> VIGILÂNCIA PREVISTA EM LEI:
o fim derradeiro do sigilo nas comunicações?

> ISO, PADRÕES ABERTOS, INTEROPERABILIDADE
e as discussões recentes sobre o ODF e o OXML

poliTICs

Uma publicação do NUPEF / RITS • novembro / 2008 • www.politics.org.br

Discriminação de conteúdos na Internet:

Pedágios na rede colocam em risco o interesse público

Editorial

a palavra 'abertura' aparece na maioria dos artigos desta segunda edição da poliTICs e, mesmo naqueles em que o termo não está expresso, o conceito de abertura nas tecnologias de informação e comunicação - especialmente na Internet - é o pano de fundo. A natureza aberta e descentralizada da Internet é um dos elementos que tornou possível a Web que conhecemos hoje – e que está ameaçada.

Algumas das ameaças à natureza original da Internet são chamadas de ataques à neutralidade da rede. Sabemos que, em se tratando de tecnologias, o termo 'neutralidade' não é pacífico – e a crítica a este conceito é bem fundamentada no artigo do pesquisador norte-americano Christian Sandvig, que abre esta revista. Sandvig mostra como funcionam alguns dos "pedágios" na Internet, que discriminam conteúdos em favor de interesses e motivos diversos (alguns, segundo ele, até justificáveis). A discriminação de conteúdos, o monitoramento e priorização do tráfego Internet também são desafios abordados por Alex Gakuru – mas, neste artigo, a perspectiva dos países africanos, historicamente explorados pelos interesses colonialistas, oferece uma noção do quanto a interferência de interesses privados na Internet pode ser perniciosa para o desenvolvimento.

Não é apenas no aspecto tecnológico que se manifestam as possibilidades de cerceamento à liberdade e à autonomia na rede: no campo jurídico também se intensificam medidas restritivas e políticas de controle. O texto do professor Jorge Alberto Machado apresenta, a partir da análise da 'Lei de Telemédia' alemã, uma tendência que se espalha pela Europa e ameaça chegar ao Brasil – sob o argumento de promoção da segurança e combate ao crime, legaliza -se a violação da privacidade, com a implementação de medidas draconianas de retenção de dados e vigilância.

A abertura dos padrões e a interoperabilidade são o tema do artigo de Cezar Taurion, que acompanhou na ISO as discussões sobre os padrões ODF e OXML – e pôde comprovar como é urgente a reforma dos processos desta organização. A necessidade de mais transparência e a garantia da defesa do interesse público na definição de padrões abertos de TICs são os principais pontos defendidos pelo autor.

Fechamos esta edição com um artigo de Joel Kelsey, da ONG norte-americana Consumers Union. A recente derrota da empresa Comcast na FCC - Comissão Federal de Comunicações dos EUA - representa, para muitos, uma folha verde de esperança planando nos ventos da mudança que parecem cruzar aquele país. A Comcast interferiu no tráfego Internet de seus clientes, dissimilou suas arbitrariedades, negou, mentiu, e foi condenada pela FCC – que optou por proteger a liberdade e fazer prevalecer os direitos dos usuários de Internet. Vale a pena conferir os detalhes.

▶ Esperamos que você aprecie a leitura, participe e opine – o espaço está aberto em **www.politics.org.br**

Um abraço,

Graciela Selaimen

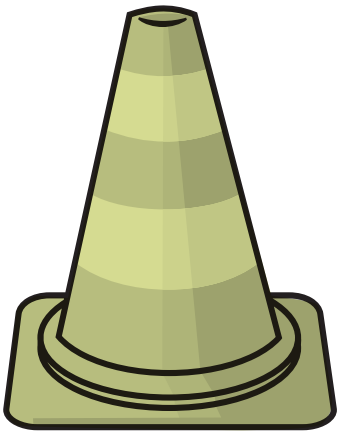
Editora da poliTICs / Coordenadora executiva do Nupef/Rits


@
www

Christian Sandvig
Professor Associado de Comunicação e Ciência Coordenada na Universidade de Illinois em Urbana-Champaign. Em 2002, foi chamado de "líder da próxima geração" em políticas de tecnologia pela Associação Americana para o Avanço da Ciência.

Neutralidade da Rede

e a nova via pública



Alguns usuários da Internet estão preocupados. Para muitos deles, a rede mundial significa uma capacidade de comunicar-se jamais experimentada antes. E, melhor ainda, na Internet serviços e conteúdo costumam ser gratuitos. A qualquer hora é possível encontrar, ver, ouvir e interagir com todo tipo de coisa. Isto, por si só, parece ser um avanço evidente em relação ao antigo mundo da mídia e das telecomunicações - onde a programação do conteúdo era fechada, as ofertas eram limitadas e, o que é pior, vinculadas a pagamento, precificação, cobrança por minuto, *pay-per-view* e seletos canais de assinaturas exclusivas. Por volta do início de 2006, começou a crescer a percepção de que essa Internet gratuita e generosa via-se ameaçada por poderosas empresas de telefonia e cabo, e que isso poderia estar ou não relacionado à metáfora das rodovias e ferrovias. Num editorial do New York Times intitulado "Pedágio na Estrada da Internet', o autor sugeriu que os provedores de serviços Internet poderiam estar favorecendo os "gigantes" contra os "pequeninos" na rede. O texto exortava o leitor a perceber que "os norte-americanos querem uma Internet aberta e livre. [Esta] é uma questão onde

o interesse público pode e deve suplantar interesses particulares".

Este artigo foca-se nas questões acerca do que se convencionou chamar de debate sobre a "neutralidade da rede"; visa a elaborar argumentos mais aprimorados sobre o papel do interesse público nas infraestruturas de comunicações em rede. Explicando de maneira crítica o conceito de neutralidade da rede - conforme é compreendido hoje -, tento desenvolver uma avaliação mais adequada do significado do pedágio e das práticas discriminatórias na Internet. Basicamente, "neutralidade" é uma abordagem conceitual falha. Na inevitavelmente discriminatória, enviesada e tarifada Internet que já existe, a questão não é neutralidade, mas sim quem discrimina por qual propósito, e se essa discriminação é oculta ou visível. Para raciocinarmos sensatamente sobre o presente e o futuro da Internet, precisamos não de neutralidade, mas sim de uma visão normativa do serviço público que a Internet deve cumprir.

:: A INTERNET DO *PAY-PER-VIEW* QUE JÁ DESPONTA NO HORIZONTE

O usuário teme cada vez mais, com o passar dos anos, que a Internet possa se tornar algo como um sistema de cabo ao estilo *pay-per-view.* Dentre as primeiras análises que surgiram na literatura especializada, a mais influente veio no ano 2000 (Bar, Cohen, Cowhey, DeLong, Kleeman, & Zysman, 2000). Citemos um exemplo memorável que este estudo nos traz. Os autores apontaram que, em seu relatório anual de 1998, a operadora de TV a cabo AT&T/@ Home traçou uma estratégia para alavancar seu controle monopolista de franquias locais de televisão a cabo para um controle de conteúdo na Internet. A empresa formara parcerias exclusivas com provedores de conteúdo para a Internet em várias áreas de conteúdos não concorrentes. Por estes rentáveis acordos secretos[1] , em troca a AT&T/@Home fornecia acesso mais rápido para os serviços de maior procura de seus "parceiros", prática à qual se referiu, em 1999, usando uma expressão típica da linguagem no mundo da televisão: estava "definindo a grade de programação da Internet".

Pela ótica do usuário, a idéia chega a dar calafrios. Um assinante de modem a cabo da AT&T/@Home podia testar jogos pela Internet usando o Sega Dreamcast e também uma outra plataforma concorrente. Jogando com o Sega, o usuário tinha uma experiência mais interativa, mais rica - mas jamais saberia que a razão para tanto não era a superioridade geral do produto e sim um acordo privado entre a SegaSoft e o monopólio de serviços a cabo. Isso foi o prenúncio do cenário de uma Internet instável e desigual, onde sítios Web e serviços podem estar disponíveis em condições bem diversas - situação já prevista em pesquisas anteriores

1. "Secretos" pois sua existência é revelada para acionistas e não para consumidores, e os termos exatos dos acordos não o são para ninguém.

que sugeriam a possibilidade do surgimento de "ilhas de alta interoperabilidade" na Internet, acessíveis somente para alguns usuários, para alguns propósitos[2].

Nesse modelo de Internet, a lógica que explica quais endereços Web seriam mais fáceis de abrir e quais seriam mais difíceis nunca se revelaria ao usuário, pois a "grade de programação" da Internet seria regida por acordos ocultos. E, o que é pior, dados a disponibilidade limitada de acesso por banda larga e o elevado custo para se trocar de um provedor para outro[3], mesmo que descobrisse a situação, o usuário talvez não tivesse outra opção de serviço.

As tendências no sentido de uma Internet desigual não se limitam a este exemplo, ou a monopólios locais de serviços a cabo. Em suma, todos os provedores de Internet tentam exercer de alguma forma um controle técnico e/ou jurídico sobre o tráfego de seus usuários, mesmo que seja apenas para coibir conteúdo ilegal. Por mais que esteja voltada a diferentes focos e seja operada de diferentes maneiras, a discriminação de conteúdos na Web a tudo permeia. Os provedores limitam o uso de criptografia em redes virtuais privadas (VPNs) normalmente usadas por empresas, limitam a operação de servidores para prover informação e aplicações que usam grande largura de banda, como vídeo-conferência e compartilhamento de arquivos *peer-to-peer.* Proibem a revenda ou compartilhamento de banda Internet com terceiros - por exemplo, através de conexões Wi-Fi abertas[4]. Os motivos para essas intervenções variam. Algumas visam claramente ao aumento do lucro, por conta da possibilidade de discriminação de preços - e este tipo de controle pode ser indiferente quanto ao teor do conteúdo que trafega. Entretanto, muitas tentativas de controlar o tráfego estão explicitamente ligadas a censura de conteúdo. Para citar alguns outros exemplos que têm sido alvo de muita atenção, governos como os da China e de Cuba bloqueiam materiais dissidentes ou religiosos[5]. Escolas públicas nos Estados Unidos bloqueiam conteúdos de sexo explícito[6]. Muitos provedores de serviços tentam detectar e-mails sobre tópicos aparentemente não solicitados e os diferenciam ou bloqueiam[7]. O provedor canadense Tellus bloqueou o acesso dos assinantes ao sítio Web do sindicato de classe dos seus funcionários durante uma disputa trabalhista[8].

A fim de corrigir a situação de provedores que censuram e manipulam o uso da Internet para atender a fins privados, extravagantes ou funestos, Tim Wu propôs uma pequena lista de regras em torno da "neutralidade da rede" (2003) que proibiriam as operadoras de discriminar o tráfego de usuários a partir de certos fundamentos. Especificamente, Wu argumentou que a discriminação baseada em

2. Bar, Borrus, & Steinberg, 1995, p. 44. 3. Como trocar de um serviço de modem a cabo por um DSL. Bar et al. estimaram que os custos com essa troca poderiam ultrapassar os 500 dólares em 2000 (p. 503). 4. Para obter um levantamento completo das proibições em acordos de Termos de Serviços, consulte Braman & Roberts, 2003. 5. Por exemplo, ver Zittrain & Edelman, 2003; Kalathil & Boas, 2003. 6. Hunter, 2000. 7. Beke, 1998. 8. OpenNet Initiative, 2005.

capacidade [de tráfego] deveria ser permitida, enquanto que a discriminação baseada em conteúdo não. O provedor pode estabelecer um teto para o tráfego que você vai gerar, mas não pode lhe dizer para enviar um tipo de conteúdo e não outro.

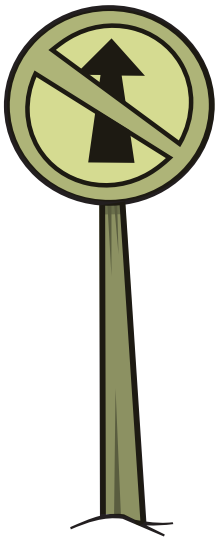
:: O ESTRANHO ENFOQUE DO DEBATE SOBRE A NEUTRALIDADE DA REDE

Na literatura e na imprensa, o difundido debate sobre a neutralidade da rede tem se concentrado nos dispositivos restritivos inseridos pelas grandes operadoras nos acordos com o assinante. Trabalhos empíricos têm catalogado e comparado as restrições impostas pelos provedores, mas esta ênfase está mal colocada. Muitos desses dispositivos não têm força de lei e são ultrajantes - o uso de termos jurídicos na apresentação destes dispositivos é uma tática para amedrontar, mas não há nenhuma obrigação contratual a ser cumprida pelo usuário. Por exemplo, os termos do acordo de prestação de serviço da Verizon Online forçam o assinante a concordar em não usar este serviço para criticar a Verizon[9]. Embora tenham sido feito esforços para tornar legítimos alguns desses acordos, eles não o são agora. Portanto, é estranho que o debate tenha se centrado nesses casos de dissimulações jurídicas - por mais feias que sejam, mesmo as piores delas provavelmente nunca terão alguma exigibilidade. Isso contrasta com a literatura mais extensa acerca da censura na Internet, que empreendeu grandes esforços para medir empiricamente os danos da censura - em lugar de se fiar nas declarações jurídicas ou políticas dos censores em potencial[10].

A manipulação **tecnológica** do tráfego, ao contrário da manipulação jurídica, não está no futuro nem é hipotética. Hoje existe uma ampla gama de pacotes de software e ferramentas para auxiliar os provedores de serviços de Internet a inspecionar e controlar o conteúdo do seu tráfego, dentre os quais o Packeteer, o L7- filter, o Packet Details Markup Language (PDML), o netscreen-IDP e o NetScout. Estas não são tecnologias prospectivas ou experimentais; muitas delas já mostraram ser robustos pacotes de software amplamente utilizados. Se o leitor usa a Internet, é provável que seu tráfego esteja passando agora por alguns desses sistemas. Seu uso principal é para discriminar o tráfego na Internet: é disso que o debate sobre a neutralidade da rede deve tratar. Vamos estudar brevemente os principais meios tecnológicos através dos quais os provedores atualmente discriminam e manipulam o tráfego na Internet. Em muitas discussões, quatro meios distintos de manipulação são identificados: bloqueio de endereço, bloqueio de porta ou protocolo, filtragem de conteúdo e priorização.

• **Bloqueio de endereço.** Falando metaforicamente, este meio de interferência não difere do bloqueio de endereço num sistema postal:

9. Este exemplo foi apontado em CYBERTELECOM-L: "Você NÃO pode usar o serviço da seguinte maneira: ... (j) para prejudicar o nome ou a reputação da Verizon." http://www.verizon.net/policies/vzcom/tos_popup.asp 10. Ver Zittrain & Edelman, 2003



a correspondência enviada para indivíduos subversivos e outros indesejáveis não é entregue. Este é o método de censura ao tráfego na Internet que tem recebido mais atenção, mas também é bastante rudimentar e óbvio. Quando se fala de liberdade na Internet, o exemplo de ameaça mais claro e convincente é o do usuário que quer visitar determinado sítio e é impedido de fazê-lo. Sistemas assim existem e estão efetivamente censurando conteúdos. Constituem-se numa forte barreira ao fluxo livre de informação pela Internet em diversos contextos, entre os quais se destacam os computadores em países autoritários e em escolas e bibliotecas dos EUA. Também foram caracterizados através do uso de frases evocativas como "A Grande *Firewall* da China". Entretanto, o bloqueio de nomes de domínio ou de endereços de IP exige que sejam mantidas listas negras, algo complicado e sujeito a erros, que pode ser contornado mudando-se os endereços ou disfarçando-se o destino do tráfego por intermédio de um re-roteamento através de terceiros. O braço publicitário da Voz da América nos EUA (o International Broadcasting Bureau) financiou recentemente o desenvolvimento de um software chamado Peacefire Circumventor, que consegue escapar da censura imposta pela Grande *Firewall* da China e dizem ser também bastante usado nas escolas e bibliotecas norte-americanas[11]. Como essa forma de discriminação tem sido bastante comentada noutras paragens, daqui em diante este artigo tratará das manipulações de tráfego que são menos óbvias.

• **Bloqueio de protocolo ou de porta.** Embora pareça ser de alta complexidade técnica, metaforicamente este não passa de um controle da correspondência postal baseado no tipo de envelope usado. Muitas pessoas descartam imediatamente a propaganda que recebem via mala direta por que reconhecem o tipo de embalagem ou envelope usado, mas é claro que os remetentes interessados em evitar tal filtragem já descobriram maneiras de disfarçar sua publicidade mudando os envelopes. Essa técnica esteve em pauta no caso FCC vs. Madison River[12]. Ela identifica aplicações de Internet através do sistema de números usados nos protocolos de Internet que entregam os dados para as aplicações compatíveis, num computador conectado à rede. Para assegurar, por exemplo, que seu pedido de página da Internet seja entregue ao seu navegador e não ao seu cliente de e-mail ou driver de impressora, foram estabelecidos números específicos para os diferentes tipos de tráfego, chamados "portas". Porta 25 ou 143 para e-mail, porta 80 para páginas da World Wide Web, antigamente 1214

11. Ver http://www.peacefire.org/ 12. Madison River Communications, um provedor DSL, foi multado em U$15,000 pela FCC (Comissão Federal de Comunicações dos EUA) por impedir seus clientes de usarem o serviço Vonage de Voice-over-Internet-Protocol (VoIP).Ver em Madison River Consent Decree, File No. EB-05-IH-0110, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A1.pdf

> Embora a idéia de discriminação de tráfego na Internet costume evocar o governo de Cuba, o vilão dessa história - se é que há vilão -, é a Universidade da Califórnia, em Berkeley.

para Napster, e assim por diante. A Madison River escaneava o tráfego de Internet de seus usuários e descartava aquele cujo número de porta era usado pelo provedor de VoIP[13] Vonage. Embora se tratasse de uma técnica bastante direta, era um método relativamente rudimentar, pois esses números não são necessariamente uma indicação confiável do tipo de aplicação que esteja de fato usando aquela porta. Quem manda uma bomba ou um volumoso maço de dinheiro pelo correio tem interesse em assegurar que o pacote não revele o que vai dentro. Como alguns vírus na Internet estão associados a números de portas específicos, o bloqueio de portas é amplamente usado pelos provedores de serviços. Esta técnica costumava ser empregada para bloquear serviços de compartilhamento de arquivos entre usuários, mas a prática do P2P[14] passou a usar números de portas de forma cada vez mais sofisticada, instituindo uma distribuição quase aleatória para designá-los. Assim como acontece com o bloqueio de endereços, o bloqueio de porta ou protocolo é uma solução tosca por várias razões - uma das quais é que as partes afetadas ficam cientes de terem sido censuradas e podem tomar providências para corrigir a situação (por exemplo, no caso da Vonage, fazendo uma petição à FCC).

•**Filtragem baseada no conteúdo.** Esta é uma técnica mais invasiva. Em lugar de examinar as informações sobre o conteúdo através dos números dos protocolos dos pacotes, trata-se de monitorar o conteúdo propriamente dito, reconstruindo o fluxo dos pacotes de dados e abrindo-os – assim como como um carteiro apaixonado, no século XIX, pode ter aberto as cartas que deveria entregar. Alguns softwares para filtragem de conteúdo na Web usam essa técnica, mas isso pode sobrecarregar o desempenho da rede e sua ação pode ser tornada ineficaz com o uso da criptografia.

•**Priorização e Condicionamento** *(traffic shaping)*. Muito mais importantes e menos consideradas são as circunstâncias que costumam receber o nome de "*traffic shaping*" ou "condicionamento". As reclamações sobre o possível "enfileiramento" de conteúdos no tráfego de Internet são reclamações sobre priorização. Nesse cenário, a numeração das portas, os endereços (ver acima) ou outros meios (como o reconhecimento de padrões da assinatura dos dados de uma aplicação ou a superposições de redes) são usados para separar alguns tráfegos de outros com o propósito de propiciar tratamento diferente a cada um deles. É esta

13. N.E.:Voice-over-intenet-protocol, ou protocolo de voz sobre IP 14. N.E.: P2P ou peer to peer (do inglês: ponto-a-ponto): rede linear, rede distribuída ou rede não hierárquica é uma topologia de redes caracterizada pela descentralização das funções na rede, onde cada terminal realiza tanto funções de servidor quanto de cliente. Fonte: Wikipedia

forma de discriminação que ainda não foi totalmente examinada e, de certa forma, é a mais problemática. No *traffic shaping*, não há como o usuário saber que foi discriminado, caso a discriminação tenha sido uma mera alteração no ritmo ou desempenho da sua transferência de dados. Hoje em dia a engenharia de redes tem segregado o tráfego de VoIP na Web para prover, por exemplo, serviços privados de telefonia VoIP a universidades e empresas.

:: SEGREGAÇÃO DE APLICATIVOS E A DEMARCAÇÃO DA INTERNET

Na história da comunicação há vários exemplos de maneiras engenhosas de se fazer censura aos meios de comunicação, sem precisar se embrenhar nos conteúdos. Esta linha de estratégia está bem viva na Internet, atuando de forma muito sutil, empregando a quarta forma de manipulação de tráfego: priorização e condicionamento do tráfego.

As regras de neutralidade propostas por Wu em 2003 permitiriam que os provedores de serviços discriminassem o tráfego se fosse necessário "evitar que alguns usuários de banda larga interferissem no uso que outros usuários fazem das suas conexões com a Internet". Um exemplo aceitável de censura que se coloca são os "limites neutros ao uso da largura de banda". Isso parece justo: pedir àqueles cujo uso é maior que paguem mais, ou limitar o tamanho da capacidade provida ao tamanho do seu orçamento (estabelecer um "teto" de uso), não parece ter nada a ver com censura. Entretanto, uma vez que as aplicações de Internet apresentam enormes disparates quanto às exigências em termos de largura de banda e latência, como funcionariam de fato essas limitações neutras ao uso de largura de banda? Por sorte, sabe-se a resposta, pois esses tetos são bastante usados no gerenciamento do tráfego e de despesas dos *backhauls*[15].

Embora a idéia de discriminação de tráfego na Internet costume evocar o governo de Cuba, o vilão dessa história - se é que há vilão -, é a Universidade da Califórnia, em Berkeley. Em 2002, à medida que o entrosamento através da Internet continuava ganhando espaço junto aos estudantes, a universidade foi ultrapassando a largura máxima de banda que estava no seu orçamento. Quando a conexão de Berkeley com a Internet ficou saturada e o desempenho decaiu, os engenheiros de rede precisaram tomar providências urgentes para resolver o problema. Primeiro, pediram à reitoria que investisse mais 50 mil dólares em largura de banda; depois, começaram a procurar um condicionamento de tráfego que estivesse coerente com as propostas de neutralidade da aplicação feitas por Wu em 2003. Conforme foi descrito em um trabalho publicado no sítio do Grupo de Estudos sobre Internet 2.0 e P2P, o campus foi dividido em duas regiões:

15. Backhaul é um ponto de transmissão de dados para uma espinha dorsal de rede (ou backbone)

os alojamentos e o que eles chamavam de "ROC" (*rest of campus*, ou resto do campus)[17]. Ao separarem esse tráfego, conseguiram estabelecer tetos diferentes para cada região. A análise da estratégia se referiu (provavelmente de brincadeira) aos alojamentos como a "má vizinhança" da rede. Estava claro que o crescimento do tráfego das comunicações entre os alunos era o problema que precisava ser resolvido. Em alguns casos em que se estabelece um teto de uso, se o tráfego não for priorizado, a aplicação de limites neutros e gerais de largura de banda pode ser muito pior do que uma limitação específica ao P2P. Quando os alojamentos atingem seu limite, sofre todo o tráfego da Internet no campus. O condicionamento do tráfego nesse caso é uma tentativa de limitar uma aplicação específica, mas é coerente com as regras de neutralidade pois o critério é claramente a geografia (alojamentos vs. "ROC"). Em suma, é uma demarcação.

É fácil achar um exemplo como este, pois as universidades divulgam seus relatórios internos rotineiramente. As operadoras privadas decerto também restringem o tráfego com base na geografia, mas não há análise e controle público dos mecanismos empregados, que são técnicos e inescrutáveis.

Uma vez que você comece a procurar, fica fácil encontrar decisões tomadas no âmbito de uma rede de um provedor de serviços de Internet que obviamente têm grande efeito sobre o uso da Internet e podem ser mudadas de forma a manipulá-lo ou censurá-lo. Um exemplo é a assimetria das conexões via DSL, cujo projeto visa a privilegiar *downloads.* Produzir informação, e não somente recebê-la é uma função importante da Internet e, com um arcabouço normativo para comunicação, fica mais claro que liberdade para produzir é um requisito básico para que a rede atenda às necessidades de uma democracia participativa.

:: A NEUTRALIDADE DA REDE E A NOVA VIA PÚBLICA

Howard Waltzman, assessor de telecomunicações para o comitê do Congresso dos EUA que planejou revisar a Lei das Telecomunicações, foi citado em 2006 reclamando que as propostas de "neutralidade de rede" para a Internet "transformariam os links de banda larga em ferrovias". Trata-se de uma reclamação sobre as leis e políticas para a Internet surpreendentemente comum; autores de todas as linhas gostam de justificar seus argumentos sobre a especificidade da Internet brandindo exemplos de infraestruturas de comunicação cujos dias de glória já passaram.

Do ponto de vista das políticas públicas, a abordagem mais útil é comparar, mas não exatamente contrastar a Internet com infraestruturas históricas como a das ferrovias. Ante o fascínio do jargão e dos novos recursos tecnológicos, a tendência nos debates em torno de

17. - Ver o documento anônimo, "Campus Bandwidth Management" em http://p2p.internet2.edu/documents/CBMMatrix.pdf

avançados sistemas de comunicação é a de seguir agindo como se todos os problemas relativos às políticas públicas atuais fossem novos. Embora a Internet seja nova, essas questões públicas não o são.

Um bom recurso onde se pode observar provas disso é na análise feita pelo falecido cientista político Ithiel de Sola Pool, do MIT, propondo que devem ser aplicadas regras de não discriminação às novas tecnologias de comunicação[18]. Pool explica vigorosa e detalhadamente que devem ser aplicados princípios semelhantes aos da neutralidade da rede também à televisão e a outras mídias eletrônicas nos EUA, idéia essa que não foi adotada. É notável observar que muitas de suas conclusões são idênticas a muitos dos princípios hoje defendidos sob o rótulo de neutralidade de rede. Em suas "políticas para a liberdade"[19] , Pool argumentou que:

1. todos os canais de comunicação devem ser tratados igualmente;
2. as regras devem ser as mesmas, quaisquer que sejam os usos e conteúdos da comunicação;
3. não se pode permitir que monopólios proprietários de canais de comunicação alavanquem seu poderio até chegar ao controle do conteúdo;
4. a verdadeira não discriminação implica no cumprimento das garantias de interconexão;
5. o cumprimento da não discriminação depende de que as empresas de telecomunicações revelem informações sobre suas operações;
6. a aplicação da lei precisa ser pós-fato para ser bem sucedida;
7. a regulação deve significar uma carga o mais leve possível;
8. as proteções da propriedade intelectual, tais como direitos autorais devem ser revisadas para se tornarem menos restritivas nas mídias eletrônicas.

A análise de Pool captura *ipsis literis* muitos dos argumentos levantados por Tim Wu nos debates sobre a neutralidade da rede. Equipara-se quase na íntegra a materiais encontrados em documentos de políticas públicas atuais. O que une o argumento apresentado por Pool em 1983 aos debates acerca da neutralidade de rede e do acesso aberto é seu fundamento na política da concorrência. Em todas essas áreas, as análises econômicas são usadas para promover a causa da concorrência - embora o material da década de 2000 seja mais provavelmente enquadrado como "política de inovação" e enfatize a concorrência entre provedores de infraestrutura e serviços ou entre eles e terceiros. Pool, por sua vez, simplesmente escreveu sobre facilitar a entrada de pequenas operadoras e sobre o uso de "tecnologias novas".

Pool remonta as comparações e justificativas para a não discriminação a um passado remoto.

18. O premiado livro Technologies of Freedom (1983), que não é mais editado. 19. Technologies of Freedom, p. 246-249.

Ele revê a regulação das ferrovias, comenta sobre canais e estradas, e tece extensas considerações sobre televisão a cabo, serviços postais, tele e radiodifusão.
O termo que inclui regras de não discriminação nesses contextos é a expressão "operadoras de vias públicas "[20]. Trata-se de um conceito jurídico da *common law*[21] que pode remontar ao Império Romano (para obter uma análise mais completa, consulte Noam, 1994). Em suma, uma operadora de via pública é uma entidade privada que oferece serviços de transporte ou comunicação e está sujeita a obrigações públicas específicas em troca de benefícios legais. A principal obrigação das operadoras de vias públicas é a não discriminação: elas precisam se incumbir de operar para todas as pessoas indiscriminadamente[22]. (Isto se encontra, é claro, no cerne do debate acerca da neutralidade de rede.) As operadoras de vias públicas incluem as ferrovias, os táxis, os aviões e os telefones[23].

Em troca dessa imposição da não discriminação, as operadoras de vias públicas receberam vários benefícios: acima de tudo, proteção contra a responsabilidade pelos conteúdos que carregam. Como podem não tomar conhecimento do conteúdo que transportam, não se responsabilizam pelo transporte de propriedade roubada: não se pode processar a empresa de telefonia por violação de direitos autorais caso um telefone seja usado para a leitura em voz alta de uma obra com direitos de *copyright* assegurados. As operadoras também não podem ser responsabilizadas por nenhum outro conteúdo ilegal: mensagens ofensivas ou indecentes, ou ameaças de morte. Além disso, as operadoras de vias públicas podem usar vias e infraestrutura públicas para prover seus serviços e podem receber outros benefícios[24].

Há várias conclusões a serem tiradas dessas comparações: uma das que importam é que a neutralidade da rede é um problema antigo que já foi muito abordado de várias maneiras que tinham a ver com os contextos histórico, político e tecnológico de cada época.

::CONCLUSÃO: UM MAPA PARA O TERRENO CONFUSO E ASSIMÉTRICO DE UMA INTERNET TENDENCIOSA?

Os argumentos levantados neste ensaio até o momento podem ser recapitulados rapidamente.
A Internet não é neutra agora.
A maior parte do debate sobre a Internet se concentra em torno de alguns tipos de discriminação de conteúdo, embora haja muitas variedades mais em jogo. O enfoque do debate sobre a neutralidade da rede pode ter sido sobre os aspectos legais, sim, mas o problema da discriminação de conteúdo costuma

20. N.E.: O termo no original em inglês é *common carriage*. 21. N.E.: A *Common Law* provém do direito inglês não escrito que se desenvolveu a partir do século XII. São princípios jurídicos e regras - que regulam a posse, o uso e a herança da propriedade e a conduta dos indivíduos -, cuja origem não é claramente conhecida e que são observadas desde períodos remotos da antiguidade, baseadas em usos e costumes. Fonte: Catholic Encyclopedia - http://www.newadvent.org/cathen/09068a.htm 22. - Outras obrigações foram impostas às operadoras de vias públicas em momentos distintos. Por exemplo, são impostos padrões mais elevados de serviços às operadoras em contextos em que há monopólio. 23. N.E.: Em inglês, o termo *common carrier* se refere a transportadoras, a serviços de telecomunicações e a alguns outros serviços públicos. 24. Por exemplo, as operadoras de vias públicas podem receber poder de domínio eminente.

ser de caráter tecnológico. Já existem muitas formas de discriminação sendo praticadas – normalmente em segredo – e não está claro, de forma alguma, que todas elas sejam uma má idéia. Os debates atualmente existentes sobre a neutralidade da rede parecem novos, mas ecoam debates acerca da operação de vias públicas que já têm um século de idade. Um exame dos textos propondo regras de não discriminação a partir do histórico da operação de vias públicas mostra que essas regras não eram absolutas.

O esforço empreendido neste ensaio nos trouxe aqui apenas com o propósito de apontar que, quando um corpo político considera aprovar uma lei sobre qual conteúdo pode ser favorecido em detrimento de outro, seria útil contar com algum conceito normativo a respeito daquilo para que a comunicação deve se prestar. Falta tal conceito nos atuais debates, que se estruturam em termos de proteger uma Internet neutra que não existe, e em termos de estimular a competição.

> Por quanto tempo caberá continuarmos acreditando na ficção de que a Internet é neutra?

Até o testemunho parlamentar mais recente sobre as regras acerca da neutralidade da rede foi escrito como se a Internet fosse neutra e como se o congresso devesse agir no sentido de "preservar" o campo "em iguais condições de jogo para todos". É claro que tais argumentos se estruturam de maneira estratégica e a nova regulação não é palatável dentro do clima de desregulamentação implantado no início do Século XXI. Ainda assim, por quanto tempo caberá continuarmos acreditando na ficção de que a Internet é neutra? Qualquer clamor por uma "legislação que proteja o ambiente para a inovação e a competição na Internet conforme a Internet propiciou em sua origem[25]" acena com uma Internet fictícia. Conforme demonstram alguns dos exemplos aqui apresentados, a discriminação de conteúdo é generalizada na Internet, e já se encontra disseminada demais para desaparecer. Em lugar de enquadrar o problema como uma questão de meramente escrever uma regra de concorrência neutra para uma Internet neutra, a abordagem mais útil seria assegurar o terreno diversificado para a rede desigual de hoje e trabalhar no sentido de elaborar uma justificação normativa para sistemas de comunicação que atendam ao público, fornecendo assim ao juiz, ao regulador e ao crítico, igualmente, uma ferramenta analítica que possa ser usada para determinar quais atos de discriminação são bons e quais não são. ●

25. Lessig, Endell, & Carlsmith, 2006:11

Alex Gakuru Diretor da ICT Consumers Association of Kenya (ICAK), consultor especialista em Tecnologias da Informação e Comunicação e membro da Coalizão da Sociedade Civil para a Liberdade de Informação no Quênia.

Controle privado da Internet

e os prejuízos para o desenvolvimento da África

"A Internet está prestes a mudar, deixar de ser uma supervia de informação livre e passar a ser controlada por grandes fortunas. Como resultado, você pode perder o seu Yahoo, Hotmail, Gmail e outras contas gratuitas de e-mail, ou elas podem tornar-se mais lentas ou pagas...", dizia um artigo num jornal queniano[1] em 15 de junho de 2006.

Entre as reações suscitadas, manifestaram-se preocupações de que o autor estaria tentando assustar os usuários – potencialmente desestimulando a adoção crescente e o uso mais amplo da Internet. Uma consultora em terceirização tomou nota do artigo por causa das suas implicações para o exercício da sua profissão. Semanas mais tarde, sem que tenham ocorrido "revelações chocantes" sobre o fenômeno assustador, a questão saiu do debate público, como sempre esquecida no fundo de algum arquivo.

Em novembro de 2007, motivada por sua necessidade de manter-se atualizada com seu escritório e sua correspondência eletrônica pessoal, uma jovem comprou um telefone celular Nokia 66 10i habilitado para

1. "Internet heads for 'dark' days", Horizons Magazine, The Daily Nation,15 de junho de 2006. Ver http://www.nation.co.ke/magazines/artandculture/-/1222/128350/-/ae95tkz/-/index.html .

Internet. Sua decisão seguiu-se a uma campanha de propaganda maciça em praticamente toda a mídia local. Tentada pela conveniência de um serviço "*always on*" de Internet de bolso por conexão GPRS [Serviços de Rádio de Pacotes Geral], que então custava apenas centavos, ela pensou que o investimento mais alto no aparelho valia a pena.

Foi muito fácil adquirir o serviço. Assinantes só precisavam enviar uma curta mensagem de texto para um número fornecido pela operadora de celular, e as configurações eram enviadas ao usuário quase imediatamente. Bastava salvar as configurações, desligar o telefone por alguns minutos e então religá-lo, e a pessoa estava conectada à Internet. Nenhuma necessidade de chamar assistência técnica e nenhum contrato a assinar – mas também nenhuma ciência dos termos e condições associados ao serviço. Incluíam-se entre esses termos e condições a aceitação da degradação dos serviços de dados e a preferência aos serviços de voz sempre que o operador da rede julgasse necessário.

O serviço era bom, e esta consumidora de Internet (este é o modo como nossa associação prefere referir-se a usuários de ferramentas modernas de informação e comunicação) pôde receber suas mensagens através do Gmail e respondê-las como desejava e onde quer que estivesse. Devido ao aumento percebido de disponibilidade, escolha e conveniência, ela talvez tenha se gabado um pouco dizendo que tinha dado "um tchau aos cibercafés abarrotados," certa da sua nova conexão funcionando dia e noite a um custo de centavos, em comparação ao preço mínimo de dez xelins cobrados pelos cibercafés.

Mas a situação começou a mudar em janeiro de 2008, com o surgimento de um problema de intermitência do serviço. A conexão deixou de ser rápida e tornava-se mais difícil durante o dia, em comparação com a noite. Listas de e-mails com reclamações foram enviados à companhia – tendo em vista a impossibilidade de acesso a assistência técnica – e as respostas traziam a sugestão de desligar o telefone por alguns minutos e ligá-lo outra vez. Embora inicialmente isso funcionasse, logo tornou-se um ritual frustrante, que não parecia trazer uma solução permanente para a conexão problemática.

Os problemas pioraram em fevereiro e, ao tentar acessar a sua tela de login no Gmail, ela começou a receber a mensagem de erro "Rede não disponível". Ela ficou bastante frustrada, tendo em vista que somente cinco semanas tinham se passado desde seu investimento num aparelho caro, motivada pela possibilidade de trocar mensagens de e-mail com sua lista de contatos preferida no Gmail, os quais ela não conseguia mais acessar. Por alguma razão, porém, seu telefone podia acessar o login do Yahoo - e assim ela abriu uma conta de e-mail no Yahoo. Usou-a até abril, quando novamente a mesma mensagem de erro "Rede não disponível" começou a aparecer o tempo todo, tornando o seu investimento sem sentido, se levarmos em conta seu propósito inicial.

Mais ou menos na mesma época, a companhia de telefonia celular acabara de introduzir um novo serviço de dados em "banda larga", e vários anúncios "estimulavam" o usuário a migrar de serviço –

se "desestimulavam" ou não o serviço GPRS em prol da mais lucrativa "banda larga", é discutível, mas altamente provável. Sendo ou não este serviço qualificado como "banda larga" por padrões internacionalmente aceitos, o fato é que os consumidores no Quênia não eram (e a maioria ainda não é) tecnicamente capacitados para dizer se o serviço é mesmo de banda larga. Felizmente, o problema da "propaganda enganosa" será regulamentado num Decreto de Proteção ao Consumidor que está sendo proposto no país, e o governo reconhece a necessidade de revisar a lei de proteção aos consumidores de Tecnologia de Informação e Comunicação (TIC).

Obviamente, a jovem consumidora desta história nunca foi informada de cláusula(s) que especificasse(m) a prioridade do tráfego de voz sobre o tráfego de dados nos termos e condições dos serviços, considerando-se que ela nunca assinou um contrato e supondo-se que ela teria compreendido e aceito os termos e condições do serviço, caso estes tivessem sido apresentados.

Ao lançar o Programa de Educação do Consumidor do órgão regulador da indústria de telecomunicações do Quênia, o ministro Samuel Poghisio[2] disse: "Sob a lei vigente, as poucas cláusulas que visam salvaguardar os interesses dos consumidores estão dispersas em vários estatutos diferentes e longe de serem adequadas. Este cenário prevalece na indústria de TICs. O governo deve continuar a revisar a lei em consulta estreita com grupos de consumidores e outras partes interessadas, em vista de garantir que esta anomalia seja enfrentada." [3]

:: ESPECULAÇÃO COM OS CONTEÚDOS DAS REDES

Curiosamente, apesar de não acessar o Gmail e o Yahoo, o telefone de nossa jovem consumidora conseguia acessar a página inicial da operadora de serviços Internet, o que a fez perguntar-se como isso era possível, "já que não havia Internet?" Pelo visto, a operadora também tinha passado a oferecer serviços de e-mail gratuitos, - os quais a consumidora, incomodada, resolveu experimentar, enviando para uma amiga uma breve mensagem de texto sem formatação como teste. Este serviço "gratuito" saiu caro no final, pois ao analisarem a conta do destinatário, assinante da mesma rede, perceberam que foram cobrados 7 xelins pelo recebimento da mensagem.

Entre os motivos para a degradação do serviço GPRS e suas consequências, podemos considerar os seguintes elementos:

a. A percepção, pela empresa provedora de acesso móvel à Internet, de que é uma "*dumb pipe*[4]" e, portanto, poderia especular controlando os conteúdos dos usuários. Tendo oferecido serviços de e-mail

2. Ministro da Informação e Comunicação do Quênia. 3. Discurso do ministro. 4. N.E. O termo "Dumb Pipe", ou "rede de baixo valor" é freqüentemente utilizado para explicar como as operadoras de telecomunicações tradicionais ("incumbents" ou "telcos") estão perdendo o controle sobre os serviços que são entregues através da infraestrutura de conexões e banda que elas próprias fornecem.Nesse cenário, a telco se limita a fornecer conectividade enquanto terceiros fornecem os serviços de maior valor que trafegam na sua infraestrutura de conexão. Em um cenário de "rede de alto valor" ("Smart Pipe"), a operadora provê tanto a conectividade quanto os serviços de maior valor ao cliente final. Fonte: Teleco. http://www.teleco.com.br.

Com as tecnologias modernas de comunicação personalizada, torna-se muito simples visar e isolar um certo indivíduo, impedindo-o de receber informação.

gratuitos, a empresa estaria abusando da propriedade da rede para bloquear alguns sítios e competir com outros serviços de e-mail gratuitos, no caso o Google e o Yahoo.

b. Retenção do cliente: ao oferecer serviços de e-mail vinculados a uma rede, a atitude da companhia é contrária à competição, tendendo à monopolização privada da comunicação dos cidadãos.

c. Migração forçada para seus novos produtos e serviços de Internet. Considerando que o GPRS, que pode ser utilizado em todo o país, não dá tanto lucro, eles projetaram serviços novos de custo mais elevado para os consumidores, assim desencorajando tecnicamente e deliberadamente o uso do GPRS.

d. Maximização dos lucros apresentando produtos de modo equívoco; por exemplo, comercializando uma "banda larga" que não corresponde aos padrões internacionais.

e. Exploração do nível geralmente baixo dos conhecimentos e competências tecnológicos dos consumidores vulneráveis. A consumidora, crendo na possibilidade de conectar-se à página inicial da rede WAP [Protocolo para Aplicações sem Fio], procura o Google ou opta por tentar o Gmail ou o Yahoo. Todavia, tendo feito a escolha, recebe a mensagem perturbadora: "Pode ser que seu telefone não suporte Gmail. Para tentar novamente, clique aqui." Quando ela tenta clicar, recebe "Rede não disponível" como resposta, o que significa que o serviço está indisponível ou desativado. Considerando que o mesmo telefone já havia acessado o serviço antes, a consumidora é levada a suspeitar que o serviço não esteja disponível por causa do seu cartão SIM [Modulo de Identidade do Assinante] ou aparelho de telefone.

f. Outra possibilidade: aparelhos podem ser alvo de ações deliberadas para desabilitar a comunicação de determinada pessoa. Com as tecnologias modernas de comunicação personalizada, torna-se muito simples visar e isolar um certo indivíduo, impedindo-o de receber informação. Neste caso, mais do que apenas uma ação ilegal, esta seria uma violação da garantia constitucional do direito do indivíduo de receber informações sem interferência. E seria uma violação ao direito à liberdade de expressão, uma violação ao Artigo 19 da Declaração Universal dos Direitos Humanos.

g. Desrespeito aos direitos dos consumidores e às condições de licença impostas pelo órgão regulador. O regulador exige que os provedores publiquem

todos os serviços oferecidos em linguagem clara e simples, e que antes que qualquer serviço deixe de ser oferecido, o órgão regulador seja informado a fim de aprovar a suspensão da oferta do serviço – salvo, geralmente, se um novo serviço oferecido em substituição for melhor e mais barato para o consumidor.

Nós, da Associação de Consumidores de TICs do Quênia, estendemos nossa atuação e passamos a fazer o monitoramento de outros provedores de Internet - nos expondo mais amplamente ao risco de censura privada. Logo depois de lançarmos o sítio da associação,[5] recebemos queixas de usuários da Internet que não conseguiam acessá-lo. Isso nos levou a promover uma série de testes que mostraram que, de fato, não era possível acessar nosso sítio a partir de alguns links. Uma campanha de conscientização sobre o problema, feita através de listas de correio eletrônico, resultou no desbloqueio, por uns poucos provedores, do acesso ao nosso sítio - mas nós temos consciência de que nosso papel como protetores dos direitos dos consumidores é manter um esforço contínuo de vigilância.

::INTERNET ABERTA

Na África, ilhas dispersas de conectividade simbolizam a entrada atrasada do continente no mundo conectado em banda larga. A última década testemunhou uma proliferação e crescimento exponencial de pontos conectados à Internet em toda a África, inclusive no Quênia. Estes pontos representam a recém-descoberta compreensão do potencial que esta tecnologia incrivelmente poderosa e capacitante representa para o desenvolvimento. Daí a recepção calorosa pelos povos de uma tecnologia que, diferente de todas as anteriores, não tem um "controle central" que possa vir a determinar o que é (in)apropriado ao seu público.

O fundamento da Internet neste design aberto resultou, no começo dos anos 1990, numa resistência oficial à sua introdução em toda a África, o que encontra-se bem documentado, entre outras fontes, em *Negotiating the Net in Africa: The Politics of Internet Diffusion*[6] (M. Muiruri et. al. 2006),[7] que narra os temores e as questões políticas, econômicas e tecnológicas envolvendo a difusão da Internet no continente.

Uma vez que ficou claro o incrível poder da Internet de mudar o cenário histórico da exploração estrutural do continente, a taxa de crescimento do uso da Internet na África entre 2000 e 2008 é a segunda maior do mundo,[8] atrás apenas do Oriente Médio. O Quênia, como outros países africanos, investiu pesadamente em conectividade por fibra terrestre e submarina. Porém, se a Internet não continuar sendo aberta como a conhecemos, a possibilidade de que venha a libertar a África e assegurar seu desenvolvimento e sua competitividade no cenário mundial

5. Ver http://www.ictconsumers.org/ 6. Negociando a rede na África: As políticas de difusão da Internet 7. Ernest J. Wilson III e Kelvin R. Wong (orgs.), Negotiating the Net in Africa: The Politics of Internet Diffusion. Com um artigo sobre a questão no Quênia: M. Muiruri. Kenya: Diffusion, Democracy, and Development.
8. O crescimento foi de 1031,2% entre 2000-2008. Ver http://www.Internetworldstats.com/stats1.htm , consultado em 30 de setembro de 2008.

fica ameaçada, e os fundos públicos investidos em infraestrutura terão sido um desperdício.

::TECNOLOGIAS CONEXAS E QUESTÕES SOCIAIS

Estreitamente ligados ao tema da neutralidade da rede, estão as preocupações com a privacidade e o medo de que a tecnologia seja usada para limitar o caráter aberto da Internet. Avanços técnicos, junto com a combinação de firewall, detecção de invasão e tecnologias de prevenção resultaram na tecnologia de filtragem de pacotes na rede, a Inspeção Profunda de Pacotes (DPI) - que analisa os conteúdos das comunicações que transitam na rede. Isto possibilita não só o fornecimento de serviços em camadas, mas a reconstrução total do tráfego. Usos típicos da tecnologia DPI pelos provedores de serviços Internet incluem interceptação legal, definição de políticas e de sanções orientadas para a diferenciação entre propaganda e serviços, a combinação de ofertas de conteúdos com níveis diferenciados de preço e a imposição de pagamento de *copyrights.*

Ao utilizarem estas tecnologias em suas redes, de uma hora para outra os provedores de acesso passam a saber muito mais sobre seus usuários e seu tráfego. Eles também adquirem a capacidade de bloquear, conformar, monitorar e priorizar este tráfego em qualquer direção. De repente, torna-se simples, digamos, priorizar a entrada de tráfego de um sítio qualquer que tenha dado ao provedor de acesso uma mala de dinheiro, enquanto os demais sítios brigam pelo tráfego nos canais "engarrafados".

Esta tecnologia hoje é usada por empresas, provedores de acesso e governos e, numa ampla gama de aplicações, será usada para limitar o caráter aberto da Internet. Além de usar a inspeção de pacotes para a segurança das suas próprias redes, os governos da América do Norte, da Europa e da Ásia a usam para vários fins de vigilância e censura em muitos projetos confidenciais.

Técnicos dizem que a privacidade não existe na arena da informação e das comunicações, ao passo que defensores dos direitos humanos advogam que ela deve existir e ser observada, apresentando provas contundentes das conseqüências quando esses direitos são violados. Ambos os argumentos se sustentam, mas suscitam a questão: quem ou o que está certo?

No Fórum sobre Governança da Internet (IGF)[9] em 2007, foi sugerido que só devemos escrever em e-mails o que pode ser dito na

9. Http://www.intgovforum.org/

frente da própria mãe ou escrito num cartão postal, pois seria imprudente para qualquer um confiar de forma excessiva em comunicações eletrônicas. Na defesa da era da convergência, o movimento social deve "convergir" com a comunidade técnica. "Os técnicos tendem a se dividir em duas categorias: especialistas e generalistas. O especialista aprende cada vez mais sobre um campo cada vez mais estreito, até finalmente, no limite, saber tudo sobre nada. O generalista aprende cada vez menos sobre um campo cada vez mais amplo, até finalmente não saber nada sobre tudo", disse William Stucke.[10]

:: RESISTIR AO CONTROLE PRIVADO DA INTERNET

A rede neutra é aquela que não tem restrições quanto aos tipos de equipamento que podem ser acoplados, sobre os modos de comunicação permitidos; ela não restringe conteúdos, sítios ou plataformas, e nela um fluxo de comunicação não é absurdamente degradado por outros fluxos de comunicação. Quando um dispositivo de filtragem de informação é inserido entre as comunicações de dois usuários, interferido desse modo na comunicação ponta-a-ponta, a natureza *on-line* da Internet é perdida. A liberdade reconhecida de receber e disseminar informação, expressão e cultura estará perdida se a batalha pela neutralidade for perdida.

Ironicamente, essas reconhecidas liberdades correm o risco de perder a batalha- não para os monopólios estatais vigentes nas telecomunicações, nem para os ditadores, ou para a corrupção, para o analfabetismo, para a doença ou para outras imagens que os países do Norte têm do continente africano -, mas sim para as mesmas velhas forças colonialistas que são provedoras da informação e das comunicações. Isso também representa um golpe contra os ganhos em transparência e governança, e contra as iniciativas bem-sucedidas de liberdade de informação na África. E, além disso, dá espaço e cria argumentos para ditaduras moribundas reprimirem a expressão e negarem os avanços democráticos.

> Cabe lembrar que as tecnologias de comunicação modernas foram introduzidas na África por forças externas a fim de incrementar interesses e objetivos outros que não os dos povos africanos.

Uma característica importante da Internet é que o acesso e o alcance das comunicações hoje são globais, em contraste com a situação no passado, quando eram estruturados em conformidade com as divisões geopolíticas da ordem imperialista.[11] A natureza aberta da Internet possibilitou que pontos conectados na África, por poucos que sejam, participassem do ecossistema do conhecimento e pôs em questão a desinformação e as representações equivocadas do passado.

10. William Stucke, presidente da AfrISPA, membro fundador e presidente da Internet Society, South Africa Chapter. 11. Ibid.

A Internet aberta – conforme a conhecemos hoje – ameaçou os controladores da comunicação, mediadores da velha ordem mundial há muito estabelecida, que exerceram deliberadamente o controle priorizando a informação que fortalecia o Norte e reforçando, com a amplificação de relatos negativos, o pessimismo africano.[12]
É fundamental lutarmos até podermos falar de uma "África vibrante",[13] confiante, com pleno acesso à informação, a públicos e a mercados globais.

::CONCLUSÕES

Sofisticadas infraestruturas de informação, comunicações e tecnologias - cuja propriedade é principalmente de países do hemisfério Norte – impõem riscos aos contínuos esforços para a redefinição das prioridades para o desenvolvimento do Sul e ameaçam a exposição eficaz desta agenda às audiências globais, e a apoiadores em potencial.

Cabe lembrar que as tecnologias de comunicação modernas foram introduzidas na África por forças externas a fim de incrementar interesses e objetivos outros que não os dos povos africanos. A chegada do telégrafo e a colocação de cabos submarinos em todo o continente desde o final dos anos 1880 tinha objetivos explícitos de domínio político e militar imperialista e de exploração comercial colonialista. Significativamente, é por isso que as primeiras conexões de telégrafo e de telefone correm paralelamente às redes ferroviárias rumo às áreas de mineração e de exploração de outras matérias-primas. [14]

O "Renascimento Africano" tentou mostrar abertamente a ira e a vergonha sentidas em nível muito pessoal e profundo - em relação ao estado do continente africano, aos horrores infligidos aos seus povos, e em relação à percepção que o restante do mundo tem da África e dos africanos.[15] Alfred Sauvy observou: "... pois afinal este Terceiro Mundo ignorado, explorado e desdenhado como o Terceiro Estado quer ser alguma coisa também..."[16]

Neste pano de fundo, é do maior interesse da África preservar a neutralidade da rede. Até porque, a maioria das companhias de telecomunicações na África e em outros "mercados emergentes" são possuídas e controladas por países ricos do Norte. A menos que a Internet seja mantida neutra, fatores estruturais responsáveis pelo fracasso do desenvolvimento da África tornarão a se manifestar. No momento mesmo em que a Internet ofereceu uma esperança de mudança, os interesses privados colonizadores do Norte estão se entrincheirando no coração da tecnologia, com seu potencial devastador – capaz de obstruir todas as esperanças de desenvolvimento. ●

Tradução de Renato Aguiar

12.Graça Machel-Madela, "É tempo de nós [africanos] agirmos individual e coletivamente para reverter o Pessimismo Africano", NEPAD APRM Kenya Country Support Mission, KICC (Nairobi), Junho de 2004. 13.Discurso de Masahiko Koumura, Dar Assalaam, Tanzânia, 4 de janeiro de 2008. 14.Kwame KariKari (discurso na FoE Nairobi Conference, 2007). 15.P. L. Berger, S. P. Huntington, Many Globalizations: Cultural Diversity in the Contemporary World, pp. 235 (ISEC, Boston University). 16. L'Observateur, 14 de agosto de 1952 http://en.wikipedia.org/wiki/Alfred_Sauvy http://en.wikipedia.org/w/index.php?title=L'Observateur&action=edit&redlink=1

Prof. Dr. Jorge Alberto S. Machado Docente do curso Gestão de Políticas Públicas, da Universidade de São Paulo

Segurança e combate ao terrorismo:

uma breve análise da lei de retenção de dados na Alemanha

Imagine, leitor, todas as suas comunicações por telefone, celular, e-mail e navegação na Internet sendo registradas e armazenadas durante três anos. Refiro-me a seus dados pessoais, a origem, destino e conteúdo dos e-mails enviados, suas ligações telefônicas, dados de horários de conexão com a Internet e com servidores, etc. Essa informação toda não estaria apenas acessível a órgãos de segurança, mas também a empresas (para controlar, por exemplo, se houve violação dos direitos de propriedade intelectual), e mesmo a pessoas físicas – talvez algum desafeto, seu chefe ou algum concorrente. E mais, todos os provedores de seu país onde estão armazenadas as contas de e-mail estariam obrigados a entregar aos organismos de segurança nacional a senha administrativa de acesso. Estes poderiam navegar livremente nesse oceano de informações dos usuários. Isso não é ficção, já existe. Desde janeiro de 2008, está vigorando na Alemanha a lei de segurança sobre informações, a *Telemediengesetz* ("Lei de

> Sendo tão amplas as possibilidades de quebra de sigilo nos dados, se antes eram as exceções que permitiam que isso ocorresse, agora o sigilo é que pode ser considerado uma exceção.

Telemédia"). Seu objetivo é reter dados de telecomunicações entre os cidadãos com o objetivo de combater o crime e, em especial, o terrorismo.

O alcance da lei é relativamente semelhante, em termos de quebra da privacidade do cidadão, às emendas à FISA[1], aprovadas em 10 de julho de 2008 nos Estados Unidos. A lei de Telemédia, entre outras medidas, prevê a retenção de dados de todas as comunicações telefônicas (telefonia fixa e móvel), e-mails, assim como as informações sobre remetentes, destinatários, origem, data, local, máquinas utilizadas. Isso significa que todas as comunicações entre os cidadãos no país podem ser rastreadas, monitoradas e analisadas, não havendo mais privacidade entre as mensagens pessoais. São coletadas informações sobre preferências, hábitos pessoais e circunstâncias de vida de cada cidadão. O acesso a tais dados é garantido à policia, a promotores públicos, a serviços secretos e a autoridades de outros países. Tudo para "combater o crime".

:: UMA LEI QUE PODE VIRAR MODA NA EUROPA

A Lei de Telemédia se insere no quadro da Diretiva Européia 2006/24/EC. Aprovada em 15 de março de 2006 pelo Parlamento Europeu, a diretiva trata sobre "a retenção de dados gerados ou processados em conexão com a provisão de publicidade dos serviços eletrônicos de comunicações públicas ou redes de comunicações públicas, emendando a Diretiva 2002/58/EC". Seu objetivo é combater *spam*, identificar autores de páginas na Internet e obrigar os servidores a dispor os dados pessoais dos usuários de serviços no caso de conflitos privados específicos sobre conteúdos disponibilizados na rede.

Embora seja apenas "complementar" à diretiva européia, a lei alemã apresenta vários problemas:

- o escopo da retenção de dados constitui uma invasão excessiva na privacidade pessoal;
- ameaça atividades profissionais (como jornalismo) e políticas que demandam sigilo por questões éticas ou morais;
- viola o direito humano à privacidade;
- seu custo, em termos dos direitos fundamentais infringidos, é muito alto e não há evidencias de que seja eficiente no combate ao terrorismo;
- causa constrangimentos aos cidadãos e aos negócios;

1. N.E.: Foreign Intelligent Surveillance Act. Ver em http://www4.law.cornell.edu/uscode/50/ch36.html

- discrimina e promove uma invasão excessiva na intimidade dos usuários de telefonia e serviços de Internet em comparação com quaisquer outros meios de comunicação (por isso tem sido chamada de Lei "Big Brother").

A parte mais polêmica está no seu artigo 14. Há uma cláusula nele que diz que os provedores de Internet têm que entregar os dados pessoais- como nome, endereço ou senha pessoal - aos órgãos responsáveis para o cumprimento da lei. A justificativa para isso pode ser: "perseguição de crimes", "o cumprimento dos dispositivos de 'proteção ao cidadão' da Constituição alemã e dos Estados federativos", "prover de informações o serviço secreto federal *(Bundesnachrichtendienst)* e o Serviço da Proteção Militar *(Militärischer Abschirmdienst)*" e, pasmem, "garantir o direito de propriedade intelectual". Isso significa que os interesses da indústria da música e do filme são colocados no mesmo nível dos serviços secretos. Formulada de maneira muito imprecisa, a lei permite, por exemplo, que tanto a indústria como indivíduos possam pedir dados pessoais no caso de dúvidas sobre a violação da propriedade intelectual.

Sendo tão amplas as possibilidades de quebra de sigilo nos dados, se antes eram as exceções que permitiam que isso ocorresse, agora o sigilo é que pode ser considerado uma exceção. A lei também é criticada por não regular as condições nas quais os órgãos públicos podem ter o acesso aos dados pessoais. Ela também aumenta a pressão sobre a autoria dos conteúdos que circulam na rede. Em um de seus artigos, a lei atribui mais responsabilidade aos *bloggers*, que passam a ser tratados como jornalistas. No entanto, deixa muitas dúvidas em relação a responsabilidade sobre conteúdos, *links* e serviços nos sítios Web. Como não há uma regulamentação específica sobre isso, na prática não há limites à aplicação da lei.

:: INOVAÇÕES JURÍDICAS E POLÍTICAS

A lei alemã saiu na frente e chama a atenção pelas seguintes características:

- é a mais rígida já implementada – complementar às diretivas européias de segurança, recrudesce-a enormemente;
- pode influenciar a implementação de leis semelhantes de combate ao terrorismo que têm sido discutidas nos países-membros da União Européia, servindo assim como paradigma para o tratamento de dados das comunicações digitais por parte de governos;
- impõe severas limitações às liberdades civis constitucionais, em especial à privacidade e à liberdade de expressão;
- traz inovações jurídicas ao contrapor o princípio da segurança às liberdades civis, dando mais peso ao primeiro, propiciando assim novas abordagens - não só jurídicas, como políticas - ao tema.

O "combate ao crime", em especial ao terrorismo e à pedofilia, tem sido usado como justificativa para convencer legisladores e cidadãos pouco informados a aceitar leis tão invasivas. Os *lobbies* dos grandes veículos de comunicação e das organizações que reúnem

gravadoras e estúdios de cinema têm pego carona na discussão para defenderem a manutenção de seus lucros, corroídos pela difusão das modernas tecnologias digitais, que tornaram banal o ato de transmitir e compartilhar arquivos. Mesmo considerando a diferença da natureza dos crimes, essa estratégia tem dado certo e a "violação da propriedade intelectual" tem sido posta como delito de igual importância ao terrorismo e à pedofilia.

O Comissário de Justiça e Segurança da União Européia, Franco Fratini, indicado por Berlusconi, defende a implementação de um sistema de filtragem em toda a Europa. Em boa parte dos países-membros tem se discutido propostas de controles sobre a rede que afetam a privacidade dos cidadãos e/ou a neutralidade da rede. Na Dinamarca e na França, tem sido discutidas propostas que permitem a quebra de sigilo dos provedores para controle sobre o compartilhamento de arquivos protegidos por *copyrights*. Na Grã-Bretanha estuda-se a implementação de medidas semelhantes a partir de 2009, caso os provedores não entreguem os dados dos usuários de forma amigável quando solicitados. Na Itália, para facilitar as investigações policiais, há um sistema nacional de filtragem aplicado ao único *backbone* que serve ao país. Curiosamente, o primeiro-ministro Silvio Berlusconi conseguiu aprovar no dia 22 de julho de 2008 uma lei que lhe garante a imunidade contra os processos de investigação que responde enquanto for primeiro-ministro.

:: O "BIG BROTHER" ESTARÁ CHEGANDO À INTENET BRASILEIRA?

A implementação da lei alemã deve ter influência sobre as políticas de segurança nos meios digitais adotadas por outros países do mundo. No Brasil, tramitam no Congresso vários projetos de leis sobre cibercrime, de defesa à propriedade intelectual e combate à "pirataria" que resultariam, se aprovadas, na aplicação de medidas invasivas em nome do aumento da segurança e da proteção de negócios nas redes digitais. O senador mineiro Eduardo Azeredo (PSDB) apresentou um substitutivo, aprovado no Senado, para três projetos que visam regular a Internet no Brasil (PLS 76/2000, PLS 137/2000 e PLC 98/20030).

A proposta do senador Azeredo, que vai à votação na Câmara dos Deputados, tem sido objeto de grande polêmica. Ela obriga a identificação dos internautas pelos provedores de acesso. A estes cabe impedir o acesso anônimo à rede, registrar e armazenar dados de conexões - como horários de entrada e saída, tempo de permanência na rede, os dados capturados (como músicas e imagens) -, e guardá-los por no mínimo três anos. O provedor terá de arquivar também informações do internauta como nome, endereço completo, data de nascimento, número do CPF, carteira de identidade e telefone. O projeto de lei determina que cabe aos provedores a responsabilidade sobre a veracidade das informações prestadas pelo usuários, e coloca-os sob

pena de responderem judicialmente por possíveis incorreções. Aos provedores cabe também denunciar usuários suspeitos às autoridades – o projeto de lei atribui aos primeiros a tarefa de vigilância e controle que deveria caber ao poder público.

Alguns dos pontos mais polêmicos do Projeto são os que mudam os artigos 285-A e 285-B do Código Penal:

Art. 285-A. *Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:*

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Art. 285-B. *Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível:*

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

O projeto de lei define de forma muito ampla o que é um "dispositivo de comunicação" ou "sistema informatizado":

I – dispositivo de comunicação: *qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;*

II – sistema informatizado: *qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;*

Assim, qualquer coisa que transmita ou armazene dados pode ser enquadrada como tais dispositivos ou sistemas, segundo a descrição do artigo 285-A. Como a lei de direitos autorais não permite cópia sem autorização, qualquer cópia simples que o usuário faça de um CD ou DVD legalmente adquirido, incorre em crime.

> Pela lei do senador Azeredo, dezenas de milhões de brasileiros poderiam ser condenados de um a três anos de reclusão.

Pela lei do senador Azeredo, dezenas de milhões de brasileiros poderiam ser condenados de um a três anos de reclusão. A descrição do artigo 285-B força o estabelecimento na prática de um sistema de autorizações na Internet, uma vez que, por padrão legal, os direitos autorais sobre obra artísticas ou culturais são automaticamente protegidos, já tendo, portanto, proteção expressa por lei.

O projeto do senador Azeredo prevê também a retenção de dados dos usuários por três anos. Mesmo a Convenção de Budapeste de combate ao cibercrime, bastante rígida em suas disposições, estabelece o prazo de três meses para isso.

Tal projeto afronta direitos fundamentais de privacidade, liberdade de expressão e acesso à cultura, consagrados respectivamente nos artigos 12, 19 e 22 da Declaração Universal dos Direitos Humanos e consagrados na Constituição Brasileira. Se implementada, essa lei poderia ser o primeiro passo para transformar a Internet brasileira num *Big Brother,* acabando com a liberdade e a privacidade dos usuários, sujeitando os internautas à bisbilhotagem geral e deixando-os a mercê de ação de juízes – freqüentemente não bem informados com respeito às características do ambiente digital.

Sabe-se que os verdadeiros criminosos da Internet dominam técnicas avançadas de criptografia, navegam anonimamente – não tendo dados privados a defender – e, às vezes, a partir de máquinas localizadas fora de seus países. Do ponto de vista prático, esse projeto é pouco eficaz no combate aos grandes criminosos na rede. Ele afeta principalmente o cidadão médio, que tem alguns de seus consagrados direitos fundamentais severamente ameaçados.

O argumento da necessidade de monitorar a Internet no combate ao crime tem sido usado com eficácia para convencer legisladores - e mesmo a parcelas da sociedade - a engrossar a cruzada para acabar com a privacidade dos cidadãos e a intimidá-los no exercício de suas liberdades de expressão e de comunicação. A Internet, para onde convergem outras tecnologias de armazenamento e transmissão de dados, permite o controle e monitoramento sobre as pessoas nunca antes visto na história. Esta discussão tem sido feita sem profundidade e com pouco debate junto à sociedade. O mais grave é que essas "exceções" legais aos direitos fundamentais têm sido aproveitadas com perspicácia por grandes corporações para defender seus supostos direitos comerciais. Isso ocorre mesmo em países desenvolvidos, como a Alemanha, e pode vir a ocorrer aqui no Brasil - se a sociedade não reagir a tempo. ●

//REFERÊNCIAS:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:pt:HTML
Backbone é a "espinha dorsal" por onde passam toda a troca de dados num sistema mais amplo.
http://www.senado.gov.br/comunica/agencia/pags/01.html
http://conventions.coe.int/Treaty/EN/Treaties/PDF/185-POR.pdf

Cezar Taurion Chede Gerente de Novas Tecnologias Aplicadas da IBM Brasil, é economista, mestre em Ciência da Computação. Autor de quatro livros, entre eles "Software Livre: Potencialidades e Modelos de Negócio".

Padrões abertos, interoperabilidade

e interesse público

Os padrões abertos devem ser entendidos como absolutamente essenciais em um mundo cada vez mais globalizado e interligado. Os países, organizações, empresas e cidadãos interoperam continuamente uns com os outros. Para que a interoperabilidade aconteça, é necessário que todos estejam de acordo sobre a forma como esta interoperabilidade vai ocorrer. Ou seja, quanto mais padronizados forem os mecanismos de interoperabilidade, menos esforço será demandado para criarmos interfaces de interoperação – e a comunicação ocorrerá de forma mais rápida e ágil. Simples assim...Aliás, sem padrões abertos simplesmente não teríamos a Internet! A Internet está se tornando o meio padrão de comunicação do planeta. E isto só é possível porque existe um padrão aberto e reconhecido por todos para a troca de dados na Internet - sejam usuários dos EUA, Brasil, China ou Uganda -, que é o protocolo TCP/IP.

Neste ponto, o conceito de interoperabilidade deve ser bem definido. Existem claras diferenças entre interoperabilidade (capacidade de diferentes

softwares trocarem informações via um conjunto padrão de interfaces e formatos abertos) e intraoperabilidade (quando um fornecedor apenas cria condições para tornar mais fácil a conexão com seus próprios produtos). Em uma situação de intraoperabilidade, o fornecedor de um determinado produto cria protocolos e formatos que favorecem ao seu negócio – mantendo seus produtos sob seu domínio, controlando sua evolução e decidindo quais funcionalidades serão mais ou menos abertas. Na interoperabilidade, os padrões são abertos e não controlados por nenhuma empresa, não privilegiando um produto específico em detrimento de outro.

Padrões abertos, ou seja, aqueles que estão publicamente disponíveis e não são controlados por nenhum governo ou corporação, tornam possível que quaisquer empresas, cidadãos e países se conectem e troquem informações com autonomia. O uso de tecnologias de informação e comunicação de padrões abertos traz benefícios a todos, potencializando a interoperabilidade (leia-se colaboração) entre todos os envolvidos no processo de comunicação. Por outro lado, padrões proprietários criam barreiras econômicas quando exigem o pagamento de *royalties* (e muitas vezes um padrão proprietário embute diversas tecnologias patenteadas, com *royalties* acumulados), encarecem os produtos e dificultam a competitividade e a interação entre pessoas, empresas, governos.

A própria Declaração de Princípios da Cúpula Mundial sobre a Sociedade da Informação[1], no parágrafo 44 diz claramente : "A padronização é um dos pilares essenciais da Sociedade da Informação. Deve haver especial ênfase no desenvolvimento e adoção de padrões internacionais. O desenvolvimento e uso de padrões abertos, interoperáveis, não-discriminatórios e orientados a demandas, que levem em conta as necessidades dos usuários e dos consumidores, é um elemento básico para o desenvolvimento e ampla difusão das TICs e para uma maior viabilidade econômica no acesso a estas tecnologias, particularmente nos países em desenvolvimento. Padrões internacionais se destinam a criar um ambiente onde os consumidores possam acessar serviços em qualquer parte do mundo, a despeito de quais sejam as tecnologias subjacentes".

Para definir e manter padrões abertos existem diversas entidades - a ISO[2] é uma delas. Recentemente ocorreu um intenso debate sobre a aprovação ou não pela ISO de uma proposta de padrões de formato de documentos, denominado OpenXML. Este debate colocou em cheque o atual modelo de aprovação de padrões – mas antes de nos aprofundarmos neste ponto, cabe primeiro analisarmos a importância para a sociedade dos padrões de formato de documentos.

1. Ver em http://www.itu.int/wsis/docs/geneva/official/dop.html 2. International Organization for Standardization : http://www.iso.org/iso/home.htm

> O uso de tecnologias de informação e comunicação de padrões abertos traz benefícios a todos, potencializando a interoperabilidade (leia-se colaboração) entre todos os envolvidos no processo de comunicação

Para explicar melhor esta importância, é preciso voltar um pouco no tempo. No início da era da computação pessoal, o enfoque da informática era a produtividade individual, com intercâmbios de arquivos limitados a troca de disquetes. Neste contexto, não havia muita preocupação com a compatibilidade entre diversos formatos de arquivos, pois não havia maiores problemas de interoperabilidade. Com o mercado de suites de escritório sendo dominado por um único fornecedor, a situação não gerava maiores problemas, pois havia uma razoável compatibilidade entre versões. Razoável, porque formatos de versões mais novas nem sempre eram lidas pelas versões anteriores. Mas, renovava-se a licença de uso, instalavam-se as versões mais novas e a vida corria normalmente.

Entretanto, à medida em que a Internet e o correio eletrônico se disseminavam, as questões de interoperabilidade começavam a se tornar mais e mais importantes. Ao mesmo tempo começávamos a ver uma crescente digitalização de documentos.

Documentos fazem parte de quase todas as nossas atividades. A maior parte das informações e memória de governos, organizações – e hoje até mesmo de indivíduos - está contida em documentos. E a cada dia mais, criamos e armazenamos documentos em formato digital - na maioria das vezes, exclusivamente em formato digital. Estima-se que hoje, pelo menos 80% das informações das empresas não estejam em bases de dados estruturadas, mas espalhada por milhares e milhares de documentos e planilhas. E à medida em que os documentos passam a ser digitalizados, cresce de forma exponencial a sua geração – há estudos que prevêem que nos próximos cinco anos geraremos um número de documentos digitais equivalente à quantidade total de documentos gerados nos últimos 25 anos.

Apresentam-se então dois desafios: o primeiro é a deterioração gradual do meio físico, o que nos obriga a, de tempos em tempos, substituir o arquivo de mídia onde armazenamos dados, para garantir sua perenidade. O segundo desafio é mais complicado: no contexto atual, os arquivos de documentos são armazenados em formato binário, proprietário. Isto significa que se quisermos acessá-los daqui a vinte ou trinta anos, os softwares que os criaram deverão continuar existindo. Ou seja, além da perenidade do meio, temos que garantir a perenidade do software.

O armazenamento e posterior recuperação de documentos eletrônicos é, sem sombra de dúvida, uma questão de absoluta importância. Os documentos gerados hoje devem poder ser recuperados no futuro, independentemente do software que os criou. Garantir a possibilidade de recuperar estes documentos significa que se deve preservar suas formatações originais - como

quebra de páginas, alinhamentos de parágrafos, numeração, etc. Para isso é essencial que os formatos que descrevem como estes documentos estão armazenados eletrônicamente sejam resistentes a mudanças nas tecnologias de software e ambientes operacionais.

Diante deste quadro, com a mudança de paradigmas relativos ao padrão desejável dos arquivos de documentos - de fechado e "preso" a um determinado aplicativo, para aberto e independente do software que o gerou -, foi criado pela entidade OASIS[3] , um padrão denominado ODF[4] (Open Document Format), que em maio de 2006 foi reconhecido pela ISO como um padrão mundial.

A Microsoft, em contrapartida, também propôs um novo formato, chamado OpenXML, enviando-o a uma entidade chamada Ecma[5], que solicitou à ISO sua aprovação como padrão mundial. Quando o OpenXML foi apresentado à comunidade técnica, representada pelos órgãos de padrões dos países membros, foram identificados diversos elementos contraditórios. Mesmo assim, a ISO aceitou levar à frente a proposta de aprovação deste formato.

O processo de votação na ISO, que aconteceu no âmbito da ISO/IEC JTC1[6], mostrou inúmeras falhas, especialmente quando adotou-se um mecanismo chamado de "*fast track*", (mecanismo de tramitação rápida). Este processo, que levou à aprovação do OpenXML (apesar de vários países, inclusive o Brasil, o questionarem formalmente), gerou dúvidas muito grandes quanto à sua validade. Analisar e debater uma proposta de padrões de importância capital para a sociedade não pode ser algo feito de forma apressada e atabalhoada.

Além disso, a adoção de um segundo padrão para fazer a mesma coisa que o padrão já aprovado anteriormente (neste caso, o ODF) é altamente questionável. Vamos imaginar um cenário hipotético: alguns países adotam o ODF como seu padrão de formato de documentos e não aprovam o OpenXML, por não concordarem com seu processo de aprovação. Outros eventualmente adotam o OpenXML e em princípio não usariam o ODF. Cria-se então um problema de conversão de formatos, sempre que houver troca de documentos entre países que adotaram padrões diferentes. A interoperabilidade plena estaria prejudicada.

Ora, se avaliarmos o OpenXML vemos que pelo menos 90% a 95% de sua funcionalidade está incorporada no padrão ODF e os 5 a 10 % ausentes relacionam-se com características específicas de um único software, o Office da Microsoft. Imagino que se todo o esforço, tempo e dinheiro investido por dezenas de países para analisar o OpenXML fossem canalizados para refinar o ODF, inserindo novas funcionalidades e harmonizando-o com o OpenXML, todo o processo

3.Organization for the Advancement of Structured Information Standards - http://www.oasis-open.org/who/ 4.Para saber mais sobre o ODF, ver o sítio http://br.odfalliance.org/ 5.Sobre a Ecma International: http://www.ecma-international.org/ 6. Núcleo na ISO dedicado a desenvover e manter padrões na área de Tecnologia da Informação.

O que queremos - ou melhor, o que sociedade demanda? Processos mais eficientes, abertos e imparciais de padrões abertos de TICs

seria muito mais útil e produtivo para a sociedade.

Recentemente a IBM aprovou uma nova politica corporativa de padrões de Tecnologias de Informação, depois de uma ampla discussão com especialistas em padrões, do mundo inteiro. Estes especialistas recomendaram que os órgãos dedicados a analisar e estabelecer padrões revejam e modernizem seus processos de aprovação, principalmente visando a uma maior transparência em todas as etapas do processo. Este seria um passo concreto na direção da atualização destes processos, que inclusive deveriam considerar a nova geopolítica mundial, onde países emergentes como Brasil, India e China têm um papel mais importante na economia mundial - importância que ainda não está refletida nos processos atuais de aprovação de padrões.

A partir destes estudos podemos alinhavar algumas recomendações para modernizar e dar maior transparência aos processos de discussão e aprovação de padrões abertos de TICs:

a. Os órgãos de padronização devem garantir elevada transparência em seus processos. Os diferentes grupos envolvidos e seus interesses devem estar claramente explicitados.
Os usuários finais devem ter voz ativa nos processos de discussão e aprovação destes padrões. Os debates, as listas de discussão e as conclusões devem ser livremente acessíveis a todos os interessados e não restritos a grupos fechados.
b. Os governos devem garantir que seus NB (*National Bodies* ou órgãos de padronização) implementem regras que garantam esta transparência e impeçam influência indevida por parte de fornecedores. No recente caso do OpenXML muitos países foram representados por NBs sem estrutura adequada para avaliar adequadamente um padrão mundial. Os NBs deveriam ter que cumprir exigências técnicas e institucionais universais e uniformes (e passíveis de auditoria) para serem considerados aptos a votar. Isto eliminaria problemas tais como a filiação à ISO de novos NBs como membros ativos, apenas dois meses antes de uma votação – o que possibilita que estes novos membros opinem sem antes terem feito uma análise mais detalhada da especificação que está sendo votada.
c. Os governos, como indutores de políticas e padrões, devem adotar em seus editais de compras na área de Tecnologia da Informação a obrigatoriedade de uso, quando disponíveis, de padrões abertos.
d. Os padrões devem ter alta qualidade e para isso os seus processos de criação e aprovação devem ser abertos, imparciais, auditáveis e altamente eficientes e profissionais. Ou seja, não podemos repetir os problemas do recente processo de aprovação do OpenXML. Neste processo, mais de 6000 páginas de documentação tiveram que ser analisadas em cerca de cinco meses. Posteriormente, por conta de um mecanismo chamado de BRM (*Ballot Resolution Meeting* ou Encontro para Resolução de Votação), houve um debate que envolveu mais de 100 delegados de 32 países, dada a imensa

quantidade de disposições a serem analisadas (mais de 1100), e os poucos dias disponíveis (cinco). Consequentemente, não houve tempo hábil para se validar todos os comentários detalhadamente - seria uma tarefa realmente impossível. Assim, apenas cerca de 20 a 30 disposições foram exaustivamente debatidas e votadas. Ou seja, mais de 80% dos comentários não foram sequer avaliados. Como a proposta do BRM era de avaliar a especificação, debatendo os comentários e as sugestões de correção e melhorias apresentadas pela Ecma, é lógico afirmar que o resultado final não foi adequado. Nenhuma reunião onde não são avaliados 80% dos itens propostos para discussão poderia ser chamada de "um sucesso"...Imaginem um hipotético projeto de software onde 80% dos itens que deveriam ser analisados pelos usuários não o são....Que usuários aprovariam tal projeto? Portanto, o processo "acelerado" de *"fast-track"* tem se mostrado totalmente inadequado para avaliar uma proposta com este nível de complexidade.

Ficou claro para todos que o processo adotado pelo comitê JTC1 da ISO para aprovar o OpenXML não atendeu às demandas da sociedade. O resultado foi um questionamento intenso que está chamando a atenção para a necessidade urgente de reforma dos processos atuais da ISO. Ficou claro também que uma certificação ISO não garante que um padrão seja realmente aberto.

O que queremos - ou melhor, o que sociedade demanda? Processos mais eficientes, abertos e imparciais de padrões abertos de TICs. Acredito que, à luz de tantos questionamentos, teremos de agora em diante um novo contexto onde os órgãos internacionais de padrões e as entidades de padrões dos países elevarão sensivelmente seus níveis de qualidade e transparência. Aliás, sem uma reengenharia dos processos de aprovação de padrões, a ISO/JTC1 correrá o risco de passar por outras situações como esta, em que sua credibilidade está sendo questionada.

Quanto ao ODF, é indiscutível que todo este debate serviu para mostrar a importância de um formato aberto de documentos. Nunca o tema foi tão debatido e gerou tantos eventos, artigos e publicações em blogs e sítios Web pelo mundo inteiro.

Lá pelos idos de 2005, quando o ODF começou a aparecer de forma discreta na mídia especializada graças à decisão do governo do estado americano de Massachussets de adotá-lo, quem poderia imaginar que toda esta celeuma seria levantada?

Assim, o fato de o OpenXML ter sido aprovado pela ISO não vai afetar a crescente curva de adoção do ODF. Pelo contrário, os governos que ainda não incluíram os formatos abertos em suas políticas de documentos, talvez esperando a decisão da ISO, o farão agora. Até mesmo para manter a coerência com seus votos.

Muitos NBs que não analisaram a fundo a especificação do OpenXML (e tenho certeza que muitos NBs que votaram a favor não tinham a mínima condição para estudar, avaliar e opinar com profundidade as mais de 6.000 páginas da especificação) terão que definir normas e procedimentos que orientarão a política de seus países para as próximas décadas. E terão que garantir que a especificação a ser adotada terá:

1. Qualidade. O fato de mais de 80% das especificações do OpenXML não terem sido analisadas significa manter um universo de *"bugs"* em potencial por muitos e muitos anos. Isto não aconteceu e nem está acontecendo com o ODF.
2. Disponibilidade de softwares. Uma vez que a especificação aprovada não é a que está sendo implementada no Office atual, devido às milhares de modificações efetuadas durante o processo e que ainda não foram oficializadas, devemos esperar algum temp o antes que surjam softwares que consigam implementar o futuro OpenXML. Enquanto isso, o ODF já está implementado por diversos softwares, de diversas empresas.

O fato é que os países e seus governos terão que adotar políticas que visem a garantir a recuperação futura de seus documentos eletrônicos. E terão que fazer isso rápido, uma vez que enquanto não agem, são gerados milhões de novos documentos em formato binário, aumentando o legado de forma exponencial.

Como vimos ao longo do processo, dificilmente produtos que não o Office conseguirão ser 100% compatíveis com o OpenXML. Assim, os governos dos países terão que arcar com a responsabilidade de, ao manterem o OpenXML, estarem perpetuando o atual monopólio da empresa que o criou.

Provavelmente veremos muitos países decidindo-se por políticas de uso de documentos que incentivem a concorrência e inserindo nos textos oficiais não apenas a exigência de um formato que tenha sido aprovado pela ISO, mas que também seja realmente aberto, e que tenha sido implementado em pelo menos dois produtos de softwares. Os países também exigirão que não haja discriminação quanto aos modelos de comercialização dos softwares que usam os formatos de documentos, de modo que permitam diversas alternativas - como modelos de código aberto.

Sem isso, os cidadãos não terão seus "direitos civis na área de TICs" (liberdade de religião, liberdade de opinião e liberdade de usar qualquer aplicação...) reconhecidos, pois serão obrigados a adquirir um software específico para poderem dialogar com seus governos!

Ora, para mim fica claro que a aprovação do OpenXML pela ISO será mais um fator impulsionador para adoção do ODF pela sociedade, por conta de o ODF ser um padrão que já existe de fato (e não apenas no papel), por incentivar a livre concorrência, por garantir os direitos dos cidadãos e inibir a formação de monopólios. Além do mais, a própria sociedade civil que, em peso, debateu exaustivamente o OpenXML durante seu processo de aprovação, continuará mobilizada e atuando com força para que padrões abertos de documentos sejam e continuem realmente abertos. ●

//PERFIL:
Cezar Taurion escreve constantemente sobre tecnologia da informação em publicações especializadas e em seu blog: www.ibm.com/developerworks/blogs/page/ctaurion Este artigo representa a opinião pessoal do autor e não necessariamente a da empresa onde trabalha.

Joel Kelsey Analista político e oficial de relações internacionais da Consumers Union.

FCC X Comcast:

muda o jogo das políticas de comunicação nos EUA

Enquanto os Estados Unidos passaram todo o verão absortos na campanha política, uma votação interessante aconteceu na Comissão Federal de Comunicações (FCC) – a poderosa, ainda que pouco conhecida, agência federal que controla as políticas de comunicações nos E.U.A. Em agosto a agência desafiou toda a sabedoria política existente em Washington DC e assumiu um posicionamento histórico para os consumidores, punindo a Comcast, a maior empresa de comunicações por cabo do país, por impedir seus assinantes de acessar conteúdos na Internet totalmente legais.

A Comissão ordenou que a Comcast deixasse de interferir no tráfego Internet; que explicasse por que razão decidiu bloquear a utilização de determinados serviços on-line por seus assinantes; e a informar os consumidores e a FCC, com total transparência, sobre qualquer nova prática de "gestão de rede". Punindo a Comcast, a FCC deu um passo certo em direção à preservação da natureza aberta da Internet e à garantia de que provedores de serviços de Internet não podem atuar como "guardas", decidindo sobre qual informação deve e não deve ser enviada através das nossas redes de comunicação.

Há mais de um ano, na primavera de 2007, um engenheiro de rede

> Punindo a Comcast, a FCC deu um passo certo em direção à preservação da natureza aberta da Internet

chamado Robb Topolski percebeu que não podia partilhar suas canções antigas favoritas – conteúdo perfeitamente legal - com outras pessoas. Depois de fazer uma pequena investigação sobre o fato e publicar suas descobertas, Topolski percebeu que ele não era o único usuário que a Comcast estava impedindo de usar redes populares de P2P - serviços de compartilhamento de arquivos como o Bit Torrent, que representam uma ameaça emergente para empresas de comunicação a cabo como a Comcast por serem uma potencial alternativa para a distribuição de vídeos on-line.

A Electronic Frontier Foundation e a Associated Press (AP) logo começaram a fazer suas próprias investigações e descobram que a Comcast estava deliberadamente identificando e interferindo no uso de tecnologias P2P como o Bit Torrent e-Gnutella.

Assim que a AP divulgou a história nos meios de comunicação, os grupos de interesse público como a Consumers Union, num movimento liderado pela Free Press, apresentaram denúncias à FCC. A Comissão abriu um inquérito em janeiro de 2008, abrindo chamadas para comentários públicos e realizando audiências em todo o país. Em pouco tempo, foi como se tivessem sido abertas as comportas: dezenas de milhares de cidadãos apresentaram as suas próprias observações à FCC; muitos apelaram à FCC solicitando punição à Comcast por enganar os seus clientes.

A Comcast reagiu, primeiro negando ter bloqueado qualquer conteúdo na Internet; em seguida, admitindo a prática e tentando justificar as suas ações chamando-as de "gestão da rede" e, por último, tentando abertamente questionar a FCC quanto à sua autoridade para intervir em nome dos consumidores. Quando se tornou claro que a FCC não aceitaria os seus desmentidos e justificativas, a Comcast tentou atrasar a decisão da Comissão, ao anunciar uma série de negociações – suspeitamente concomitantes - com empresas como a Pando Networks, a BitTorrent e a Vonage, alegando que o mercado resolveria a situação por si. Naturalmente, a motivação por trás desta tentativa de auto-regulação não foi a "magia do mercado em ação", mas a "magia" da ameaça da intervenção governamental.

::FELIZMENTE, A FCC NÃO ENGOLIU ESSE JOGO.

A FCC votou sobre este caso em 1º de agosto, e considerou a Comcast responsável por violar a "neutralidade da rede", o princípio que impede que provedores de acesso à Internet por cabo, telefone ou outros meios discriminem determinados sítios e servi-

ços on-line devido ao seu conteúdo, origem ou destino.

A Comcast não convenceu a FCC com suas tentativas de mascarar a verdade. O mandado da Comissão afirmava que a "ginástica verbal" da Comcast e suas tentativas de tornar obscura a questão do bloqueio foram "não convincentes e fora de propósito".

A Comissão ficou particularmente indignada com as mentiras e dissimulações da Comcast: "a primeira reação da Comcast às alegações de tratamento discriminatório de tráfego não foi honesta, na melhor das hipóteses foram tentativas de desorientação e ofuscação dos fatos. O que mostra se uma ação é razoável ou não é o fato de um fornecedor estar disposto a divulgar aos seus clientes aquilo que está fazendo ." [1]

Esta decisão muda o jogo das políticas de comunicação nos Estados Unidos. A FCC tem deixado claro que a Internet é uma plataforma essencial para o desenvolvimento tecnológico e a liberdade de expressão. Ao bloquear a possibilidade de seus assinantes utilizarem serviços na Internet que poderiam competir com os seus próprios, e escondendo o fato dos clientes, a Comcast violou brutalmente os direitos dos consumidores.

A decisão da FCC reconhece que a arquitetura aberta em que a Internet tem operado deve ser protegida de "guardas de trânsito" que esperam obter lucros decidindo quem pode enviar que tipo de informação na rede.

Isto protege não apenas a liberdade de expressão, mas também a inovação e o crescimento econômico. Uma articulação clara das regras relativas à forma como os dados são geridos na Internet permite que desenvolvedores de software, engenheiros de rede e outros pensadores da inovação construam o próximo salto tecnológico. Esta é a teoria ponta-a-ponta[2] sobre a qual a Internet foi criada - como na rede elétrica, na qual você sabe o que está recebendo quando você pluga a tomada ou liga o interruptor. Quando os operadores de rede começam a interferir no fluxo do conteúdo que passa nas suas redes, como a Comcast fez, as regras do jogo são arbitrariamente mudadas e limita-se o ambiente para inovação.

No entanto, nem todos nós podemos fazer o mesmo que Topolski Robb, nem deve-se esperar que o façamos. Embora parar as arbitrariedades da Comcast tenha sido uma grande vitória, no futuro não deveríamos ter de contar com aficcionados por música, que por acaso também sejam engenheiros de rede, como a nossa principal frente de defesa. Isso é o que boas políticas de comunicação deveriam fazer: proteger a liberdade de expressão dos cidadãos. Um mercado restrito, onde há um duopólio de prestadores de serviços, não vai se auto-governar. É por isso que precisamos de neutralidade da rede nos termos da lei, em termos inequívocos. Temos que criar regras claras que impeçam a discriminação em todas as redes de comunicações no século XXI - com fios, sem fios, seja lá como forem. ●

Tradução de Graciela Selaimen

1. FCC. Memorandum Opinion and Order, Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications. WC Docket No. 07-52. August 20, 2008. 2. N.E.: este é um princípio que faz parte do desenho da arquitetura da Internet. Em teoria de redes, a abordagem ponta-a-ponta significa não centralizar o controle de certas camadas (especialmente conteúdo) e deixar que as decisões respectivas estejam nas mãos de quem está nas extremidades da rede.