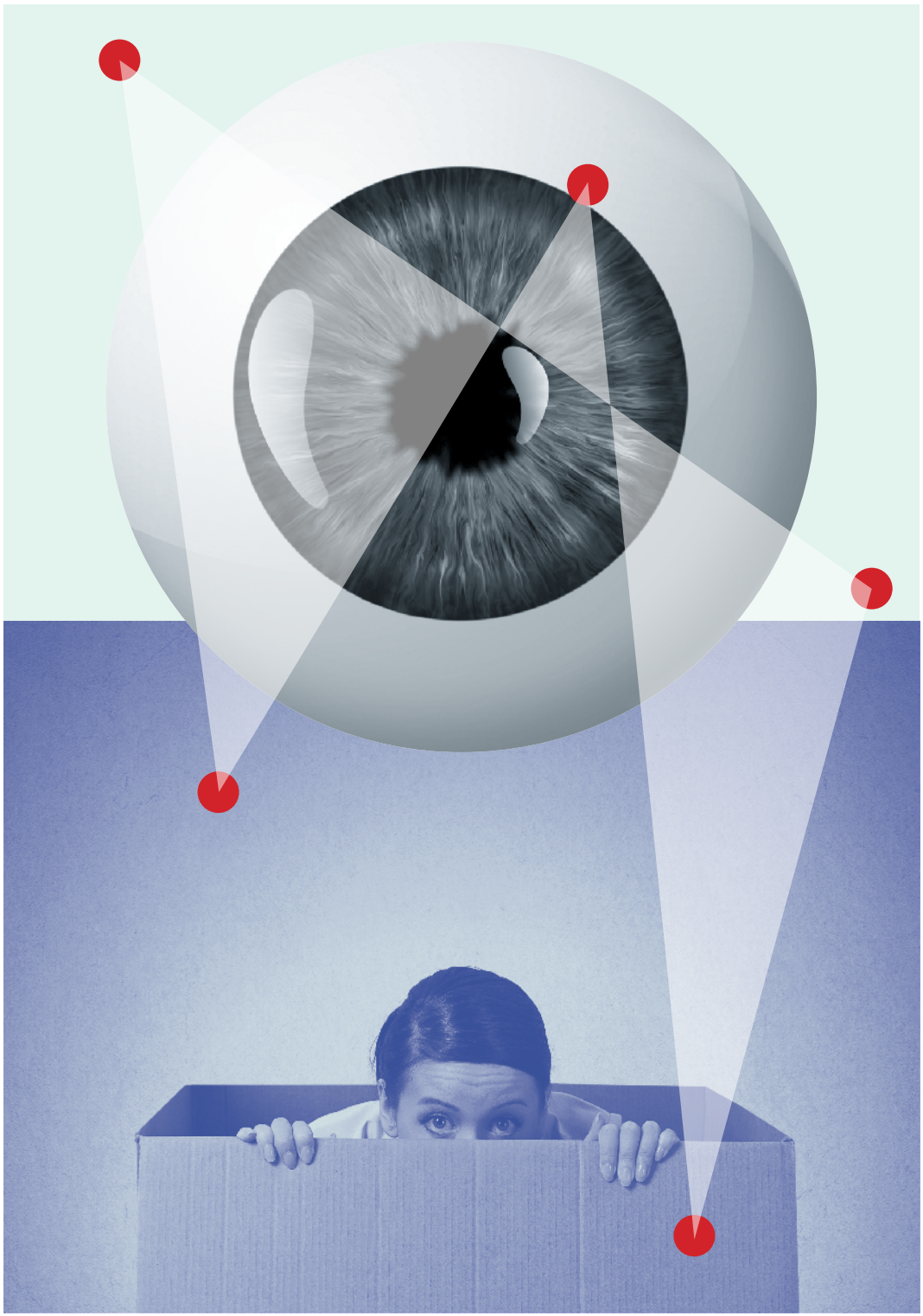
- O desenvolvimento de setores nacionais de TIC depende da criação de quadros regulatórios necessários.
- As políticas de telecomunicações deveriam facilitar o estabelecimento de um mercado de telecomunicações eficiente com mais concorrência, custo baixo e uma ampla variedade de serviços prestados.

A criação de um ambiente facilitador é uma tarefa demandante, implicando a desmonopolização gradual do mercado de telecomunicações, a implementação de leis relacionadas à Internet (abrangendo direitos autorais, privacidade, comércio eletrônico, etc.) e a concessão de acesso a todos, sem restrições políticas, religiosas ou quaisquer outras.

Em termos institucionais, um dos primeiro passos é o estabelecimento de autoridades regulatórias independentes e profissionais na área das telecomunicações. A experiência dos países desenvolvidos mostra que reguladores sólidos são uma pré-condição para o crescimento rápido na infraestrutura de telecomunicações. Nos países em desenvolvimento, o desenvolvimento de autoridades regulatórias está bem no início. Elas costumam ser fracas e sem independência, e frequentemente fazem parte de um sistema no qual operadoras estatais exercem influência nos processos regulatórios e políticos.

Outro grande desafio tem sido a liberalização do mercado de telecomunicações. A Índia e o Brasil costumam ser mencionados como países em desenvolvimento no qual essa liberalização facilitou o rápido crescimento da Internet e do setor de TIC, beneficiando o crescimento econômico geral. Outros países, mais especificamente os menos desenvolvidos, acharam a liberalização do mercado de telecomunicações um grande desafio. Com o fim dos monopólios das telecomunicações, os governos nesses países perderam uma fonte importante de receita orçamentária. Os orçamentos mais baixos afetaram todos os outros setores da vida social e econômica. Em alguns casos, enquanto perderam receitas de telecom, esses países não colheram os frutos da liberalização na forma de custos mais baixos e serviços melhores de telecomunicações, principalmente porque a privatização das empresas de telecomunicações não foi suplementada pelo estabelecimento de um mercado efetivo e da concorrência. Essas práticas levaram o Banco Mundial

a enfatizar que os países deveriam abrir grandes segmentos de mercado para a concorrência, antes ou simultaneamente à privatização das operadoras estatais; dessa forma, reduzirão custos mais rápido que os países que privatizarem primeiro e abrirem para a concorrência depois.



Cesta sociocultural

A Internet teve um impacto considerável sobre o tecido social e cultural da sociedade moderna. É difícil identificar qualquer segmento da nossa vida social que não seja afetado por ela. Ela introduz novos padrões de comunicação social, quebra as barreiras linguísticas, e cria novas formas de expressões criativas - para citar apenas alguns dos seus efeitos. Hoje, a Internet é um fenômeno social tanto quanto um fenômeno tecnológico.

Direitos Humanos

O conjunto básico de direitos humanos relacionados à Internet inclui privacidade; liberdade de expressão; o direito de receber informações; vários direitos que protegem a diversidade cultural, linguística e de minorias; e o direito à educação. Não é de se estranhar que as questões relacionadas com os direitos humanos muitas vezes são discutidas com muita eloquência tanto na CMSI quanto no IGF. Embora os direitos humanos sejam geralmente abordados explicitamente, eles também estão presentes em questões transversais que aparecem quando se lida com a neutralidade da rede (direito de acesso, liberdade de expressão, anonimato), a cibersegurança (respeito aos direitos humanos durante a realização de atividades de segurança cibernética e de proteção), o controle do conteúdo, etc. As revelações de Snowden sobre a vigilância em massa desencadeou o processo diplomático sobre privacidade online no âmbito da Assembleia Geral das Nações Unidas e do Conselho de Direitos Humanos da ONU.

Os direitos humanos *online x offline*

O princípio de que os mesmos direitos humanos do qual as pessoas usufruem offline também devem ser protegidos online foi firmemente estabelecido pelas resoluções da Assembleia Geral da ONU e do Conselho de Direitos Humanos da ONU. A Associação para o Progresso das Comunicações (APC) na Carta dos Direitos da Internet argumenta que os direitos humanos relacionados à Internet estão fortemente incorporados no sistema de direitos humanos das Nações Unidas com base na Declaração Universal dos Direitos

Humanos (DUDH) e em outros instrumentos.[1] As especificidades dos direitos humanos online estão relacionadas a sua implementação.

DIREITO DE ACESSO À INTERNET

A Estônia foi o primeiro país a garantir juridicamente o direito de acessar a Internet por meio de uma legislação para serviços universais.[2] Desde julho de 2010 todos os cidadãos da Finlândia têm direito a uma conexão banda larga de um megabit.[3] No entanto, o direito de acessar a Internet é discutido mais no sentido da liberdade de expressão e informação do que propriamente da velocidade de conexão da Internet. As opiniões ainda são variadas com relação ao forte reconhecimento global do acesso à Internet como um direito humano, uma vez que este acesso envolve diferentes recursos – desde o acesso à infraestrutura até o acesso ao conteúdo – conforme indicado pelo relatório do Conselho de Direitos Humanos das Nações Unidas.[4]

Contudo, ainda existem opiniões que resistem a considerar a banda larga como um direito humano básico, quando ainda existem pessoas brigando por água limpa, cuidados médicos e alimentação. Isto diminuirá os esforços e os recursos despendidos com os direitos humanos mais básicos?

As atividades do Conselho da Europa referentes aos direitos humanos e à Internet

Um dos principais atores no campo dos direitos humanos e da Internet é o Conselho da Europa (CoE). O CoE é a instituição central dedicada

1 A APC Internet Rights Charter inclui acesso à Internet para todos; liberdade de expressão e associação; acesso à informação; educação e criação compartilhada - software livre e aberto e desenvolvimento de tecnologia; privacidade, vigilância e criptografia; governança da Internet; conscientização, proteção e realização de direitos. Acessível em <http://www.apc.org/en/node/5677> [acessado em 10 de agosto de 2014].

2 Borg-Psaila S (2011) Right to access the Internet: the countries and the laws that proclaim it. Acessível em <http://www.diplomacy.edu/blog/right-access-internet-countries-and- laws-proclaim-it> [acessado em 10 de agosto de 2014].

3 CNN Tech (2010) First nation makes broadband access a legal right. Acessível em <http://articles.cnn.com/2010-07-01/tech/finland.broadband_1_broadband-access-internet- access-universal-service?_s=PM:TECH> [acessado em 10 de agosto de 2014]. Nota do Tradutor: o endereço foi substituído por <http://edition.cnn.com/2010/TECH/web/07/01/finland.broadband/> [acessado em 7 de março de 2017].

4 Assembleia Geral das Nações Unidas (2011) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. Acessível em <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf> [acessado em 10 de agosto de 2014]. Para uma discussão sobre o relatório das Nações Unidas, ver Wagner A (2012) Is Internet access a human right? The Guardian. Acessível em <https://www.theguardian.com/law/2012/jan/11/is-internet-access-a-human-right> [acessado em 10 de agosto de 2014].

aos direitos humanos no âmbito pan-europeu, tendo a Convenção para a Proteção dos Direitos Humanos e Liberdades Fundamentais [5] como seu principal instrumento. Desde 2003, o Conselho da Europa adota diversas declarações destacando a importância dos direitos humanos na Internet.[6] Ele é também o depositário da Convenção sobre Crime Cibernético[7] como o principal instrumento global neste campo, o que pode posicioná-lo como uma das principais instituições na busca de equilíbrio justo entre os direitos humanos e considerações sobre cibersegurança no desenvolvimento futuro da Internet.

Liberdade de expressão e o direito de buscar, receber e transmitir informações

A liberdade de expressão online tem recebido destaque na agenda diplomática nos últimos anos; está na agenda do Conselho de Direitos Humanos da ONU. A liberdade de expressão na Internet também tem sido discutida em várias conferências internacionais, sendo que a discussão online a respeito é uma área política controversa. Trata-se de um dos direitos humanos fundamentais, geralmente aparecendo em destaque nas discussões sobre o controle de conteúdo e a censura. Na Declaração Universal dos Direitos Humanos da ONU,[8] a liberdade de expressão (artigo 19) é contrabalançada pelo direito do Estado de limitar a liberdade de expressão para o bem da moralidade, da ordem pública e do bem estar geral (artigo 29). Dessa forma, tanto a discussão quanto a implementação do artigo 19 devem ser colocadas no contexto do esta-

5 Conselho da Europa (2010) Convention for the Protection of Human Rights and Fundamental Freedoms. Acessível em <http://conventions.coe.int/treaty/en/treaties/html/005.htm> [acessado em 10 de agosto de 2014].

6 O Conselho da Europa adotou as declarações principais a seguir, relevantes para os direitos humanos e a Internet: The Declaration on Freedom of Communication on the Internet (28 de maio de 2003). Acessível em <https://wcd.coe.int/ViewDoc.jsp?id=37031> [acessado em 10 de agosto de 2014]; The Declaration of Human Rights and the Rule of Law in the Information Society (13 de maio de 2005). Acessível em <https://wcd.coe.int/ViewDoc.jsp?id=849061> [acessado em 10 de agosto de 2014]. The Declaration on the Digital Agenda for Europe (29 de setembro de 2010). Acessível em <https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Decl(29.09.2010_1)&Language=lanEnglish&Ver=original&direct=true> [acessado em 10 de agosto de 2014].

7 Conselho da Europa (2001) Convention on Cybercrime. Acessível em <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm> [acessado em 30 de abril de 2014].

8 Nações Unidas (sem data) The Universal Declaration of Human Rights. Acessível em <http://www.un.org/en/documents/udhr/> [acessado em 30 de abril de 2014].

belecimento de um equilíbrio adequado entre duas necessidades. Esta situação ambígua abre muitas possibilidades para diferentes interpretações de normas e, por fim, diferentes implementações. A controvérsia em torno do equilíbrio certo entre os artigos 19 e 29 no mundo real se reflete nas discussões sobre a realização deste equilíbrio na Internet.

A liberdade de expressão é a prioridade específica de ONGs de direitos humanos como a Anistia Internacional e a Freedom House. A Freedom House avalia o nível de liberdade na Internet e no telefone celular vivenciado por usuários comuns numa amostra de países de todo o mundo. O mais recente estudo observa que a liberdade na Internet no âmbito mundial está em declínio, com 34 de 60 países vivenciando uma trajetória negativa, impulsionada por grande vigilância, novas leis que controlam o conteúdo da Web e detenções crescentes de usuários de mídia social. No entanto, o estudo também observa que os ativistas estão se tornando mais eficazes na conscientização de ameaças emergentes e, em vários casos, têm ajudado a evitar novas medidas repressivas.[9]

Direitos das pessoas com deficiência[10]

De acordo com estimativas das Nações Unidas, há um bilhão de pessoas com deficiência no mundo.[11] Os fatores que contribuem para o aumento deste número incluem a guerra e a destruição por causas naturais e humanas; a pobreza e condições de vida insalubres; e a falta de conhecimento sobre a deficiência, as suas causas, prevenção e tratamento.

A Internet oferece novas possibilidades para a inclusão social das pessoas com deficiência. A fim de maximizar as possibilidades tecnológicas para pessoas com deficiência, há a necessidade de desenvolver a governança da Internet e o necessário quadro de políticas. O principal instrumento internacional neste campo é a Convenção sobre os Direitos de Pessoas com Deficiências,[12] ado-

9 Freedom House (2013) Freedom on the Net. A Global Assessment of Internet and Digital Media. Acessível em <http://freedomhouse.org/report/freedom-net/freedom-net-2013#.Uz7L3VcZes1> [acessado em 4 de abril de 2014].

10 Comentários e contribuições valiosos foram dados por Jorge Plano

11 UN Enable (sem data) Factsheet on Persons with Disabilities. Acessível em <http://www.un.org/disabilities/default.asp?id=18> [acessado em 4 de abril de 2014]

12 Convention on the Rights of Persons with Disabilities. Acessível em <http://www.un.org.disabilities/default.asp?navid=14&pid=150> [acessado em 30 de abril 2014]. Nota do Tradutor: o endereço foi substituído por <https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html> [acessado em 7 de março de 2017].

tada pela ONU em 2006 e assinada por 159 países (abril de 2014), estabelecendo os direitos que estão atualmente sendo incluídos na legislação nacional, o que irá torná-los aplicáveis.

A conscientização da necessidade de oferecer soluções tecnológicas que incluam pessoas com deficiência está aumentando com o trabalho das organizações que ensinam e incentivam o apoio à comunidade de portadores de deficiência, como a Coligação Dinâmica em Acessibilidade e Deficiência do IGF,[13] o Departamento de Deficiências e Necessidades Especiais da Internet Society,[14] e o International Center for Disability Resources on the Internet.[15]

A falta de acessibilidade é oriunda da lacuna entre as capacidades necessárias para o uso de hardware, software e conteúdo e as capacidades apresentadas pela pessoa com deficiência. Para diminuir esta lacuna, há dois caminhos a seguir para as ações de políticas:

- Incluir normas de acessibilidade nos requisitos para a concepção e o desenvolvimento de equipamentos, software e conteúdo.
- Fomentar a presença de acessórios em hardware e software que aumentem ou substituam as capacidades funcionais da pessoa.

No campo da governança da Internet, o foco principal é o conteúdo da Web, uma vez que está em rápido desenvolvimento e constitui um espécie de infraestrutura. Muitos aplicativos Web não cumprem as normas de acessibilidade devido à falta de conscientização ou à percepção da complexidade e dos altos custos envolvidos (o que hoje está longe de ser uma realidade). As normas internacionais de acessibilidade Web são concebidas pelo W3C dentro de sua Iniciativa de Acessibilidade Web.[16]

Políticas de conteúdo

Uma das principais questões socioculturais é a política de conteúdo, muitas vezes abordada do ponto de vista dos direitos humanos (liberdade de expressão e o direito de se comunicar), do governo (controle de conteúdo) e da tecnologia (ferramentas para controle de conteúdo). As discussões geralmente se concentram em três grupos de conteúdo.

13 IGF, Dynamic coalition on accessibility and disability. Acessível em <http://www.intgovforum.org/cms/index.php/dynamic-coalitions/80-accessibility-and-disability> [acessado em 30 abril de 2014

14 ISOC Disability and Special Needs Chapter. Acessível em <http://www.isocdisab.org/> [acessado em 30 de abril de 2014].

15 ICDRI. Acessível em <http://www.icdri.org/> [acessado em 30 de abril de 2014]

16 WAI. Acessível em <http://www.w3.org/WAI/> [acessado em 30 de abril de 2014].

- Conteúdo com consenso global para o seu controle. Incluem-se aqui a pornografia infantil, [17] justificativa de genocídio e incitamento ou organização de atos terroristas.
- Conteúdo sensível para países, regiões ou grupos étnicos específicos devido aos seus valores religiosos e culturais particulares. A comunicação globalizada online apresenta desafios para valores locais, culturais e religiosas em muitas sociedades. A maior parte do controle de conteúdo no Oriente Médio e países asiáticos é justificada oficialmente pela proteção de valores culturais específicos. Isso geralmente significa que o acesso a sites pornográficos ou de apostas é bloqueado.[18]
- Censura política na Internet. Os Repórteres sem Fronteiras emitem relatórios anuais sobre a liberdade de informação na Internet. Até 2012, o relatório costumava listar os países com programas de censura e vigilância. O Relatório de 2014 concentra-se em instituições que executam atividades de censura e vigilância.[19]

De que forma as políticas de conteúdo são conduzidas

Um menu à la carte para as políticas de conteúdo contém as seguintes opções jurídicas e técnicas, que são usadas em diferentes combinações.

Filtragem governamental de conteúdo

Os governos que filtram o acesso ao conteúdo geralmente criam um Índice de Internet de sítio web bloqueados para acesso dos cidadãos à Internet. Em termos técnicos, a filtragem utiliza principalmente o bloqueio de IP com base em roteador, servidores proxy, e redirecionamento de DNS. [20] A filtragem de conteúdo é realizada em muitos países. Além dos países geralmente associa-

17 Zick T (1999) Congress, the Internet, and the intractable pornography problem: the Child Online Protection Act of 1998, Creighton Law Review, 32, pp. 1147, 1153, 1201. Acessível em <http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1873&context=facpubs> [acessado em 2 de abril de 2014].

18 Para uma discussão sobre jogos de aposta na Internet, ver: Girdwood S (2002) Place your bets ... on the keyboard: Are Internet casinos legal? Campbell Law Review 25. Acessível em <http://scholarship.law.campbell.edu/cgi/viewcontent.cgi?article=1398&context=clr> [acessado em 2 de abril de 2014]

19 Repórteres sem Fronteiras (2014). Enemies of the Internet. Acessível em <http://12mars.rsf.org/wpcontent/uploads/EN_RAPPORT_INTERNET_BD.pdf> [acessado em 10 de agosto de 2014]

20 A OpenNet Initiative documentou a filtragem de rede da Internet pelos governos nacionais em mais de 40 países em todo o mundo. Ver Noman H and York J (2011) West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011 OpenNet Initiative Bulletin. Acessível em <http://opennet.net/west-censoring-east-the-use- western-technologies-middle-east-censors-2010-2011> [acessado em 2 de abril de 2014]

dos a estas práticas, como a China, a Arábia Saudita e Cingapura, outros países estão adotando cada vez mais a prática.

Classificação privada e sistemas de filtragem

Confrontado com o risco potencial da desintegração da Internet por meio do desenvolvimento de diversas barreiras nacionais (sistemas de filtragem), o W3C e outras instituições na mesma linha tomaram medidas pró-ativas propondo a implementação de sistemas de classificação e filtragem controlados pelo usuário.[21] Nestes sistemas, mecanismos de filtragem podem ser implementados por software em computadores pessoais ou na camada do servidor que controla o acesso à Internet.[22]

Filtragem de conteúdo com base na localização geográfica

Outra solução técnica relacionada ao conteúdo é o software de geolocalização, que filtra o acesso a determinado conteúdo privado da Web de acordo com a origem geográfica ou nacional de usuários. O processo referente ao Yahoo! foi importante neste sentido, uma vez que o grupo de especialistas envolvidos, incluindo Vint Cerf, indicou que em 70-90% dos casos o Yahoo! era capaz de determinar se as seções de um de seus sítio web de hospedagem de objetos nazistas eram acessadas a partir da França. [23] Esta avaliação ajudou o tribunal a tomar uma decisão final, na qual solicitou que o Yahoo! filtrasse o acesso da França aos objetos nazistas. Desde o processo de 2000 envolvendo o Yahoo!, a precisão de geolocalização aumentou ainda mais por meio do desenvolvimento de software de geolocalização altamente sofisticado.

Controle de conteúdo por meio de motores de busca

A ponte entre o usuário final e o conteúdo da Web costuma ser o motor de busca. A filtragem de pesquisas foi fonte de tensão entre o Google e autoridades chinesas[24], que culminou com a decisão tomada pelo

21 O PICS foi substituído pelo POWDER: <http://www.w3.org/2009/08/pics_superseded.html> Informações sobre o POWDER estão disponíveis em <http://www.w3.org/standards/techs/powder#w3c_all> [acessado em 10 August 2014]

22 Para um panorama dos tipos de filtragem disponíveis, ver a página da National Academy of Sciences, acessível em <http://www.nap.edu/netsafekids/pro_fm_filter.html> [acessado em 2 de abril de 2014].

23 Apesar de Vint Cerf ter participado do painel, contestou o relatório final, que ele afirmou "não ter focado nas falhas ou nas implicações mais amplas da implementação de gates online". Fonte: Guernsey L (2001) Welcome to the world wide web, passport, please? New York Times, 15 de março de 2001. Acessível em <http://www.nytimes.com/2001/03/15/technology/welcome-to-the-web-passport-please.html?pagewanted=all&src=pm> [acessado em 2 de abril de 2014].

24 Knight W (2002) On-off access for Google in China. New Scientist Internet edition, 13 de setembro. Acessível em <http://www.newscientist.com/article/dn2795-onoff-access- for#.U-fUu2PCfMU> [acessado em 8 de agosto de 2014]

Google em janeiro de 2010 de redirecionar as pesquisas realizadas no Google.cn aos seus servidores baseados em Hong Kong. No entanto, mais tarde naquele ano, o Google voltou atrás em sua decisão, pressionado pela recusa por parte do governo chinês de renovar sua licença de Internet Content Provider.[25]

O risco da filtragem de resultados de pesquisa, no entanto, não vem somente da esfera governamental; interesses comerciais podem interferir também, de forma mais ou menos óbvia ou difusa. Comentaristas começaram a questionar o papel dos motores de busca (o Google mais especificamente, considerando sua posição dominante na preferência dos usuários) na mediação do acesso do usuário à informação e para alertar sobre o seu poder de influenciar o conhecimento e as preferências dos usuários.[26]

Desafio da Web 2.0: usuários na qualidade de colaboradores

Com o desenvolvimento das plataformas Web 2.0 - blogs, sítio web de compartilhamento de documento, fóruns e mundos virtuais - a diferença entre o usuário e o criador ficou indefinida. Os internautas podem criar grandes pedaços de conteúdo da Web, como blogs, vídeos e galerias de fotos. Identificar, filtrar e rotular sítio web "inadequados" está se tornando uma atividade complexa. Enquanto técnicas automáticas de filtragem para textos são bem desenvolvidas, o reconhecimento automático, a filtragem e a rotulagem de conteúdo visual ainda estão no início do seu desenvolvimento.[27]

Uma abordagem utilizada em algumas ocasiões no Marrocos, Paquistão, na Turquia e Tunísia, é bloquear o acesso ao YouTube e ao Twitter em todo o país. Esta abordagem maximalista, contudo, resulta no bloqueio de conteúdo adequado, inclusive material didático. Durante os eventos da Primavera Árabe, os governos tomaram como medida extrema cortar o acesso à Internet completamente, a fim de dificultar a comunicação através das plataformas de redes sociais.[28]

25 Drummond D (2010) An update on China, 28 de junho de 2010. The Official Google Blog. Acessível em <http://googleblog.blogspot.com/2010/06/update-on-china.html> [acessado em 2 de abril de 2014]

26 Um bom ponto de partida para este debate é o post no blog de Mary Murphy sobre o blog de Governança da Internet da DiploFoundation e os comentários surgidos a partir dele: Google...stop thinking for me! Acessível em <http://www.diplomacy.edu/blog/googlestop-thinking-me> [acessado em 10 de abril de 2012].

27 Jiang Y (2011) Consumer Video Understanding: A Benchmark Database and An Evaluation of Human and Machine Performance ICMR'11. 17-20 de abril, Trento, Itália. Acessível em <http://www.ee.columbia.edu/~yjiang/publication/icmr11-consumervideo.pdf> [acessado em 2 de abril de 2012].

28 Crete-Nishihata M and York J (2011) Egypt's Internet Blackout: Extreme Example of Just-in-time Blocking. OpenNet Initiative. Acessível em <https://opennet.net/blog/2011/01/egypt%E2%80%99s-internet-blackout-extreme-example-just-time-blocking>

A necessidade de haver um quadro jurídico adequado

O vácuo jurídico no campo das políticas de conteúdo concede aos governos altos níveis de poder discricionário para decidir qual conteúdo deve ser bloqueado. Como as políticas de conteúdo são uma questão delicada para todas as sociedades, a adoção de instrumentos jurídicos é vital. A regulamentação nacional em matéria de política de conteúdos pode proporcionar uma melhor proteção dos direitos humanos e resolver os papéis às vezes ambíguos dos ISPs, dos órgãos de aplicação da lei e de outros atores. Nos últimos anos, muitos países implementaram uma legislação de políticas de conteúdo.

Iniciativas internacionais

No âmbito internacional, as principais iniciativas surgem em países europeus com legislação forte no campo do discurso do ódio, inclusive o antirracismo e o antissemitismo. Instituições regionais europeias tentaram impor estas regras no ciberespaço. O principal instrumento jurídico a abordar a questão do conteúdo foi o Protocolo Adicional à Convenção sobre Crime Cibernético do CoE,[29] referente à criminalização dos atos de natureza racista e xenófoba cometidos por meio de sistemas informatizados (2003). Em um nível mais prático, a UE implementou o programa Para uma Internet mais segura da UE, que inclui os principais pontos a seguir:

- Criação de uma rede europeia de linhas diretas para denunciar conteúdo ilegal.
- Incentivo à autorregulação.
- Desenvolvimento de classificação de conteúdo, filtragem e filtragem padrão.
- Desenvolvimento de software e serviços.
- Ações de conscientização para a utilização segura da Internet.[30]

A Organização para a Segurança e Cooperação na Europa (OSCE) também atua neste campo. Desde 2003, ela organiza uma série de conferências e reuniões com foco específico na liberdade de expressão e na potencial utilização inadequada da Internet (por exemplo, propaganda racista, xenófoba e antissemita).

[acessado em 2 de abril de 2014]

29 Conselho da Europa (2003) Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Acessível em <http://conventions.coe.int/Treaty/en/Treaties/html/189. htm> [acessado em 30 de abril de 2014].

30 EU Information Society (sem data) Safer Internet action plan. Acessível em <http:/ec.europa.eu/information_society/activities/sip/index_en.htm> [acessado em 8 de agosto de 2014].

Questões

Controle de conteúdo x liberdade de expressão

Quando se trata de controle de conteúdo, o outro lado da questão é frequentemente a restrição à liberdade de expressão. Isto é especialmente importante nos EUA, onde a Primeira Emenda garante ampla liberdade de expressão, até mesmo o direito de publicar materiais nazistas e de conteúdo similar.

A liberdade de expressão define em grande parte a posição dos EUA no debate internacional sobre questões relacionadas ao conteúdo na Internet. Por exemplo, embora os EUA assinem a Convenção sobre Crime Cibernético, o país não pode assinar o Protocolo Adicional a esta convenção, que trata do discurso do ódio e controle de conteúdo. A questão da liberdade de expressão também foi levantada no contexto do processo judicial do Yahoo!. Em suas iniciativas internacionais, os EUA não ultrapassam a linha que pode pôr em risco a liberdade de expressão, conforme estipulada na Primeira Emenda.

Ilegal offline – ilegal online

Tal como acontece com os direitos humanos, a visão dominante é que as regras do mundo offline se aplicam à Internet quando se trata de políticas de conteúdo.

Um dos argumentos da abordagem cibernética à regulação da Internet é que a quantidade (intensidade de comunicação, número de mensagens) apresenta diferença qualitativa. De acordo com este ponto de vista, o problema do discurso do ódio não é que não há regulação contra ele, mas que o compartilhamento e a divulgação por meio da Internet o torna um tipo diferente de problema jurídico. Mais indivíduos são expostos e é difícil fazer cumprir as regras existentes. Portanto, a diferença suscitada pela Internet está principalmente relacionada a problemas de cumprimento das regras, e não às regras em si.

A efetividade do controle de conteúdo

Nas discussões sobre as políticas de Internet, um dos principais argumentos é que a natureza descentralizada da Internet consegue driblar a censura. Em países com controle de conteúdo administrado pelo governo, usuários com habilidades técnicas têm encontrado uma maneira de driblar esse controle. No entanto, o controle de conteúdo não se destina a este pequeno grupo de usuários com habilidades técnicas; destina-se à população em geral. Lessig faz uma afirmação concisa sobre o problema: "A regulação

não precisa ser completamente eficiente para ser considerada suficientemente eficiente".[31]

Quem deve ser responsável pelas políticas de conteúdo?

Os principais atores na área de controle de conteúdo são parlamentos e governos. Eles prescrevem o conteúdo a ser controlado e a forma de controle. Os ISPs, na qualidade de gateways de Internet, são normalmente considerados responsáveis pela execução da filtragem de conteúdo, conforme as prescrições do governo ou conforme a autorregulação (pelo menos com relação a questões de consenso geral, como a pornografia infantil). Alguns grupos de usuários, tais como os pais, estão ansiosos pela implementação de uma política de conteúdo mais eficiente para proteger as crianças. Diversas iniciativas de classificação ajudam os pais a encontrar conteúdo adequado para as crianças. Novas versões de software de navegador de Internet costumam incluir inúmeras opções de filtragem. As empresas privadas e universidades também fazem controle de conteúdo. Em alguns casos, o conteúdo é controlado através de pacotes de software; por exemplo, o movimento da Cientologia distribui um pacote de software, o Scienositter, para seus membros, impedindo o acesso a sítio web com críticas à Cientologia.[32]

Educação

A Internet abriu novas possibilidades para a educação. Várias iniciativas de ciberaprendizagem, educação online e ensino à distância foram implementadas; o principal objetivo destas iniciativas é usar a Internet como um meio para a realização de cursos. Embora não se possa substituir o ensino tradicional, a educação online oferece novas possibilidades para a aprendizagem, especialmente quando restrições de tempo e espaço impossibilitam a presença física em sala de aula.

Tradicionalmente, a educação tem sido regulada por instituições nacionais. O credenciamento de instituições de ensino, o reconhecimento das qualificações e garantia de qualidade são todos regulados no âmbito nacional. No entanto, a educação transnacional requer o desenvolvimento de novos sistemas de governança. Muitas iniciativas internacionais visam preencher a lacuna de governança, especialmente em áreas como a garantia da qualidade e o reconhecimento da formação acadêmica.

31 Lessig L (1996) The Zones of Cyberspace. Stanford Law Review 48 pp. 1403, 1405

32 Steve A (sem data) Church of Scientology censors net access for members. Acessível em <http://www.xenu.net/archive/events/censorship> [acessado em 2 de abril de 2012].

Questões

A OMC e a educação

Uma questão polêmica nas negociações da OMC é a interpretação dos Artigos I (3)b e (3)c do GATS,[33] que especificam exceções ao regime de comércio livre para serviços fornecidos pelo governo. De acordo com determinado ponto de vista, apoiado principalmente pelos EUA e pelo Reino Unido, estas exceções devem ser tratadas com ressalvas, de facto permitindo o livre comércio no ensino superior. Este ponto de vista é predominantemente baseado nos interesses do setor educacional de língua inglesa para expandir sua cobertura global do mercado de educação, tendo recebido forte resistência de muitos países.[34]

O próximo debate, que provavelmente se desenvolverá no âmbito da OMC e de outras organizações internacionais, priorizará o dilema da educação como mercadoria ou bem público. Se a educação for considerada uma mercadoria, as regras de livre comércio da OMC serão implementadas neste campo também. Se ela for considerada um bem público, por outro lado, preservará o atual modelo de educação em que as universidades públicas possuem status especial como instituições de importância para a cultura nacional.

Garantia de qualidade

A disponibilidade dos sistemas de educação online e a fácil entrada neste mercado levantaram a questão da garantia da qualidade. O foco na realização de cursos online pode ignorar a importância da qualidade dos materiais e da didática. Inúmeras possíveis dificuldades podem colocar em risco a qualidade da educação. Uma delas é a entrada fácil no mercado de novas instituições educacionais de fins comerciais, que frequentemente possuem poucas das capacidades acadêmicas e didáticas necessárias. Outro problema relacionado à garantia de qualidade é que a simples transferência de materiais impressos existentes para um meio online implica no aproveitamento do potencial didático do novo meio. Este aspecto levou as organi-

33 GATS. Acessível em <http://www.wto.org/english/res_e/booksp_e/analytic_index_egats_01_e.htm#article1A> [acessado em 30 de abril de 2014]. Nota do Tradutor: o endereço foi substituído por <https://www.wto.org/english/docs_e/legal_e/26-gats.pdf> [acessado em 7 de março de 2017].

34 Para um estudo abrangente da interpretação do GATS relacionado à educação superior, ver Tilak J (2011) Trade in higher education: The role of the General Agreement on Trade in Services (GATS). UNESCO: International Institute for Educational Planning, Paris. Acessível em <http://unesdoc.unesco.org/images/0021/002149/214997e.pdf> [acessado em 3 de abril de 2014]

zações educacionais a começar a elaborar normas e diretrizes para avaliar a concepção e o conteúdo de palestras realizadas online.[35]

O reconhecimento da formação acadêmica e a transferência de créditos

O reconhecimento de diplomas se tornou uma questão particularmente relevante no ambiente da educação online. Quando se trata da educação online, o principal desafio é o reconhecimento da formação acadêmica para além do contexto regional, principalmente no âmbito global.

A UE elaborou um quadro regulatório por meio do Sistema Europeu de Transferência e Acumulação de Créditos (European Credit Transfer and Accumulation System - ECTS). [36] A região da Ásia-Pacífico implementou seu próprio modelo regional para o intercâmbio de estudantes e um sistema de crédito relacionado – o programa Mobilidade Universitária na Ásia e no Pacífico (University Mobility in Asia and the Pacific - UMAP).[37]

Padronização da educação online

A fase inicial de desenvolvimento do projeto de educação online foi caracterizado pelo rápido desenvolvimento e pela grande diversidade de materiais, no sentido de plataformas, conteúdo e didática. No entanto, é necessário desenvolver padrões comuns a fim de facilitar o intercâmbio de cursos online e implementar certo padrão de qualidade. A maioria das padronizações é realizada nos EUA por instituições privadas e profissionais. Outras iniciativas, incluindo as internacionais, são realizadas em menor escala.

35 Para uma lista de exemplos de organizações e trabalhos que abordam as recomendações e os padrões da educação à distância, ver Bates T (2010) E-learning quality assurance standards, organizations and research. Acessível em <http://www.tonybates.ca/2010/08/15/e-learning-quality-assurance-standards-organizations-and-research/> [acessado em 3 de abril de 2014].

36 Comissão Europeia (sem data) ECTS. Acessível em <http://ec.europa.eu/education/tools/ects_en.htm (atenção para /> [acessado em 3 de abril 2014].

37 UMAP (sem data) UMAP. Acessível em <http://www.umap.org/en/cms/detailphp?id=106> [acessado em 3 de abril de 2014]. Nota do Tradutor: o endereço foi substituído por <http://umap.org/about/> [acessado em 7 de março de 2017].

Segurança das crianças no ambiente online[38]

As crianças sempre foram vulneráveis à vitimização. A maioria das questões relacionadas à segurança na Internet se refere principalmente aos jovens, especialmente aos menores de idade. No entanto, as linhas indefinidas costumam ganhar nitidez quando se trata da segurança das crianças. Os conteúdos reprováveis são aqueles claramente entendidos como abusivos e inadequados, sendo que incluem uma ampla variedade de materiais, entre os quais pornografia, ódio e violência, bem como conteúdos que implicam riscos à saúde, tais como conselhos sobre suicídio, anorexia e assuntos similares.

Questões

Ciberbullying

O assédio é uma ameaça específica quando o alvo são menores de idade, uma vez que eles são vulneráveis ao usar as diferentes ferramentas de comunicação tais como mensagens, salas de bate papo ou redes sociais. As crianças podem facilmente se tornar vítimas de ciberbullying, na maioria das vezes de seus pares usando TIC - combinando câmeras de telefones celulares, sistemas de compartilhamento de arquivos e redes sociais - como uma ferramenta conveniente.

Abuso e exploração sexual

O comportamento nocivo direcionado a menores de idade pode ser particularmente perigoso quando conduzido por adultos. Disfarçar a identidade é uma das abordagens mais frequentes realizadas por pedófilos na Internet – ao fingirem ser do mesmo grupo, estes predadores online coletam informações e manipulam constantemente a criança, conseguindo facilmente ganhar sua confiança, até mesmo com o objetivo de marcar um encontro presencial. A ação virtual, dessa forma, transforma-se em contato real, podendo gerar consequências tão extremas quanto o abuso e a exploração de crianças, pedofilia, o aliciamento de menores para exploração sexual e até mesmo o tráfico de crianças.

Jogos violentos

O impacto dos jogos violentos no comportamento dos jovens está sendo amplamente debatido. Os jogos mais detestáveis envolvem armas sofisticadas (com as funcionalidades de armas reais e/ou outros recursos fantasiosos) e derramamento de sangue, e geralmente são

38 Este texto foi elaborado por Vladimir Radunovic para o curso temático avançado sobre Cibersegurança (Internet Governance Capacity Building Programme – DiploFoundation).

rotulados como "aliviadores de estresse". O dez jogos mais vendidos para diferentes plataformas de hardware, entre os quais o Microsoft Xbox, o Nintendo DS, o Nintendo Wii, PC, Playstation, são majoritariamente jogos de ação/violentos.[39]

Combate às ameaças

O grande desafio que os educadores e os pais estão enfrentando para proteger as crianças no mundo virtual é o fato de que os "nativos digitais" têm muito mais conhecimento sobre a forma de usar as TIC - eles sabem mais do que seus pais, porém entendem menos. A estreita cooperação entre pares - pais, educadores e a comunidade - é mais importante para o desenvolvimento de iniciativas para proteger as crianças em ambientes informatizados.

Para aumentar a conscientização entre as partes interessadas, a Comissão Europeia lançou o projeto InSafe [40] como uma rede europeia de nodos para a conscientização da segurança na Internet, fornecendo materiais de conscientização para pais e educadores em diversas línguas, gratuitos para download e divulgação. A campanha de mídia polonesa sobre ciberbullying resultou em um conjunto de vídeos e em um curso à distância sobre segurança na Internet para crianças. A iniciativa NetSafe na Nova Zelândia, fundada em 1998, é uma das primeiras iniciativas nacionais em matéria de segurança na Internet que reúne as principais partes interessadas, entre as quais ministérios, o setor empresarial e a mídia.

Um passo muito necessário para além da conscientização e da formação dos jovens, pais e educadores é a capacitação na área de segurança na Internet, voltada para o grupo multissetorial de formuladores de políticas: servidores públicos, empresas, mídia, universidades, centros de estudo, organizações não governamentais, etc. Várias organizações internacionais estão discutindo possíveis modelos de cooperação para criar programas, entre eles o CoE, a UIT, o CPI e a DiploFoundation.

Em períodos mais longos, faz-se necessário atualizar os currículos educacionais, para incluir programas nas próprias escolas sobre as questões de segurança na Internet, tais como a proteção à privacidade e à segurança pessoal, o cuidado à reputação pessoal e à reputação

39 Reilly J (2012) The Best-Selling U.S. Games Of 2011. gameinformer. Acessível em <http://www.gameinformer.com/b/news/archive/2012/01/12/these-are-the-10-best-selling-u-s- games-in-2011.aspx> [acessado em 12 de abril de 2014].

40 Insafe. Acessível em <http://www.saferinternet.org/web/guest/home> [acessado em 30 de abril de 2014].

de terceiros, a ética, a transferência de exemplos morais e de competências da vida real para o mundo virtual, etc. Existem inúmeras iniciativas como estas em todo o mundo, tais como Cyber Smart!,[41] iKeepSafe,[42] i-Safe,[43] e NetSmartz.[44]

Os mecanismos jurídicos e de políticas nacionais e internacionais sincronizados também são componentes indispensáveis. Um exemplo é a Prague Declaration for a Safer Internet for Children, exitosa declaração pan-europeia adotada na Conferência Ministerial (Praga, abril de 2009).[45] A Agenda Global de Cibersegurança (GCA)[46] apresenta a iniciativa Proteção Online de Crianças (Child Online Protection - COP), como parte integrante da referida agenda. Há muitos outros fóruns internacionais nos quais a proteção da criança é uma questão de alta prioridade nos debates, inclusive o IGF com sua Coalizão Dinâmica de Segurança Online da Criança (Dynamic Coalition on Child Online Safety) .

A cooperação internacional no âmbito da proteção das crianças tem sido exitosa há um bom tempo na área de emergência e linhas diretas internacionais. Algumas destas iniciativas bem sucedidas:

- A cooperação oficial COSPOL Internet Related Child Abusive Material Project (CIRCAMP) iniciada pelo Chefe Europeu da Força Tarefa Policial (Police Task Force).
- Trabalhos de ONGs em cooperação com governos, por exemplo, Internet Watch Foundation, Perverted Justice Foundation, The International Centre for Missing & Exploited Children, ECPAT International, Save the Children e Child Exploitation and Online Protection Centre.
- Parcerias público-privadas como a cooperação entre a Telecom da Noruega e a Polícia da Noruega.

41 CyberSmart. Acessível em <http://www.cybersmart.org/> [acessado em 30 de abril de 2014
42 IKeepSafe. Acessível em <http://www.ikeepsafe.org/> [acessado em 30 de abril de 2014].
43 I-Safe. Acessível em <http://www.isafe.org/> [acessado em 30 de abril de 2014
44 NetSmartz. Acessível em <http://www.netsmartz.org/Parents> [acessado em 30 de abrilde 2014].
45 EU2009. Prague Declaration for a Safer Internet for Children. Acessível em <http://ec.europa.eu/information_society/activities/sip/docs/events/prague_decl.pdf> [acessado em30 de abril de 2014]
46 UIT (sem data) Global Cybersecurity Agenda. Acessível em < http://www.itu.int/osg/csd/cybersecurity/gca> [acessado em 30 de abril de 2014].

Multilinguismo e diversidade cultural

Desde seus primeiros dias, a Internet tem sido um meio cujo idioma predominante é o inglês. De acordo com algumas estatísticas, aproximadamente 56% do conteúdo da Web está em inglês, [47] ao passo que 75% da população mundial não fala este idioma.[48] Esta situação levou muitos países a tomar medidas combinadas de promoção do multilinguismo e proteção da diversidade cultural. A promoção do multilinguismo não se resume a uma questão cultural; ela está diretamente relacionada à necessidade de aprofundar o desenvolvimento da Internet. [49] Se a Internet for para ser utilizada por mais partes da sociedade e não apenas pelas elites nacionais, o conteúdo deve ser acessível em mais idiomas.

Questões

Alfabetos não romanos

A promoção do multilinguismo requer normas técnicas que facilitem a utilização de alfabetos não romanos. Uma das primeiras iniciativas relacionadas à utilização multilíngue de computadores foi realizada pela Unicode Consortium – instituição sem fins lucrativos que cria padrões para facilitar o uso de conjuntos de caracteres para idiomas diferentes.[50] Por sua vez, a ICANN e a IETF deram um passo importante na promoção de Nomes de Domínios Internacionais (Internationalised Domain Names - IDN). A IDN facilita a utilização de nomes de domínio escritos em chinês, árabe e outros alfabetos não latinos.

Tradução automática

Houve bastante esforço para melhorar a tradução automática. Dada a sua política de traduzir todas as atividades oficiais para os idiomas de todos os estados-membros, a UE apoiou várias atividades de desenvolvimento no campo da tradução automática. Apesar de grandes avanços realizados, ainda existem limitações.

47 W3Techs (2014) Usage of content languages for websites. Acessível em <http:/w3techs.com/technologies/overview/content_language/all> [acessado em 3 de abril de 2014]

48 British Council (sem data) How many people speak English. Acessível em <http://www.britishcouncil.org/learning-faq-the-english-language.htm> [acessado em 10 de agosto de 2014].

49 Para mais informações relacionadas ao multilinguismo na Internet, consultar o estudo a seguir: AlShatti Q, Aquirre R and Cretu V (2007) Multilingualism – the communication bridge. DiploFoundation's Internet Governance Research Project, 2006/2007. Acessível em <http://textus.diplomacy.edu/thina/TxFsetW.asp?tURL=http://textus.diplomacy.edu/thina/txgetxdoc.asp?IDconv=3241> [acessado em 3 de abril de 2014].

50 Unicode Consortium. Acessível em <http://unicode.org/> [acessado em 30 de abril de 2014].

Estruturas governamentais apropriadas

A promoção do multilinguismo requer estruturas de governança adequadas. O primeiro elemento dos regimes de governança foi fornecido por organizações como a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), que tem incentivado muitas iniciativas com enfoque no multilinguismo, entre as quais a adoção de documentos importantes, como a Declaração Universal sobre Diversidade Cultural.[51] Outro promotor importante do multilinguismo é a UE, uma vez que engloba o multilinguismo como um dos seus princípios políticos e operacionais básicos.[52]

A evolução e ampla utilização de ferramentas Web 2.0, que possibilitam aos usuários comuns se tornarem colaboradores e desenvolvedores de conteúdo, oferece oportunidade para uma maior disponibilidade de conteúdo local em uma ampla variedade de idiomas. No entanto, sem um quadro mais amplo para a promoção do multilinguismo, a oportunidade pode acabar aprofundando a defasagem, uma vez que os usuários sentem a pressão para utilizar a linguagem comum a fim de atingir um público mais amplo.

Bens públicos globais

O conceito de bens públicos globais pode estar ligado a muitos aspectos da governança da Internet. As conexões mais diretas são encontradas nas áreas de acesso à infraestrutura de Internet, proteção do conhecimento desenvolvido por meio da interação na Internet, proteção das normas técnicas públicas e acesso à educação online.

As empresas privadas predominantemente operam a infraestrutura da Internet. Um dos desafios é a harmonização da propriedade privada da infraestrutura Internet com o status da Internet de público global. As legislações nacionais preveem a possibilidade de a propriedade privada ser restrita por certos requisitos públicos, entre os quais a concessão de direitos iguais a todos os potenciais usuários e a não interferência no conteúdo transportado.

Uma das principais características da Internet é que através da interação mundial de usuários, novos conhecimentos e informações são produzidos. Construiu-se conhecimento considerável através de intercâmbios em listas de discussão, redes sociais e blogs. Exceto pelo

51 UNESCO (2001) Universal Declaration on Cultural Diversity. Acessível em <http://portal.unesco.org/en/ev.php-URL_ID=13179&URL_DO=DO_TOPIC&URL_SECTION=201.html> [acessado em 30 de abril de 2012]

52 Comissão Europeia (sem data) Languages. Acessível em <http://ec.europa.eu/languages/index_en.htm> [acessado em 10 de agosto de 2014]

Creative Commons,[53] não existe nenhum mecanismo para facilitar o uso legal de tal conhecimento. Apresentando incerteza jurídica, pode ser modificado e comercializado. Esta base comum de conhecimento, uma base importante de criatividade, corre o risco de se esgotar. Quanto mais o conteúdo da Internet é comercializado, menos espontâneas são as trocas, podendo levar a uma menor interação criativa. O conceito de bens públicos globais, combinado com iniciativas como o Creative Commons, poderia oferecer soluções que tanto protegeriam o ambiente criativo atual da Internet quanto preservariam o conhecimento construído na Internet para gerações futuras.

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

Questões

O equilíbrio entre interesses privados e públicos

Um dos desafios subjacentes ao futuro desenvolvimento da Internet é encontrar um equilíbrio entre interesses privados e públicos. A questão é como oferecer ao setor privado um ambiente comercial adequado, assegurando simultaneamente o desenvolvimento da Internet como um bem público global. Em muitos casos, não é um jogo onde há perdedores, mas sim uma situação onde todos ganham. O Google e muitas outras empresas da Web 2.0 vêm tentando desenvolver modelos de negócios que gerem renda e possibilitem o desenvolvimento criativo da Internet.

Proteção da Internet como bem público global[54]

Algumas soluções podem ser desenvolvidas com base em conceitos econômicos e jurídicos existentes. Por exemplo, a teoria econômica tem um conceito bem desenvolvido de bens públicos, ampliado no

53 A Creative Commons é uma organização sem fins lucrativos que desenvolve, apoia e administra a infraestrutura jurídica e técnica que maximiza a criatividade digital, o compartilhamento e a inovação. Acessível em <http://creativecommons.org/> [acessado em 3 de abril de 2014]

54 Para mais informações sobre a Internet como um bem público global, consultar o estudo a seguir: Seiiti A and Psaila S (2006) The Protection of the Public Interest with regards to the Internet. DiploFoundation's Internet Governance Research Project, 2005/2006. Acessível em <http://archive1.diplomacy.edu/poolbin.asp?IDPool=128> [acessado em 3 de abril de 2014].

âmbito internacional para bens públicos globais. Um bem público tem duas propriedades importantes: o consumo não competitivo e a não exclusão. O primeiro estipula que o consumo de um indivíduo não diminui o de outro; o segundo estipula que é difícil, ou até mesmo impossível, excluir uma pessoa de usufruir o bem público. Acesso a materiais baseados na Web e muitos outros serviços da Internet cumprem ambos os critérios.

Atores da governança da Internet

No momento, a governança da Internet envolve uma ampla variedade de atores ou partes interessadas, como são frequentemente chamados. Entre os atores da Internet estão governos nacionais, organizações internacionais, o setor empresarial, a sociedade civil e a comunidade técnica (conforme especificado no artigo 49 da Declaração da CMSI de Túnis de 2005). Enquanto a multissetorialismo é adotada como princípio, o debate principal é sobre o papel específico de cada ator, focando principalmente a relação entre atores estatais e não estatais.

QUAL É A DIFERENÇA ENTRE A GOVERNANÇA DA INTERNET E OUTROS PROCESSOS DE POLÍTICAS GLOBAIS?

Na governança da Internet, os governos tiveram que entrar em um sistema não governamental que já existia, construído em torno das instituições IETF, ISOC e ICANN. Em outras áreas relacionadas a políticas (ex., mudança climática, comércio, migração), tem sido o contrário. As negociações intergovernamentais tiveram que se abrir gradualmente a atores não governamentais. Desde a CMSI de 2003, a maior parte do tempo e da energia gastos com a governança da Internet tem sido dedicada à convergência entre regimes diplomáticos não governamentais e tradicionais. Essa convergência também tem sido a causa das principais controvérsias.

Governos

A última década - desde a introdução da governança da Internet na agenda diplomática mundial em 2003 - tem sido um processo de aprendizagem para muitos governos. Mesmo para os países grandes e ricos, lidar com questões de governança da Internet tem resultado em inúmeros desafios, como a administração da natureza multidisciplinar da governança da Internet (ou seja, aspectos tecnológicos, econômicos e sociais) e envolvimento de uma grande variedade de atores. Muitos governos tiveram de treinar funcionários simultaneamente, desenvolver políticas e participar ativamente de várias reuniões internacionais da Internet.

Coordenação nacional

Em 2003, no início do processo da CMSI, a maioria dos países abordou questões de governança da Internet por meio dos ministérios de

telecomunicações, geralmente aqueles que tinham sido responsáveis pelas relações com a UIT. Gradualmente, à medida que eles perceberam que a governança da Internet consistia em mais do que "fios e cabos", os governos começaram a incluir funcionários de outros ministérios, como os funcionários das áreas de relações exteriores, cultura, meios de comunicação e justiça.

O principal desafio para muitos governos tem sido desenvolver uma estratégia para reunir e coordenar efetivamente o apoio de atores não estatais, tais como universidades, empresas privadas e ONGs que muitas vezes têm o conhecimento necessário para lidar com as questões de governança da Internet. Nos anos após a CMSI de 2003, a maioria dos países grandes e médios do G20 conseguiu desenvolver capacidade institucional satisfatória para acompanhar as negociações globais de governança da Internet. Alguns deles, como o Brasil, desenvolveram uma estrutura nacional inovadora para acompanhar o debate sobre a governança da Internet, envolvendo ministérios de telecomunicações, o serviço diplomático, setor empresarial, a sociedade civil e as universidades.[1]

Coerência nas políticas

Dada a natureza multidisciplinar da governança da Internet e a grande diversidade de atores e fóruns políticos, é particularmente desafiador alcançar coerência nas políticas. Por exemplo, a questão da proteção e privacidade de dados é abordada sob as perspectivas dos direitos humanos, do comércio, da padronização e da segurança, entre outras. Alcançar coerência nas políticas no campo da governança da Internet requer uma forma flexível de coordenação de políticas, inclusive a comunicação horizontal entre os diferentes ministérios, o setor empresarial e outros atores.

1 O modelo brasileiro de gestão do nome de domínio do país é tido como exemplo de êxito da abordagem multissetorial. O órgão nacional responsável pelos domínios brasileiros – CGI – é aberto a todos os usuários, inclusive autoridades governamentais, o setor empresarial e a sociedade civil. O Brasil gradualmente estendeu este modelo a outras áreas da Governança da Internet, principalmente nos preparativos para o IGF 2007, sediado no Rio de Janeiro.

GEO-ESTRATÉGIA DOS CABOS E A (IN) COERÊNCIA DE POLÍTICAS

A Entente Anglo Francesa[2] foi estabelecida em 1904. Ao firmar cooperação estreita com a Alemanha, porém, o Ministério de Assuntos Telegráficos da França não seguiu a política externa do país. O principal objetivo desta ação era reduzir o domínio britânico sobre a geoestratégia para cabos e ao mesmo tempo instalar novos cabos telegráficos em cooperação com a Alemanha. O historiador francês Charles Lesage fez o seguinte comentário sobre esta (in)coerência das políticas adotadas: "A divergência prolongada entre os princípios gerais da diplomacia francesa e os procedimentos das políticas para telégrafos resultam, creio eu, do fato de que neste país cada ministério adota sua própria política externa: o Ministério de Relações Exteriores adota uma política, o Ministério das Finanças adota outra.... A Administração de Correios e Telégrafos também tem, ocasionalmente, uma política externa; conforme ocorreu, nestes últimos anos, sem ser inteiramente hostil à Inglaterra, demonstrou forte inclinação em direção à Alemanha."[3]

VER A SEÇÃO 2 PARA UMA DISCUSSÃO MAIS APROFUNDADA SOBRE A NEUTRALIDADE DA REDE

Além do desafio de gestão, a realização da coerência nas políticas é geralmente limitada pela existência de interesses concorrentes nestas mesmas políticas. Isto é especialmente válido em países com economias de Internet bem desenvolvidas e diversificadas. Por exemplo, a neutralidade da rede é uma das questões nas quais o governo dos EUA se envolveu, apresentando um equilíbrio delicado entre a indústria da Internet (Google, Facebook, Yahoo!), que defende a neutralidade da rede, e o setor de telecomunicações / entretenimento (Verizon e AT & T, lobby de Hollywood), que vê a neutralidade da rede como um obstáculo ao desenvolvimento de um novo modelo de negócios com base, por exemplo, em Internet(s) mais rápida (s) para fornecimento de conteúdos multimídia.

A importância das missões permanentes baseadas em Genebra

Para muitos governos, as suas missões permanentes em Genebra têm sido importantes ou até mesmo essenciais nos processos da CMSI e da governança da Internet. A maioria das atividades acon-

2 Géraud A (1954) The rise and fall of the Anglo-French Entente. Foreign Affairs. Acessível em <http://www.foreignaffairs.com/articles/71095/andre-geraud-pertinax/rise-and-fall-of-the-anglo-french-entente> [acessado em 15 de agosto de 2014].

3 Lesage C (1915) La rivalite franco-britannique. Les cables sous-marins allemands Paris. p.257–258; citado em: Headrick D (1991) The Invisible Weapon: Telecommunications and International Politics 1851–1945 Oxford: Oxford University Press. p. 110

teceu em Genebra, sede da UIT, que teve papel principal nos processos da CMSI. A primeira CMSI ocorreu em Genebra em 2003, onde todas as reuniões preparatórias foram realizadas, com exceção de uma, mantendo as missões permanentes do local diretamente envolvidas. Atualmente, a Secretaria do IGF tem sede em Genebra e a maioria das reuniões preparatórias do IGF é realizada na cidade. Para países grandes e desenvolvidos, as missões permanentes faziam parte da ampla rede de instituições e indivíduos que lidavam com os processos da CMSI e da governança da Internet. Para países pequenos e em desenvolvimento, as missões permanentes eram os principais atores, e em alguns casos os únicos, dos referidos processos. As questões de governança da Internet contribuíram para a agenda das missões frequentemente curtas e sobrecarregadas dos países em desenvolvimento. Em muitos casos, o mesmo diplomata tinha que realizar as tarefas associadas à CMSI, juntamente com outras questões, como direitos humanos, saúde, comércio e trabalho.

Posições dos governos

Estados Unidos

A Internet foi desenvolvida como parte de um projeto científico patrocinado pelo governo dos EUA. Desde a origem da Internet até hoje, o governo dos EUA participa da governança da Internet por meio de vários departamentos e agências; inicialmente, o Departamento de Defesa, depois, a National Science Foundation e, mais recentemente, o Departamento de Comércio. A FCC também desempenha um papel importante na criação do quadro regulatório da Internet.

Um elemento constante na participação do governo dos Estados Unidos é sua abordagem hands-off (não interventiva), sendo geralmente descrito como um "custodiante distante". O país define o quadro, ao mesmo tempo deixando a responsabilidade da governança da Internet para aqueles que trabalham diretamente com ela, principalmente a comunidade técnica. No entanto, o governo dos EUA interveio mais diretamente em algumas ocasiões, como ocorreu em meados dos anos 1990, quando o projeto CORE poderia ter movido o servidor raiz e a gestão da infraestrutura central da Internet dos EUA para Genebra. Este processo foi interrompido pela famosa (pelo menos na história da Internet) nota diplomática enviada pela Secretária de Estado Madeleine Albright ao Secre-

tário General da UIT.[4] Paralelamente à ação de interromper a iniciativa CORE, o governo dos EUA iniciou consultas que resultaram na criação da ICANN.

Em 2009, o Departamento de Comércio dos EUA emitiu a Afirmação de Compromissos[5] com o objetivo de sair da função de supervisor da ICANN. A próxima fase deste processo começou em 14 de março 2014, quando a NTIA iniciou o processo de análise da relação específica entre o Departamento de Comércio dos EUA e a ICANN.[6] O núcleo desta relação - supervisão da função da IANA - deve ser passado do governo dos EUA para algum outro compromisso global até 30 de setembro de 2015. O anúncio da NTIA estabelece requisitos nos quais a supervisão da função da IANA não pode ser passada para um órgão intergovernamental. O resultado deste processo influenciará o futuro papel dos Estados Unidos na governança global da Internet.

União Europeia

A União Europeia apresenta combinação única de hard power e soft power digitais para fazer avançar compromissos futuros de governança da Internet. O hard power digital da UE tem como base a atratividade de um rico mercado de 500 milhões de pessoas com alta penetração de Internet (73%).[7] Conforme mostra a concentração do lobby da indústria da Internet em Bruxelas, este tipo de hard power é relevante. Ao negociar com a UE sobre questões antimonopolistas e de proteção de dados, o Google e o Facebook, entre outros, negociam com o resto do mundo (os acordos da UE com a indústria da Internet muitas vezes inspiram outros países e regiões a tomar medidas semelhantes). Em uma situação em que, por exemplo, o Google controla mais de 90% do mercado europeu de buscas, a UE é a única instituição internacional que poderia

4 Crítica da Secretária de Estado dos Estados Unidos à UIT pela iniciativa: "sem autorização dos governos membros de realizar uma reunião global envolvendo gastos não autorizados com recursos e celebrando acordos internacionais". Citado em Drake W. (2004) Reframing Internet Governance Discourse: Fifteen Baseline Propositions, p. 9. Acessível em <http://www.un-ngls.org/orf/drake.pdf> [acessado em 14 de agosto de 2014].

5 ICANN (sem data) Affirmation of Commitments. Acessível em <https://www.icann.org/resources/pages/aoc-2012-02-25-en> [acessado em 15 de agosto de 2014].

6 ICANN (2014) Administrator of the Domain Name System launches global multistakeholder accountability process. Acessível em <https://www.icann.org/resources/press-material/release-2014-03-14-en> [acessado em 15 de agosto de 2014].

7 Internet World Stats (sem data) Internet usage in the European Union. Acessível em <http://www.internetworldstats.com/stats9.htm> [acessado em14 de agosto de 2014].

abordar de forma eficiente o risco de monopólio de mercado do Google.[8]

O soft power digital da UE se baseia em uma espécie de diplomacia aikido digital que transforma fraquezas em forças. Mais especificamente, a UE não possui nenhuma grande empresa de Internet desde que o Skype foi comprado pela Microsoft. Paradoxalmente, esta fraqueza pode ser transformada em força no âmbito da governança da Internet.

Sem ter que proteger os interesses econômicos da indústria da Internet, a UE tem mais liberdade para promover e proteger os interesses públicos (direitos do usuário, a inclusão, a neutralidade de rede). Desta forma, a UE pode se tornar a guardiã dos "usuários da Internet" e a promotora de um ambiente favorável para o crescimento da indústria da Internet na UE (e no mundo). A UE pode atingir ambos os objetivos éticos e estratégicos, o que frequentemente não é o caso na política internacional.

A abordagem da UE com relação ao desenvolvimento de diferentes alianças pautadas por temas começou a emergir. No CMTI-12, a Europa apoiou os EUA; embora nas discussões sobre o status da ICANN a UE frequentemente se alia aos BRICS e aos países em desenvolvimento. Em matéria de proteção e privacidade de dados, a posição da UE está mais próxima da posição dos países latino-americanos. Suíça e Noruega têm posição próxima à UE na maioria das questões de governança da Internet.

Brasil

O Brasil tem sido um dos países mais ativos na política digital global. Sendo um país democrático e em desenvolvimento com um ambiente digital vibrante, o Brasil tem um grande potencial para viabilizar o compromisso entre os dois campos no debate sobre a governança da Internet (intergovernamentais e não governamentais). Este papel se tornou evidente na sequência das revelações de Snowden, ocasião em que o Brasil teve forte ação diplomática. Em seu discurso na 68ª Sessão da Assembleia Geral das Nações Unidas, a presidente do Brasil, Dilma Rousseff, fez este pedido: " [as] Nações Unidas devem desempenhar um papel de liderança para regular a conduta dos Es-

8 Comissão UE (2013) Antitrust: Commission seeks feedback on commitments offered by Google to address competition concerns. European Commission – IP/13/371. Acessível em <http://europa.eu/rapid/press-release_IP-13-371_en.htm> [acessado em 15 de agosto de 2014].

tados com relação a essas tecnologias". Além disso, ela definiu a vigilância como "uma violação do direito internacional" e "um caso de desrespeito à soberania nacional" do Brasil[9] Quando parecia que o Brasil insistia em uma abordagem intergovernamental, a presidente Dilma Rousseff retornou ao espectro das políticas, ao propor coorganizar um encontro NETmundial destinado a desenvolver ainda mais a governança da Internet multissetorial. O Brasil tinha um papel complexo a desempenhar, no qual seu principal objetivo era assegurar o êxito da reunião.

Em termos concretos, como exemplo, o Brasil não obteve êxito em alcançar uma linguagem mais sólida na Declaração Multissetorial da NETmundial[10] com relação à neutralidade da rede e à vigilância em massa, duas áreas prioritárias para a diplomacia da Internet no Brasil. Além disso, o Brasil viu alguns dos principais parceiros do BRICS se distanciarem: a Rússia se opôs abertamente à declaração da NETmundial; a Índia manifestou sérias preocupações e demorou em adotar a declaração final; e a China e a África do Sul foram muito discretas em suas manifestações. Resta saber se a alta capacidade de convergência do Brasil para promover o equilíbrio nas negociações de Governança da Internet será mantida na fase pós-NETmundial.

China

Sendo o país com o maior número de usuários da Internet, a China é um ator importante no âmbito da governança da Internet. Ela tenta manter o equilíbrio da política digital entre a comunicação livre movida pela economia com o resto do mundo e o acesso filtrado à internet, com base na política, para usuários chineses. A proteção da soberania como um dos pilares da política externa chinesa se encontra refletida no ciberespaço. Adam Segal, ao relatar um discurso proferido por Lu Wei, ministro da administração do ciberespaço da China, na Segunda Mesa Redonda sobre Internet entre a China e a Coreia do Sul, cita Wei: "Assim como o século XVII testemunhou a expansão da soberania nacional sobre partes do mar, e o século XX sobre o espaço

9 Nota do Tradutor: Rousseff D (2013) Declaração de Dilma Rousseff, presidente da República Federativa do Brasil, na abertura do debate geral da 68a Sessão da Assembleia Geral das Nações Unidas. Acessível em <https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf> [acessado em 7 de março de 2017]

10 NETmundial (2014) NETmundial Multistakeholder Statement. Acessível em <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf> [acessado em 15 de agosto de 2014].

aéreo, a soberania nacional agora é expandida sobre o ciberespaço [...] 'mas o ciberespaço sobrevive sem a soberania".[11]

A China alcançou elevado grau de soberania digital ao proibir e/ou restringir o acesso ao mercado chinês para as empresas estrangeiras de Internet (Facebook, Google, Twitter) e ao desenvolver as empresas chinesas de mídia social como a RenRen e a Sina Weibo. A maioria dos dados pertencentes a indivíduos e instituições chinesas é armazenado em servidores na China. Na política digital externa, a China defende a abordagem intergovernamental. No entanto, ela é discreta em suas manifestações, deixando a Rússia e outros países liderarem as iniciativas intergovernamentais em fóruns globais.

Índia

A Índia é um dos países indecisos no debate sobre a governança da Internet, apresentando posições diversas – e às vezes conflitantes. As complexas políticas de governança da Internet da Índia refletem a complexidade de suas decisões sobre as políticas digitais adotadas para o país. Ela apresenta um dos cenários sociais mais diversos e vibrantes no âmbito da governança global da Internet. A sua diplomacia tende à abordagem intergovernamental para a governança da Internet, ao passo que seu setor empresarial se aproxima da abordagem não governamental neste sentido. Tal dicotomia levou a algumas ações surpreendentes. Por exemplo, a Índia propôs a criação da UN Committee for Internet-Related Policies (CIRP) como forma de realizar a supervisão intergovernamental de recursos críticos da Internet. No entanto, o país mudou de posição no campo das políticas de Internet ao se aliar aos EUA e a outros países desenvolvidos no CMTI-12. A Índia não assinou os ITRs alterados e se afastou da posição dos países do G77. Esta ação inesperada foi justificada pela considerável força do lobby da indústria indiana de TIC.

Rússia

A Rússia vem sendo o país ativo e consistente na promoção da abordagem intergovernamental da governança da Internet. Na CMTI-12, a Rússia tentou incluir a Internet nos trabalhos da UIT por meio dos ITRs. Ela também apresenta um foco forte em cibersegurança por meio do trabalho da primeira comissão da Assembleia Geral das Nações Unidas.

11 Segal A (2013) Cyberspace cannot live without sovereignty, says Lu Wei. Acessível em <http://blogs.cfr.org/asia/2013/12/10/cyberspace-cannot-live-without-sovereignty-says-lu-wei/#cid=soc-twitter-at-blogs-cyberspace_cannot_live_without-121013> [acessado em 14 de agosto de 2014].

Países pequenos

A complexidade das questões e das dinâmicas das atividades fez com que fosse quase impossível para muitos países pequenos, principalmente países pequenos em desenvolvimento, acompanhar os processos das políticas de governança da Internet. Consequentemente, algumas pequenas nações vem defendendo a estrutura de one-stop-shop (balcão único) para questões de governança da Internet. [12] A agenda longa e a capacidade limitada das políticas dos países em desenvolvimento, tanto internamente quanto externamente, em suas missões diplomáticas continuam sendo alguns dos principais obstáculos para sua plena participação no processo. A necessidade de capacitação no campo da governança da Internet e das políticas pertinentes foi reconhecida como uma das prioridades da Agenda da CMSI de Túnis para a Sociedade de Informação.

GOVERNANÇA DA INTERNET – ABORDAGEM DA GEOMETRIA VARIÁVEL

A governança da Internet requer o envolvimento de diversas partes interessadas que são diferentes em muitos aspectos, entre os quais capacidade jurídica internacional, interesse em questões particulares de governança da Internet e o conhecimento que podem oferecer. Esta variedade pode ser harmonizada por meio da abordagem da geometria variável sugerida no Artigo 49 da Declaração da CMSI, [13] que especifica as seguintes funções para as principais partes interessadas:

- Estados – "competência referente às políticas das questões de políticas públicas relacionadas à Internet" (inclusive aspectos internacionais).
- Setor privado– "desenvolvimento da Internet, tanto no campo técnico quanto no campo econômico".
- Sociedade civil – "papel importante nas questões relacionadas à Internet, principalmente no âmbito comunitário".
- Organizações intergovernamentais – "a coordenação de questões de políticas públicas relacionadas à Internet".
- Organizações internacionais – "desenvolvimento de padrões técnicos relacionados à Internet e políticas pertinentes".

12 A conveniência do "one-stop shopping" (balcão único) foi um dos argumentos para estabelecer a UIT como o ator principal da governança da Internet.

13 WSIS (2003) Declaration of principles. Acessível em <http://www.itu.int/net/wsis/docs/geneva/official/dop.html> [acessado em 15 de agosto de 2014].

O setor empresarial[14]

Quando a ICANN foi criada em 1998, uma das principais preocupações do setor empresarial foi a proteção de marcas registradas. Muitas empresas enfrentaram problemas com a ciberespeculação e o mau uso das suas marcas registradas por indivíduos que eram rápidos o suficiente para registrá-las antes. No processo de criação da ICANN, os círculos empresariais claramente priorizaram as ações de proteção de marcas registradas e, consequentemente, esta questão foi imediatamente abordada assim que a ICANN foi formada, com a criação da Política para Resolução Uniforme de Litígios sobre Nomes de Domínios (Universal Dispute Resolution Procedures-UDRP).

THE INTERNATIONAL CHAMBER OF COMMERCE (ICC)

A Câmara Internacional de Comércio (International Chamber of Commerce -ICC), conhecida como a principal associação representativa do comércio em diversos setores e fronteiras geográficas, posicionou-se como uma das principais representantes do setor empresarial nos processos de governança da Internet global. A ICC esteve ativamente envolvida nas negociações iniciais do GTGI e da CMSI, e continua sendo colaboradora ativa no atual processo do IGF.

Hoje, com o crescimento da Internet, o interesse das empresas na governança da Internet se tornou ampla e diversificada, com os principais grupos de empresas a seguir: as empresas de nomes de domínio, os ISPs, empresas de telecomunicações e empresas de conteúdo da Internet.

Empresas de nomes de domínio

As empresas de nomes de domínio incluem agentes de registro e registros que vendem nomes de domínio da Internet (por exemplo, .com e .net). Os principais atores neste setor incluem a VeriSign e a Afilias, sendo que seus negócios são diretamente influenciados pelas decisões políticas da ICANN em áreas tais como a introdução de novos domínios e resolução de litígios, tornando-os um dos atores mais importantes no processo de formulação de políticas da ICANN. Também estiveram envolvidos no processo mais amplo de políticas

14 Comentários valiosos foram dados por Ayesha Hassan.

de governança da Internet (CMSI, GTGI, o IGF) tendo como objetivo principal reduzir o risco de alguma organização internacional potencialmente assumir a função da ICANN.

Provedores de Serviços de Internet (ISPs)

Uma vez que os ISPs são os principais intermediários online, eles são particularmente importantes para a governança da Internet. A sua participação se dá principalmente no âmbito nacional, lidando com autoridades governamentais e jurídicas. No âmbito global, alguns ISPs, principalmente dos EUA e da Europa, têm atuado ativamente nos processos da CMSI / GTGI / IGF, tanto individualmente quanto por meio de organizações empresariais específicas do setor nacional e regional, como a Associação de Tecnologia da Informação da América (Information Technology Association of America - ITAA), entre outras.

Empresas de telecomunicações

Estas empresas facilitam o tráfego da Internet e operam a infraestrutura da Internet. Os principais atores incluem empresas como a Verizon e a AT & T. Tradicionalmente, as empresas de telecomunicações participam da política internacional de telecomunicações por meio da UIT. Elas têm participado cada vez mais das atividades da ICANN e do IGF, sendo que seu principal interesse na governança da Internet é garantir um ambiente global favorável para o desenvolvimento de uma infraestrutura de telecomunicações da Internet. Ao longo dos últimos anos, a ETNO tem se posicionado ativamente, especialmente em questões como a neutralidade da rede.[15]

Empresas de conteúdo da Internet

VER A SEÇÃO 2 PARA UMA DISCUSSÃO MAIS APROFUNDADA SOBRE CIBERSEGURANÇAE NEUTRALIDADE DA REDE

Google, Facebook e Twitter são cada vez mais ativos na governança da Internet. O seu principal modelo de negócios poderia ser diretamente afetado, por exemplo, pelos acordos governamentais relacionados à proteção e privacidade de dados. Os produtores de conteúdos, tais como Disney, também são importantes atores, preocupados com a preservação do alcance global e da dominância de seus produtos e modelos para desenvolvimento de conteúdo local, bem como com a proteção de seus direitos autorais no nível global. As prioridades

15 Sítio web da ETNO (sem data) European Telecommunications Network Operators' Association. Acessível em <https://www.etno.eu/> [acessado em 15 de agosto de 2014].

comerciais dessas empresas estão intimamente ligadas às várias questões de governança da Internet, tais como propriedade intelectual, privacidade, cibersegurança e neutralidade da rede. A sua presença é cada vez mais perceptível nos processos globais de governança da Internet, inclusive por meio de financiamento para fóruns multissetoriais, como o IGF.

Sociedade civil

A sociedade civil tem sido o promotor mais expressivo e ativo da abordagem multissetorial à governança da Internet. A crítica comum sobre a participação da sociedade civil em fóruns multilaterais anteriores era a falta de coordenação adequada e a presença de muitas opiniões, frequentemente dissonantes. No processo da CMSI, no entanto, a representação da sociedade civil conseguiu aproveitar essa complexidade e diversidade inerentes por meio de algumas organizações, entre as quais o Escritório da Sociedade Civil (Civil Society Bureau), o Plenário da Sociedade Civil (Civil Society Plenary) e o Grupo de Conteúdos e Temas (Content and Themes Group). Confrontado com possibilidades limitadas para influenciar o processo formal, os grupos da sociedade civil criaram uma abordagem desenvolvida em duas vertentes. Mantiveram sua presença no processo formal aproveitando oportunidades disponíveis para participar e pressionar os governos e, em paralelo, elaboraram a Declaração da Sociedade Civil (Civil Society Declaration), uma visão alternativa à principal declaração adotada na CMSI de Genebra.[16]

ONGS E CMSI

A participação de ONGs na CMSI foi relativamente pequena. De aproximadamente 3000 ONGs com status consultivo junto ao ECOSOC das Nações Unidas, apenas 300 participaram da CMSI.

Devido à natureza multissetorial do GTGI, a sociedade civil chegou a um alto nível de envolvimento. Grupos da sociedade civil propuseram oito candidatos para o GTGI, todos posteriormente nomeados pelo Secretário-Geral das Nações Unidas. Na fase de Túnis (a segunda fase da

16 Plenário da Sociedade Civil da CMSI (2003) Shaping information societies for human needs. Acessível em <http://www.itu.int/wsis/docs/geneva/civil-society-declaration.pdf> [acessado em 15 de agosto de 2014].

CMSI, depois de Genebra), a principal dinâmica das políticas das organizações da sociedade civil foi transferida para o GTGI, influenciando muitas conclusões e decisões referentes à definição do IGF como espaço multissetorial para a discussão de questões de governança da Internet.

A sociedade civil continua participando ativamente de atividades do IGF. Uma das formas sui generis de representação da sociedade civil nos processos de governança da Internet é a Convenção de Governança da Internet (Internet Governance Caucus - IGC). Ela inclui os indivíduos interessados em compartilhar opiniões, opções de políticas e conhecimento sobre questões de governança da Internet, que são discutidas em um formato de lista de discussão.

As organizações da sociedade civil têm participação ativa em quase todos os temas de governança da Internet – desde o desenvolvimento de infraestrutura por meio de modelos econômicos até os direitos e as liberdades - priorizando principalmente a proteção dos interesses públicos. Muitas organizações empregam especialistas e acadêmicos com conhecimento e entendimento sólidos das especificidades da Internet, que muitas vezes fornecem valiosas contribuições para o processo de tomada de decisão.

Recentemente, houve uma divisão entre organizações da sociedade civil em matéria de proteção do interesse público global. Alguns membros da sociedade civil, mais especificamente dos países em desenvolvimento, entendem que uma atuação governamental mais forte é a maneira de contrabalançar o enorme poder da indústria da Internet. A sociedade civil dos países desenvolvidos, por outro lado, muitas vezes se alia à indústria da Internet e à comunidade técnica, principalmente com relação à questão da livre circulação de dados.

Organizações internacionais

A UIT foi a organização internacional central no processo da CMSI, como sede do Secretariado da CMSI e contribuindo em termos de políticas para as principais questões. A participação da UIT no processo da CMSI fez parte de sua tentativa em curso para definir e consolidar a sua nova posição no cenário global das telecomunicações em rápida mudança global, cada vez mais definido pela Internet. O papel da UIT tem sido contestado de várias maneiras. Ela estava perdendo seu tradicional domínio das políticas devido à liberalização do mercado global de telecomunicações liderada pela OMC. A mais recente tendência de transferir o tráfego de telefone das telecomunicações tradicionais à Internet (por meio do protocolo de voz- VoIP) reduziu ainda mais o

impacto rregulatório da UIT no campo das telecomunicações globais. A possibilidade de que a UIT pudesse ter surgido a partir do processo da CMSI como a Organização Internacional da Internet de facto causou preocupação nos EUA e em alguns outros países desenvolvidos, ao passo que ganhou apoio em alguns países em desenvolvimento. Ao longo da CMSI, esta possibilidade gerou tensões políticas subjacentes, que ficaram especialmente evidentes no campo da governança da Internet, no qual a tensão entre a ICANN e a UIT existia desde a criação da ICANN em 1998. A CMSI não resolveu esta tensão. Com a crescente convergência de várias tecnologias de comunicação, é muito provável que a questão do papel mais ativo da UIT no campo da governança da Internet permanecerá na agenda de políticas globais; ela já está ativa no campo da cibersegurança.

Outra questão diz respeito ao estabelecimento da agenda multidisciplinar da CMSI dentro da família de órgãos especializados da ONU. Aspectos não técnicos de comunicações e tecnologia da Internet, tais como características sociais, econômicas e culturais, são parte da missão de outros órgãos das Nações Unidas. O ator mais importante neste contexto é a UNESCO, que aborda questões como o multilinguismo, a diversidade cultural, a sociedade do conhecimento e o compartilhamento de informações. O equilíbrio entre a UIT e outras organizações das Nações Unidas foi cuidadosamente administrado. Os processos de acompanhamento da CMSI também refletem este equilíbrio, sendo que seus principais atores incluem a UIT, a UNESCO, e o PNUD.

Comunidade técnica

A comunidade técnica inclui instituições e indivíduos que tenham desenvolvido e promovido a Internet desde a sua criação. Historicamente, os membros da comunidade técnica estiveram principalmente ligados a universidades dos Estados Unidos, que trabalharam principalmente para desenvolver normas técnicas e estabelecer a funcionalidade básica da Internet. A comunidade técnica também estabeleceu a essência inicial da Internet, com base nos princípios do compartilhamento de recursos, do acesso aberto e da oposição à participação do governo na regulamentação da Internet. Desde o início, os seus membros protegiam o conceito inicial da Internet contra a comercialização intensiva e a influência governamental extensiva.

TERMINOLOGIA

Outros termos são usados de forma intercambiável com a comunidade técnica, tais como comunidade da Internet, desenvolvedores da Internet, fundadores da Internet, pais da Internet e tecnólogos. O termo "comunidade técnica" é usado nas declarações da CMSI e em outros documentos sobre políticas.

No contexto das relações internacionais, a comunidade técnica poderia ser descrita como uma comunidade epistêmica.[17] A comunidade técnica primitiva era coordenada por algumas regras, principalmente regras tácitas, e por um procedimento formal central - Request for Comments (RFC). Todos os padrões principais e básicos da Internet são descritos por meio do RFC. Embora não tivessem regulação rigorosa ou estrutura formal, as primeiras comunidades da Internet eram regidas por práticas sólidas e pressão entre pares. A maioria dos participantes neste processo compartilhava valores, sistemas de avaliação e condutas similares. A administração inicial da Internet pela comunidade técnica foi questionada em meados dos anos 90, quando a Internet se tornou parte da vida social e econômica global. O crescimento da Internet fez surgir um grupo composto por novas partes interessadas, como o setor empresarial, que trouxe consigo diferentes culturas profissionais e entendimentos da Internet e sua governança, o que levou ao aumento da tensão. Por exemplo, na década de 90, comunidades da Internet e a empresa Network Solutions[18] se envolveram na chamada guerra do DNS, conflito pelo controle do sistema de servidores raiz e nomes de domínio.

A Internet Society é um dos principais representantes da comunidade técnica. Abriga o IETF, defende a Internet aberta e desempenha um papel ativo na construção de capacidades.

A comunidade técnica tem sido um importante ator no processo de criação e gestão da ICANN. Um dos pais da Internet, Vint Cerf, foi o Presidente do Conselho da ICANN de 2000 a 2007. Os membros da

17 A comunidade técnica preenche todos os critérios da definição de Peter Haas sobre a comunidade epistêmica: "o grupo profissional que acreditar nas mesmas relações de causa e efeito, nos testes da verdade para aceitá-las, compartilha valores comuns; os seus membros compartilham um entendimento comum do problema e de suas soluções". Haas P (1990) Saving the Mediterranean: the politics of international environmental cooperation. Nova York: Columbia University Press, p. 55.

18 A empresa de tecnologia Network Solutions www.networksolutions.com foi fundada em 1979. O segmento de registro de domínio de nome era a divisão mais importante da empresa; a empresa diversificou sua carteira para incluir serviços da Web para pequenos negócios.

comunidade técnica detêm posições importantes em vários órgãos de decisão da ICANN.

Hoje, com quase três bilhões de usuários, a Internet ultrapassou o quadro de políticas baseadas na ICANN, priorizando a comunidade técnica como membro principal. Com base neste argumento, com a indefinição da fronteira entre cidadãos e usuários da Internet, é necessário um maior envolvimento dos governos e de outras estruturas representativas dos cidadãos, em lugar dos que apenas representam os usuários da Internet, frequentemente descritos como a comunidade técnica. Aqueles que defenderam um maior envolvimento dos governos na governança da Internet utilizaram esta abordagem da representação de cidadãos em vez de usuários e comunidades da Internet.

A comunidade técnica geralmente justifica sua posição particular na governança da Internet pelos seus conhecimentos técnicos. Ela argumenta que a ICANN é uma organização essencialmente técnica e, portanto, técnicos com conhecimento técnico devem administrá-la. Com a crescente dificuldade de manter a ICANN como uma organização exclusivamente técnica, esta justificativa do papel singular da comunidade técnica tem sido frequentemente contestada . É muito provável que os membros da comunidade técnica sejam gradualmente integrados aos principais grupos interessados, principalmente à sociedade civil, ao empresariado e às universidades, como também aos governos.

A Corporação da Internet para Atribuição de Nomes e Números (ICANN)

A ICANN é a principal instituição de governança da Internet, sendo que sua responsabilidade é gerenciar a infraestrutura básica da Internet, que consiste em endereços IP, nomes de domínio e servidores-raiz. O crescente interesse no papel de ICANN surgiu em paralelo ao rápido crescimento da Internet no início da década iniciada em 2000, e a ICANN chamou a atenção dos círculos de políticas globais durante o processo da CMSI (2002-2005).

Embora a ICANN seja um dos principais atores no campo da governança da Internet, ela não governa todos os aspectos da Internet. Ela é às vezes descrita, embora erroneamente, como o governo da Internet. A ICANN gerencia a infraestrutura de Internet, mas ela não tem autoridade direta sobre outras questões de governança da Internet, tais como cibersegurança, políticas de conteúdo, proteção de direitos autorais, proteção da privacidade, manutenção da diversidade cultural, ou redução da exclusão digital.

A ICANN é uma instituição multissetorial que envolve uma ampla variedade de atores de diferentes capacidades e funções. Eles são classificados em quatro principais grupos informais.

- Atores envolvidos desde a fundação da ICANN, entre os quais a comunidade técnica, a comunidade empresarial e o governo dos EUA.
- Organizações internacionais, sendo que as funções mais importantes são desempenhadas pela UIT e pela OMPI.
- Governos nacionais cujo interesse crescente em ter uma maior participação na ICANN começou com o processo da CMSI.
- Usuários da Internet (a comunidade em geral).

A ICANN tem testado várias abordagens a fim de envolver os usuários da Internet. Em seus primórdios, a primeira tentativa foi a de envolver os usuários da Internet por meio de eleições diretas para representantes das diretorias da ICANN. Foi uma tentativa de assegurar a legitimidade da ICANN. Com baixa participação e uso indevido do processo, o voto direto não funcionou porque não proporcionou representatividade real aos usuários da Internet. Mais recentemente, a ICANN vem tentando envolver os usuários da Internet por meio de uma estrutura de governança "geral". Esta experiência organizacional é essencial para garantir a legitimidade da ICANN.[19]

O processo de tomada de decisões da ICANN foi influenciado por processos iniciais de governança da Internet baseado em uma abordagem ascendente, transparente, aberta e inclusiva. Uma diferença importante entre a comunidade técnica inicial da década de 1980 e o atual contexto de tomada de decisão da ICANN é o nível de "capital social". No passado, a comunidade técnica apresentava elevado nível de confiança mútua e de solidariedade, o que fazia com que a tomada de decisão e a resolução de litígios fossem muito mais simples do que são agora. O crescimento da Internet atingiu milhões de novos usuários e novos atores, muito além da comunidade técnica inicial. Consequentemente, este rápido crescimento da Internet reduziu o capital social que existia em seus anos iniciais. Assim sendo, as propostas frequentemente feitas pela comunidade técnica para manter o processo de tomada de decisão anterior e informal sobre a Internet não têm sido realistas. Sem o capital social, a principal forma de garantir um processo de tomada de decisão totalmente funcional é formalizá-la e desenvolver vários mecanismos de pesos e contrapesos.

19 ICANN (sem data) ALAC. Acessível em <http://atlarge.icann.org/alac> [acessado em 15 de agosto de 2014].

Algumas correções nos processos decisórios já foram feitas para refletir esta realidade sob mudança. A mais importante foi a reforma da ICANN em 2002, que incluiu o fortalecimento do Comitê Consultivo Governamental (Governmental Advisory Committee - GAC) e a desistência do sistema de votação direta.

Questões

Gestão técnica x gestão de políticas

A dicotomia entre a gestão técnica e a gestão de políticas criou tensão contínua nas atividades da ICANN. A ICANN se definiu como um órgão de coordenação técnica da Internet que lida apenas com questões técnicas e se abstém dos aspectos de políticas públicas da Internet. Funcionários da ICANN consideraram que esta natureza técnica específica era o principal argumento conceitual para defender o status singular da instituição e sua estrutura organizacional. A primeira Presidente da ICANN, Esther Dyson, salientou que: "a ICANN não 'tem a intenção de resolver' quaisquer questões de governança da Internet; na verdade, ela governa a canalização, não as pessoas. Ela tem competência muito limitada para administrar determinados aspectos (amplamente técnicos) da infraestrutura da Internet em geral e do DNS em particular". [20]
Os críticos desta afirmação normalmente apontam para o fato de que não existem soluções tecnicamente neutras. Em última análise, cada solução técnica ou decisão promove certos interesses; capacita certos grupos; e afeta a vida social, política e econômica. O debate sobre questões como as .xxx (materiais adultos) ilustram claramente que a ICANN tem que lidar com aspectos de políticas públicas relacionadas às questões técnicas. A declaração final da reunião NETmundial recomenda que futuras discussões relacionadas à ICANN e à IANA abordem "a relação adequada entre os aspectos das políticas e operacional".10 Lidar com as novas questões de gTLDs fará com que a ICANN avance ainda mais no sentido de abordar questões de políticas públicas.

Status internacional da ICANN

A relação especial entre a ICANN e o governo dos Estados Unidos têm sido um dos principais focos de críticas, que assumem duas formas principais. A primeira se refere à responsabilidade global da ICANN e se baseia nas considerações sobre princípios, ressaltando que o elemento vital da infraestrutura global da Internet, que poderia afetar

20 0 Resposta de Esther Dyson às Perguntas de Ralph Nader (15 de junho de 1999). Acessível em <http://www.icann.org/en/correspondence/dyson-response-to-nader-15jun99.htm> [acessado em 14 de agosto de 2014].

todas as nações, seja supervisionado por um só país. Esta crítica ficou clara durante o processo da CMSI e foi reforçada pela suspeita geral da política externa dos EUA após a intervenção militar no Iraque. O contra-argumento típico a esta crítica se baseia no fato histórico de que a Internet foi criada nos EUA, com o apoio financeiro do governo os EUA. Consequentemente, de acordo com este argumento, isto concede ao governo norte-americano razões morais para decidir sobre a forma e o ritmo da globalização da governança da Internet. Esta abordagem é particularmente forte no Congresso dos EUA, que se opôs a qualquer globalização deste tipo - e especialmente as funções principais de outros governos (modelo conhecido como internacionalização pelos proponentes da abordagem multilateral).

A segunda crítica contra a relação especial entre a ICANN e os EUA se baseia em considerações práticas e jurídicas. Como a ICANN é uma entidade jurídica com sede nos EUA, tem que obedecer a lei dos EUA. Algumas destas leis podem afetar a regulação de instalações globais da ICANN. Aqueles que criticam o papel dos EUA geralmente citam o exemplo das sanções: se o Judiciário dos EUA exercer as suas competências e implementar corretamente o regime de sanções contra o Irã e Cuba, ele poderia forçar a ICANN – na qualidade de entidade privada dos EUA - a remover da Internet os domínios de países destes dois países. De acordo com este argumento, ao reter os nomes de domínio iranianos e cubanos, a ICANN viola a legislação dos EUA referente a sanções. Embora a remoção de nomes de domínio de país nunca tenha acontecido, continua a ser uma possibilidade dada à situação jurídica atual da ICANN.

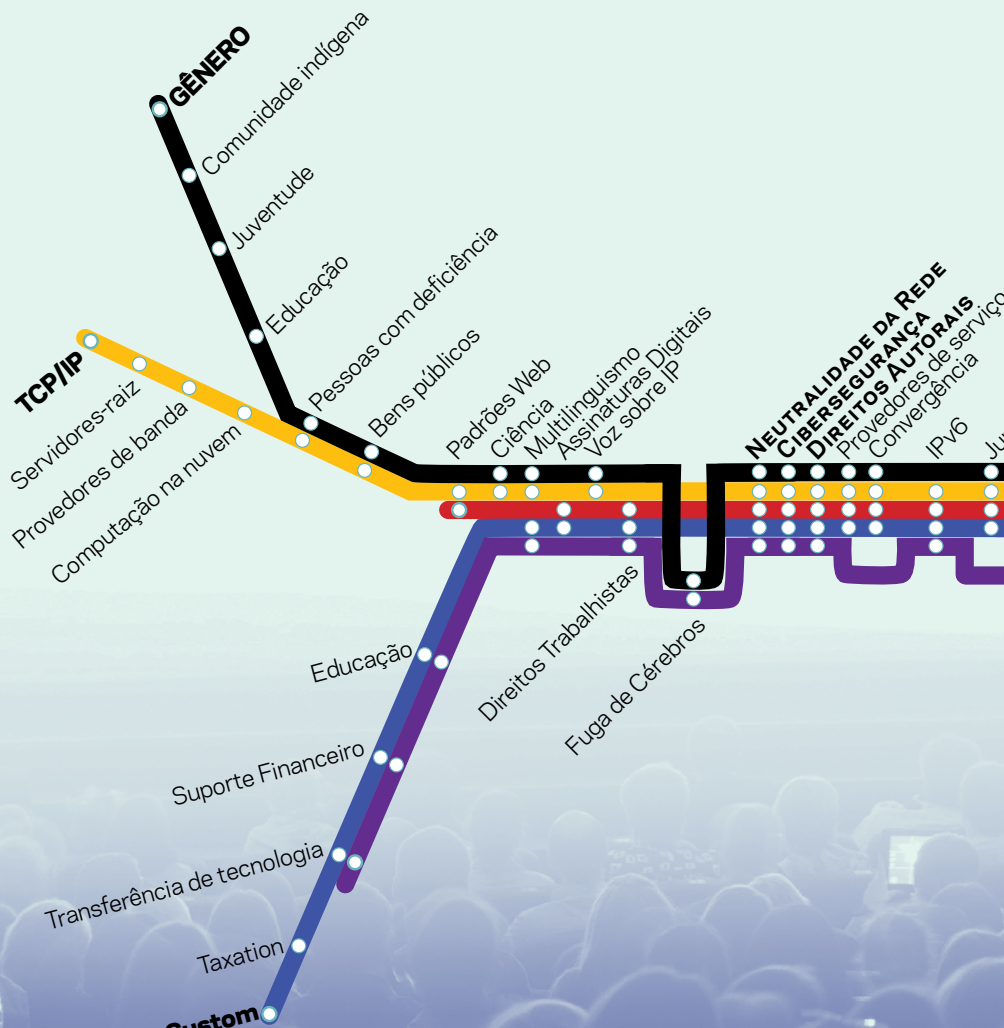
Próximos passos

O novo status da ICANN teve início com o anúncio da NTIA em 14 de março de 2014. Ambas as questões-chave - no domínio da política pública e da globalização - poderiam ser resolvidas com a mudança do status da ICANN, o que reduziria as ambiguidades e tornaria sua missão mais clara. O desenvolvimento futuro da ICANN exigirá soluções inovadoras, inclusive a possibilidade de transformar a ICANN em uma instalação global sui generis; isto preservaria todas as vantagens da atual estrutura da ICANN, bem como solucionaria suas deficiências, em particular os problemas da atribuição de responsabilidades e a legitimidade internacional. As inspirações para tais soluções criativas podem ser encontradas no Movimento Internacional da Cruz Vermelha e do Crescente Vermelho, que tem testado mecanismos para integrar as várias partes interessadas em um quadro legítimo de políticas internacionais, que equilibra os interesses públicos e as iniciativas privadas.

Anexos

Uma Jornada pela Governança na Internet

Uma Jornada através da governança da Internet
Questões chave e suas inter-relações 51 questões
em 5 linhas

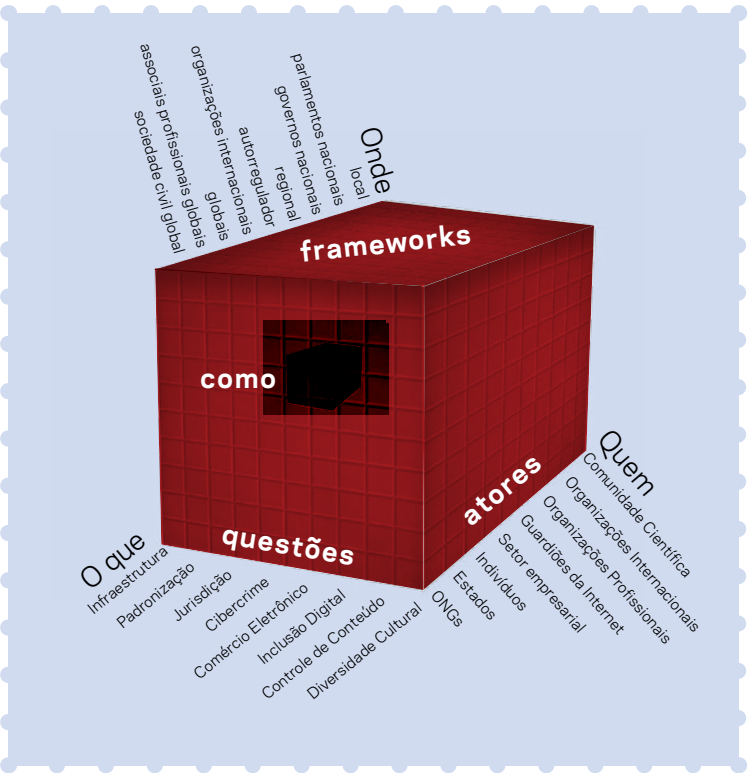


Este mapa é baseado na metodologia de pesquisa e de treinamento da Diplo sobre as TIC e Governança da Internet desenvolvida no período de 1998-2010.

A versão original foi desenvolvida por Stefano Baldi, Eduardo Gelbstein and Jovan Kurbalija

DiPLO
www.diplomacy.edu

O cubo da Governança da Internet



O cubo de governança da Internet é a visualização de processos de governança da Internet.

O eixo referente ao O QUÊ está relacionado às questões da governança da Internet (por exemplo, infraestrutura, direitos autorais e privacidade). Ele destaca a natureza multidisciplinar das questões de governança da Internet.

O eixo referente ao QUEM do cubo destaca os principais ATORES (Estados, organizações internacionais, sociedade civil, setor privado). Este é o aspecto multissetorial.

O eixo referente ao ONDE do cubo se refere ao QUADRO no qual as questões da Internet devem ser abordadas (de natureza autorreguladora, local, nacional, regional e global). Esta é uma abordagem multinivelada da governança da Internet.

Quando movemos as peças no cubo de governança da Internet, chegamos à intersecção - COMO. Esta é a seção do cubo que pode nos

ajudar a ver como as questões específicas devem ser regulamentadas, tanto em termos de técnicas cognitivas (ex., analogias) quanto em termos de instrumentos jurídicos (ex., leis não vinculativas, tratados e declarações). Por exemplo, uma intersecção específica pode nos ajudar a ver COMO questões de privacidade (O QUÊ) devem ser abordadas pelos governos, empresas e pela sociedade civil (QUEM) no âmbito regional (ONDE).
Separado do cubo de governança da Internet encontramos o quinto componente – QUANDO.

DiPLO
www.diplomacy.edu

A DiploFoundation é uma organização sem fins lucrativos que trabalha pela diplomacia inclusiva e eficiente. Ela foi criada em 2002 pelos governos de Malta e da Suíça. As atividades da Diplo estão relacionadas às nossas prioridades em educação, qualificação e construção de capacidades, e se integram a elas:

-Cursos: oferecemos cursos acadêmicos de pós-graduação e oficinas de formação sobre uma variedade de tópicos relacionados à diplomacia para diplomatas, funcionários públicos, funcionários de organizações internacionais e ONGs e estudantes de relações internacionais. Os nossos cursos são realizados por meio de educação online e educação mista.

- Capacitação: com o apoio de doadores e agências parceiras, oferecemos programas de capacitação para os participantes de países em desenvolvimento em uma série de temas, incluindo a Governança da Internet, Direitos Humanos, Diplomacia e Advocacia Pública e Diplomacia da Saúde.

- Pesquisas: através da nossa pesquisa e conferências, investigamos temas relacionados à diplomacia, governança da Internet e educação online.

- Publicações: nossas publicações vão desde a análise da evolução contemporânea da diplomacia até novas análises dos aspectos tradicionais da diplomacia.

- Desenvolvimento de software: criamos um conjunto de aplicações de software personalizadas para diplomatas e outras

pessoas que trabalham com relações internacionais. Também nos destacamos no desenvolvimento de plataformas de educação online.

A Diplo está localizada em Malta, com escritórios em Genebra e em Belgrado.

Para mais informações sobre a Diplo, visite http://www.diplomacy.edu

Geneva Internet Platform

O Departamento Federal de Negócios Estrangeiros (EDA) e o Serviço Federal de Telecomunicações (BAKOM) iniciaram a Plataforma Internet Genebra (GIP), que cumpre a missão de um centro de observação e capacitação (online e in situ) e um centro para discussão. A GIP é hospedada e administrada pela DiploFoundation.

As atividades da GIP são implementadas com base em três pilares:

- Uma plataforma física em Genebra
- Uma plataforma online e um observatório
- Um laboratório de inovação

O foco especial da GIP é ajudar países pequenos e em desenvolvimento a participar de forma significativa nos processos de governança da Internet. Este apoio é adaptado às necessidades destes atores e inclui atividades de formação, consciência, consultas e briefings (apresentação de informações).

Para mais informações sobre as atividades da GIP, consultar http://www.giplatform.org ou escrever para gip@diplomacy.edu

Posfácio

A estrutura brasileira de governança da Internet

Carlos Afonso

O Comitê Gestor da Internet no Brasil tem a atribuição de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil e diretrizes para a execução do registro de Nomes de Domínio, alocação de Endereço IP (Internet Protocol) e administração pertinente ao Domínio de Primeiro Nível ".br". Também promove estudos e recomenda procedimentos para a segurança da Internet e propõe programas de pesquisa e desenvolvimento que permitam a manutenção da qualidade técnica e inovação no uso da Internet.

O processo de criação

O Brasil foi pioneiro na formulação e realização de uma abordagem particular para a governança da Internet, por conta de uma intensa articulação realizada pela comunidade acadêmica e por organizações da sociedade civil[1] na década de 90. Esse processo, vindo das iniciativas de redes acadêmicas que resultaram na RNP (Rede Nacional de Pesquisa) e de iniciativas de entidades civis (notadamente o Instituto Brasileiro de Análises Sociais e Econômicas-Ibase)[1] que desde 1984 buscavam formas alternativas de comunicação para a integração internacional de suas atividades, recebeu um forte impulso com o envolvimento dessas entidades, em especial a APC (Associação para o Progresso das Comunicações)[2] e o Ibase na organização da Eco 92.

Respondendo a demandas da sociedade civil internacional para aproveitar a oportunidade de pela primeira vez ter uma participação ativa em uma conferência da ONU, o Ibase, com o apoio da APC e do Secretariado da Eco 92[3], iniciou em 1991 um processo para garantir

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

2 Associação para o Progresso das Comunicações – <http://www.apc.org>

3 Deve ser ressaltado o papel decisivo de membros do Secretariado da Eco 92, em particular o engenheiro nuclear Janos Pasztor (encarregado dos aspectos técnicos e logísticos da conferência e hoje assessor sênior do secretário-geral da ONU sobre mudanças climáticas), e o vice-secretário geral da Eco 92, Nitin Desai (coordenador do Grupo de Trabalho sobre

que a Internet pudesse ser parte de uma estrutura de comunicação que ampliasse a participação internacional na conferência.

A inclusão de um projeto de rede Internet no Acordo de Sede entre o governo brasileiro e a ONU para os espaços da conferência, planejado e operado pelo Ibase (através de seu projeto pioneiro AlterNex[4]) e técnicos da APC, e contando com as conexões de rede acadêmica da RNP, fez com que finalmente o Brasil pudesse contar com duas conexões permanentes internacionais à Internet nos EUA, uma das quais permitiu o acesso à Internet dos três telecentros da Eco 92. A conferência marcou o momento em que a Internet chegou ao Brasil para ficar, em um processo que levou à formação do Comitê Gestor da Internet no Brasil (CGI.br) em maio de 1995. A criação e a trajetória do CGI.br são marcadas também por outros fatos importantes que merecem ser mencionados.

A visão estratégica das lideranças do governo, da academia e da sociedade civil que criaram o CGI.br é bem caracterizada pela publicação, também em maio de 1995, da Norma 4, que estabelece a separação regulatória entre telecomunicações e serviços de valor agregado (SVAs) que utilizem as redes de telecomunicações, incluindo a Internet[5]. Tecnicamente, a Internet é um conjunto de serviços baseado em protocolos de endereçamento e transporte de dados, uma camada lógica que funciona sobre várias infraestruturas de telecomunicações, que por sua vez utiliza meios físicos como fios, fibras, rádio terrestre, rádio via satélite. É portanto ortogonal à regulação de telecomunicações. É de se notar que essa construção de conceitos foi anterior à Lei Geral das Telecomunicações (LGT, 1997[6]) e à criação da agência regulatória nacional do setor, a Anatel[7] – estas duas últimas criadas com vistas à privatização das telecomunicações. A preparação para a privatização foi iniciada em agosto de 1995 com a Emenda Constitucional nº 8 (separando telecomunicações de radiodifusão). Em julho de 1998 o processo foi efetivamente iniciado, com o desmembramento do conglomerado estatal Telebrás em 12 empresas a serem privatizadas.

Governança da Internet na Cúpula Mundial sobre a Sociedade da Informação – CMSI – e coordenador do grupo multissetorial assessor do IGF – MAG – de 2006 a 2009).

4 <https://pt.wikipedia.org/wiki/Alternex>

5 <http://www.anatel.gov.br/legislacao/normas-do-mc/78-portaria-148>

6 <http://www.planalto.gov.br/ccivil_03/leis/l9472.htm>

7 <http://www.anatel.gov.br>

A sequência de eventos (CGI.br e Norma 4 em 1995, Anatel e LGT em 1997) revela uma curiosa lacuna do processo na época. Mesmo tendo sido a LGT publicada depois da criação do CGI.br e da norma definindo a separação entre Internet e telecomunicações, sequer a palavra "Internet" aparece na LGT sancionada dois anos depois – lembrando que o ministro das Comunicações ainda era Sergio Motta, o mesmo que participou da criação do CGI.br (e da Norma 4) em 1995. Perdeu-se aqui a oportunidade da própria LGT incorporar as diretrizes da Norma 4, em vez de ficar apenas na referência a SVAs de modo genérico[8].

Soma-se a isso o fato de que em 1998 foi publicado pela Anatel o Regulamento Geral de Interconexão (RGI)[9], para que as empresas resultantes da privatização tivessem parâmetros regulatórios para interconectar[10] suas redes – lembrando que antes todos os serviços de telecomunicações estavam sob uma única estatal, a Telebrás, onde esse problema não existia. O RGI regula a interconexão da infraestrutura de telecomunicações, não os SVAs que utilizam essa infraestrutura, e basicamente estabelece regras para mitigar a disputa de preços entre operadoras – essencialmente quem paga o que a quem quando uma chamada de uma rede é feita a usuário de outra rede. Também determina que todas as redes de telecomunicações devem interconectar-se. De novo, nenhuma menção sobre Internet no regulamento.

A Lei 12.965, de 23 de abril de 2014 (o Marco Civil da Internet[11]) contém um detalhamento excepcional sobre direitos e deveres no âmbito da Internet. Na redação da Lei, não há, ao menos de forma explícita, menção a telecomunicações. A rigor, a única menção relacionada é a referência à Anatel. O texto tampouco faz referência à infraestrutura de telecomunicações propriamente dita; refere-se, apenas, ao SVA conhecido planetariamente como Internet.

Missão e consolidação

O CGI.br foi originalmente composto por nove voluntários escolhidos pelo governo federal, incluindo representantes deste, operadoras de telecomunicações, provedores de acesso, comuni-

8 Artigo 61 da LGT

9 <http://www.anatel.gov.br/legislacao/resolucoes/2005/167-resolucao-410>

10 Essa interconexão é definida no RGI assim: "ligação entre redes de telecomunicações funcionalmente compatíveis, de modo que usuários dos serviços de uma rede possam comunicar-se com os usuários de serviços de outra ou acessar serviços nela disponíveis."

11 <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>

dade acadêmica e representante dos usuários. Coube aos então ministérios da Ciência e Tecnologia e das Comunicações a formalização do comitê. A missão central do CGI.br desde então tem sido exercer as funções de coordenação e governança da infraestrutura 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 nome de domínio de topo brasileiro (ccTLD)[12] ".br" como um bem da comunidade e como a identidade do Brasil na Internet. A noção e defesa do ".br" como a identidade da nação brasileira na Internet vai além dos símbolos da nacionalidade – através do ".br" a comunidade brasileira, com toda sua diversidade, expressa sua cultura, sua economia, sua política para todo o planeta. O ".br" é restrito a pessoas físicas e jurídicas brasileiras ou com residência permanente no país. Uma pessoa ou entidade que queira 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).

Em consequência dessa visão, a função central de gestão de domínios e números IP tem sido desde o início um serviço sem fins lucrativos no qual a cessão anual dos nomes de domínio custa o mesmo valor qualquer que seja o nome de domínio[13]. Essa anuidade é necessária para cobrir os custos anuais de operação e desenvolvimento do sistema de governança.

As principais funções do sistema brasileiro de governança encabeçado pelo CGI.br são, conforme o Decreto Nº 4.829, de 3 de setembro de 2003[14]:

- estabelecer diretrizes estratégicas relacionadas com o uso e o desenvolvimento da Internet no Brasil;
- estabelecer diretrizes 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 téc-

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

13 O valor da anuidade, de R$30, será ajustado para R$40 a partir de janeiro de 2017.

14 <http://cgi.br/pagina/decretos/108>

nicas, bem como estimular a disseminação da Internet por todo o Brasil, buscando oportunidades para agregar valor aos bens e serviços relativos à rede;

- 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.

A representatividade no CGI.br é bastante debatida. Desde sua criação, até 2004, todos os conselheiros eram escolhidos pelo governo federal. Depois da mudança de governo no início de 2003, iniciou-se um processo de transição a partir de sugestões apresentadas ao novo governo em fevereiro daquele ano 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. Como resultado deste processo o novo governo federal determinou, por meio do Decreto 4.829, que o número de membros do comitê 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 passou a ser seguinte:

- o governo federal escolhe oito conselheiros;

as secretarias estaduais de Ciência e Tecnologia escolhem um conselheiro;

- entidades civis sem fins de lucro e não empresariais (o chamado "terceiro setor") escolhem quatro conselheiros;

- associações empresariais escolhem um conselheiro para cada um dos seguintes setores:

- provedores de acesso e conteúdo da Internet;

- provedores de infraestrutura de telecomunicações;
indústria de bens de informática, de bens de telecomunicações e de software;
- e setor empresarial usuário – somando 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.

Dado o papel estratégico do CGI.br e a crescente necessidade de uma personalidade jurídica que possibilitasse a implementação das decisões e projetos do comitê, em 2004, definiu-se que fosse formalizada (sob a supervisão do CGI.br), uma sociedade civil sem fins de lucro, de direito privado, o Núcleo de Informação e Coordenação do Ponto BR, conhecido pela sigla NIC.br[15], especialmente criada para assumir funções operacionais e administrativas. 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 cobrava na época pela distribuição de números IP) estava a cargo de um projeto junto à Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp)[16] em acordo com o governo federal, já que o comitê não tinha uma estrutura institucional que permitisse executar essas funções. Entre as atividades do NIC.br estão o registro de domínios, a distribuição de números IP, a operação de uma rede nacional de pontos de troca de tráfego e a 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. Vale notar que os recursos arrecadados com a distribuição de nomes e números, segundo o TCU, são considerados de natureza privada, integralmente geridos pelo NIC.br, sob a supervisão do comitê.[17] Todas as iniciativas apoiadas pelo CGI.br e todos os projetos conduzidos pelos NIC.br são exclusivamente financiados com esses recursos.

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

- administrar o registro e manutenção dos nomes de domínios que

15 <http://nic.br>
16 <http://www.fapesp.br>
17 Representação/Processo nº 012.048/2001-5 TCU. Acórdão 1164/2012.

usam o ".br", e a distribuição de blocos contíguos de endereços IPv4 e IPv6, através do serviço conhecido como registro.br;
- manter um centro de tratamento e resposta a incidentes de segurança em computadores envolvendo redes conectadas à Internet no país, através do projeto Cert.br (iniciado em 1997);
- desenvolver projetos técnicos que aprimorem a infraestrutura de redes brasileira (Ceptro.br, IX.br);
- conduzir e apoiar pesquisas, bem como a produção e publicação de indicadores, estatísticas e informação estratégica sobre o desenvolvimento da Internet no Brasil (Cetic.br);
- realizar e apoiar estudos e recomendar procedimentos, normas e padrões técnicos para a Web (W3C.br, Ceweb.br);
- prover 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.

Deste modo, 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 até o início de 2006, e que hoje somam mais de R$ 371 milhões, estão ainda retidos na 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 por esta para a empresa estadunidense 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, hoje IX.br)[18], com o objetivo de promover como serviço a criação de infraestrutura necessária para manter diversos pontos de troca de tráfego nas grandes cidades

18 <http://ix.br>

brasileiras, visando à 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[19]. Em setembro de 2016, o conjunto de PTTs operados pelo projeto IX.br, com mais de 860 redes filiadas, trafegava uma média de 1,2 Tbit/s (terabits por segundo), com picos de até 1,8 Tbit/s, classificando-se como o sexto maior do planeta[20].

As conquistas

O registro de domínios e números do Brasil é reputado internacionalmente como iniciativa muito bem administrada e tecnicamente sofisticada. Além de sediar parte dos serviços técnicos do Registro Regional de Números IP (Lacnic) também compartilha infraestrutura com outros registros de países.

Atualmente o registro de domínios ".br" está entre os maiores em número de domínios de países. Com mais de 3,9 milhões de domínios registrados no final de setembro de 2016[21], é o sétimo maior ccTLD e o décimo primeiro domínio de topo mundial[22]

O NIC.br suporta em suas instalações em São Paulo e nos principais pontos de troca de tráfego no Brasil 15 "espelhos" (duplicata) de 3 dos 13 servidores-raiz[23] da rede mundial – os servidores-raiz F, I e L. 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 iniciar a resolução de um nome na Internet, trazendo melhora de performance mas principalmente independência da rede brasileira em relação ao acesso à raiz do DNS Internet.

Os servidores que respondem pelo ".br" estão sediados com conjuntos globais em São Paulo, Rio de Janeiro (Embratel), Brasília (RNP), Freemont (HE), Frankfurt (DENIC) e Seul (KRNIC). Além destes

19 Estavam em operação em setembro de 2016 os PTTs do projeto nas cidades de Americana (SP), Belém (PA), Belo Horizonte (MG), Brasília (DF), Campina Grande (PB), Campinas (SP), Caxias do Sul (RS), Cuiabá (MT), Curitiba (PR), Florianópolis (SC), Fortaleza (CE), Foz do Iguaçu (PR), Goiânia (GO), Lajeado (RS), Londrina (PR), Manaus (AM), Maringá (PR), Natal (RN), Porto Alegre (RS), Recife (PE), Rio de Janeiro (RJ), Salvador (BA), São Carlos (SP), São José do Rio Preto (SP), São José dos Campos (SP), São Paulo (SP) e Vitória (ES).

20 <https://en.wikipedia.org/wiki/List_of_Internet_exchange_points_by_size>

21 Ver a tabela completa, atualizada regularmente, em _http://registro.br/estatisticas.html_

22 <https://www.verisign.com/assets/domain-name-report-sept2016.pdf_>

23 <http://www.root-servers.org/_>

temos algumas dezenas de cópias anycast espalhadas pelo mundo, na sua maioria em acordos de compartilhamento de infraestrutura.

O NIC.br presta serviço DNS secundário para dezenas de domínios de países. Ajudou a montar e colabora na operação de uma rede DNS anycast do Lactld[24] que melhora a publicação DNS em toda a região da América Latina.

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 centenas de profissionais de 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 Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (Cetic.br) foi criado em 2005, com a missão de monitorar a adoção das tecnologias de informação e comunicação (TICs) no país – em particular, o acesso e uso de computadores, Internet e dispositivos móveis. Entre seus objetivos está a elaboração de indicadores e a condução de pesquisas relacionadas ao acesso e uso das TICs no Brasil. O processo de pesquisa é estruturado de forma multiparticipativa, contando com um grupo de mais de 200 especialistas da academia, organizações sem fins lucrativos e do governo, que colaboram voluntariamente com a definição metodológica e processo de análise dos resultados das pesquisas.

Para garantir a comparabilidade internacional dos dados produzidos, o Cetic.br adota critérios de pesquisa que têm por base orienta-

24 <http://www.lactld.org/anycast/>

ções metodológicas e parâmetros estabelecidos por vários organismos internacionais multilaterais. Entre eles estão a União Internacional de Telecomunicações (UIT)[25], a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (Unctad), a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (Unesco), o Instituto de Estatísticas da Comissão Europeia (Eurostat) e a Comissão Econômica para a América Latina e Caribe (Cepal). O Cetic.br é reconhecido também como um Centro Regional Unesco.

O NIC.br sedia desde novembro de 2007 o escritório do Consórcio da Web Mundial (Worldwide Web Consortium, W3C)[26] no Brasil – o primeiro na América do Sul. O W3C é um consórcio internacional que tem como missão conduzir a Web ao seu potencial máximo, criando padrões e diretrizes que garantam sua evolução permanente. Mais de 80 padrões já foram publicados, entre eles HTML, XML, XHTML e CSS. O W3C no Brasil reforça os objetivos globais de uma Web para todos, em qualquer dispositivo, baseada no conhecimento, com segurança e responsabilidade.

O NIC.br também mantém o projeto Ceweb.br (Centro de Estudos sobre Tecnologias Web) para estimular a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas. O Ceweb.br nasceu inspirado pelos princípios e projetos já desenvolvidos pelo Escritório Brasileiro do W3C (World Wide Web Consortium)[27], hospedado e apoiado pelo NIC.br no Brasil desde 2008, com a missão de promover atividades que estimulem o uso de tecnologias abertas e padronizadas na Web.

Por fim, o Brasil foi 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 de processos e

25 <http://itu.int>
26 <http://www.w3c.br/Home/WebHome>
27 <http://w3c.org>

eventos como o Fórum de Governança da Internet da ONU (IGF)[28]. No entanto, através de Grupos de Trabalho voluntários, busca acompanhar esses temas (conteúdo, acesso, inclusão digital, privacidade, regulação, uso indevido, entre outros). É importante destacar que o CGI.br participa de forma destacada nos principais fóruns, conferências, organismos e eventos internacionais relacionados ao desenvolvimento e governança da Internet, entre os quais as reuniões da ICANN[29], da IETF[30] e do IGF, e foi a principal entidade organizadora do IGF 2007 no Rio de Janeiro, do IGF 2015 em João Pessoa, e do Encontro NETmundial[31] em 2014 em São Paulo.

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 tem sido utilizada desde então no apoio a projetos e eventos nacionais e internacionais relativos a temas cruciais do ecossistema da Internet. 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.

Em conformidade com sua missão, tal como especificada no decreto de 2003, tanto o CGI.br como o NIC.br têm atuado na formulação de recomendações para vários aspectos da governança da Internet no Brasil e no mundo. Em 2009, depois de quase dois anos de diálogo interno, o CGI.br publicou seus "Dez Princípios para a Governança e Uso da Internet"[32] – uma carta de referência sobre os tópicos centrais da governança da Internet construída por consenso de todos os setores participantes do comitê (e por isso mesmo o processo foi mais demorado). Os Princípios foram a semente para a construção da proposta do Marco Civil da Internet, que custou vários anos de consultas públicas e debates com todos os setores até culminar na Lei 12.965, sancionada pela presidenta Dilma Rousseff durante o Encontro NETmundial, em 23 de abril de 2014.

Apesar de todas essas atividades e realizações cruciais para o desenvolvimento da Internet no país, e o respeito internacional adquirido tanto pela qualidade como pelo pioneirismo de suas atividades e abordagem de governança, o CGI.br e as atividades do NIC.br são

28 <http://intgovforum.org>
29 <http://icann.org>
30 <http://ietf.org>
31 <http://netmundial.br>
32 <http://www.cgi.br/principios>

muito pouco divulgados para o público brasileiro – alguns chegam a dizer que é um dos segredos mais bem guardados da rede no Brasil, ou ainda que esse trabalho excepcional é muito mais conhecido no exterior do que em seu próprio país. Este é outro desafio: fazer com que esta experiência e seus excepcionais resultados sejam conhecidos amplamente, e na medida do possível replicados como referência de governança pluralista em outros setores que envolvam formulação e decisão sobre políticas públicas – uma forma de legitimar e consolidar estrategicamente esse trabalho e essa visão participativa.

Sobre o autor

Jovan Kurbalija é o diretor fundador da DiploFoundation e chefe da Plataforma Internet Genebra. É um ex-diplomata com experiência profissional e acadêmica em direito internacional, diplomacia e tecnologia da informação. Em 1992, ele estabeleceu a Unidade de Tecnologia da Informação e Diplomacia na Academia Mediterrânea de Estudos Diplomáticos em Malta. Após mais de dez anos de treinamento, pesquisa e publicação, em 2002 a Unidade evoluiu para a DiploFoundation.

Desde 1994, o Dr. Kurbalija tem ministrado cursos sobre o impacto da OAC TIC/Internet na diplomacia e governança de TIC/Internet. Atualmente, ele é professor convidado do Colégio Europeu de Bruges e da Universidade de St Gallen. Ele lecionou na Academia Mediterrânea de Estudos Diplomáticos em Malta, na Academia Diplomática de Viena, no Instituto Holandês de Relações Internacionais (Clingendael), no Instituto Universitário de Altos Estudos Internacionais de Genebra, no Colégio de Funcionários do Sistema das Nações Unidas e na Universidade do Sul da Califórnia. Ele concebeu e atualmente dirige o Programa de

Capacitação em Governança da Internet da DiploFoundation (2005-2014). Os principais interesses de pesquisa do Dr. Kurbalija incluem o desenvolvimento de um regime internacional para a Internet, a utilização da Internet na diplomacia e nas negociações contemporâneas, e o impacto da Internet sobre as relações internacionais contemporâneas.

O Dr Kurbalija publicou e editou inúmeros livros, artigos e capítulos, entre os quais: The Internet Guide for Diplomats, Knowledge and Diplomacy, The Influence of IT on Diplomatic Practice, Information Technology and the Diplomatic Services of Developing Countries, Modern Diplomacy e Language and Diplomacy. Com Stefano Baldi e Eduardo Gelbstein, ele foi coautor do Information Society Library, um conjunto de oito cadernos abrangendo uma ampla gama de questões relacionadas à Internet.

jovank@diplomacy.edu

Sobre o co-autor

Carlos Alberto Afonso estudou engenharia na Poli-USP e é mestre em Economia pela York University do Canadá, onde cursou o doutorado em Pensamento Social e Político. Foi diretor de tecnologia e planejamento da Rede de Informações para o Terceiro Setor (RITS) e é consultor do Instituto Nupef. Foi um dos pioneiros no desenvolvimento da Internet no Brasil, ao criar o Alternex em 1987 como um sistema de troca de mensagens experimental para entidades civis, que viria a evoluir para o primeiro provedor de serviços de Internet do país em 1989. Em 1995, enquanto era um dos diretores do IBASE, trabalhou para a criação do CGI.br, para o qual também foi indicado como membro. Em 2003, participou da proposta de reestruturação do Comitê, com a votação por um colégio eleitoral dos 11 representantes não-governamentais. Foi eleito Conselheiro do CGI.br em julho de 1995 e abril de 2003, eleito em junho de 2007, reeleito em fevereiro de 2011 e julho de 2014.

nic.br

Núcleo de Informação
e Coordenação do
Ponto BR