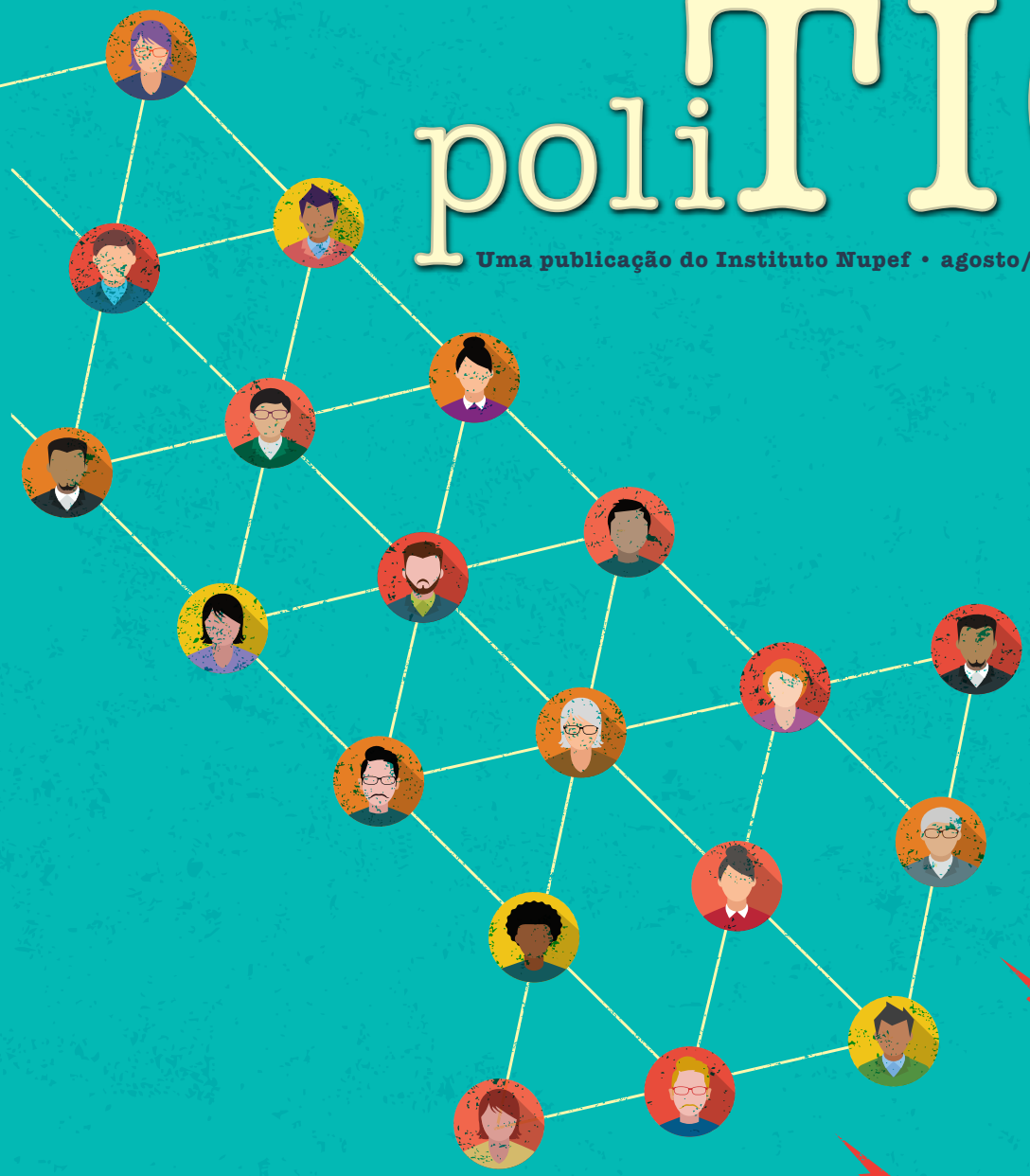
> A INTERNET.ORG E O FUTURO da web no Paquistão

> LET'S Encrypt!

> CARTA ABERTA A Mark Zuckerberg

poliTICs

Uma publicação do Instituto Nupef • agosto/ 2015 • www.politics.org.br



Zero-rating: bom negócio para quem?

Uma introdução ao debate

poliTICs

EDITOR CARLOS A. AFONSO • CAPA, PROJETO GRÁFICO E DIAGRAMAÇÃO MONTE DESIGN
COORDENAÇÃO TÉCNICA E VERSÃO ONLINE: PAULO DUARTE • TRADUÇÕES RICARDO SILVEIRA

instituto nupef

Rua Sorocaba, 219 | 501 - parte | Botafogo | 22271-110
Rio de Janeiro RJ Brasil | telefone +55 (21) 3259-0370

Apoio:

FORD FOUNDATION
Strengthen democratic values, reduce poverty and injustice, promote international cooperation and advance human achievement

Google

nic.br
Núcleo de Informação e Coordenação do Ponto BR

Esta é uma publicação do Instituto Nupef. Versão digitalizada disponível em www.politics.org.br
e no sítio do Nupef - www.nupef.org.br | Para enviar sugestões, críticas ou outros comentários: **politics@nupef.org.br**

A tiragem das edições da poliTICs é pequena. Se quiser receber gratuitamente a edição impressa, envie um email a **politics@nupef.org.br** com seu nome, endereço completo incluindo CEP, e área de atuação.

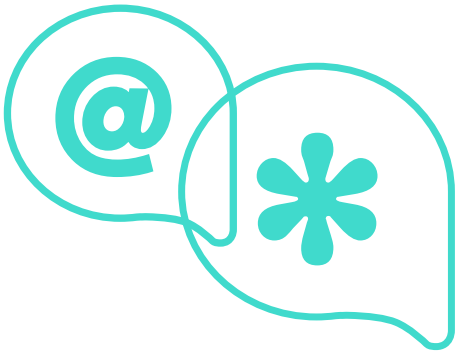
Os originais foram compostos com OpenOffice 3.X e GNU/Linux

ISSN: 1984-8803

A poliTICs procura aderir à terminologia e abreviaturas do Sistema Internacional de Unidades (SI), adotado pelo Instituto Nacional de Metrologia do Brasil (Inmetro). Assim, todos os textos são revisados para assegurar, na medida do possível e sem prejuizo ao conteúdo, aderência ao SI. Para mais informação: http://www.inmetro.gov.br/consumidor/unidLegaisMed.asp

poliTICs nº21

Índice



Editorial

Esta edição da poliTICs procura trazer pontos de vista e informações aprofundadas sobre as práticas de acesso patrocinado à Internet, do ponto de vista dos direitos do usuário e dos princípios de governança e uso da Internet, em especial os expressos pelo Marco Civil. Traz também uma descrição detalhada da iniciativa de certificação criptográfica gratuita Let's Encrypt, liderada pela Electronic Frontier Foundation (EFF) e que deve ser ativada ainda em 2015.

Pedro Henrique Soares Ramos descreve em detalhe o conceito e as modalidades típicas das estratégias comerciais de *zero-rating* nas ofertas de acesso móvel à Internet, sua relação com a visão de neutralidade da rede expressa no Marco Civil e os desdobramentos que podem afetar os direitos do consumidor.

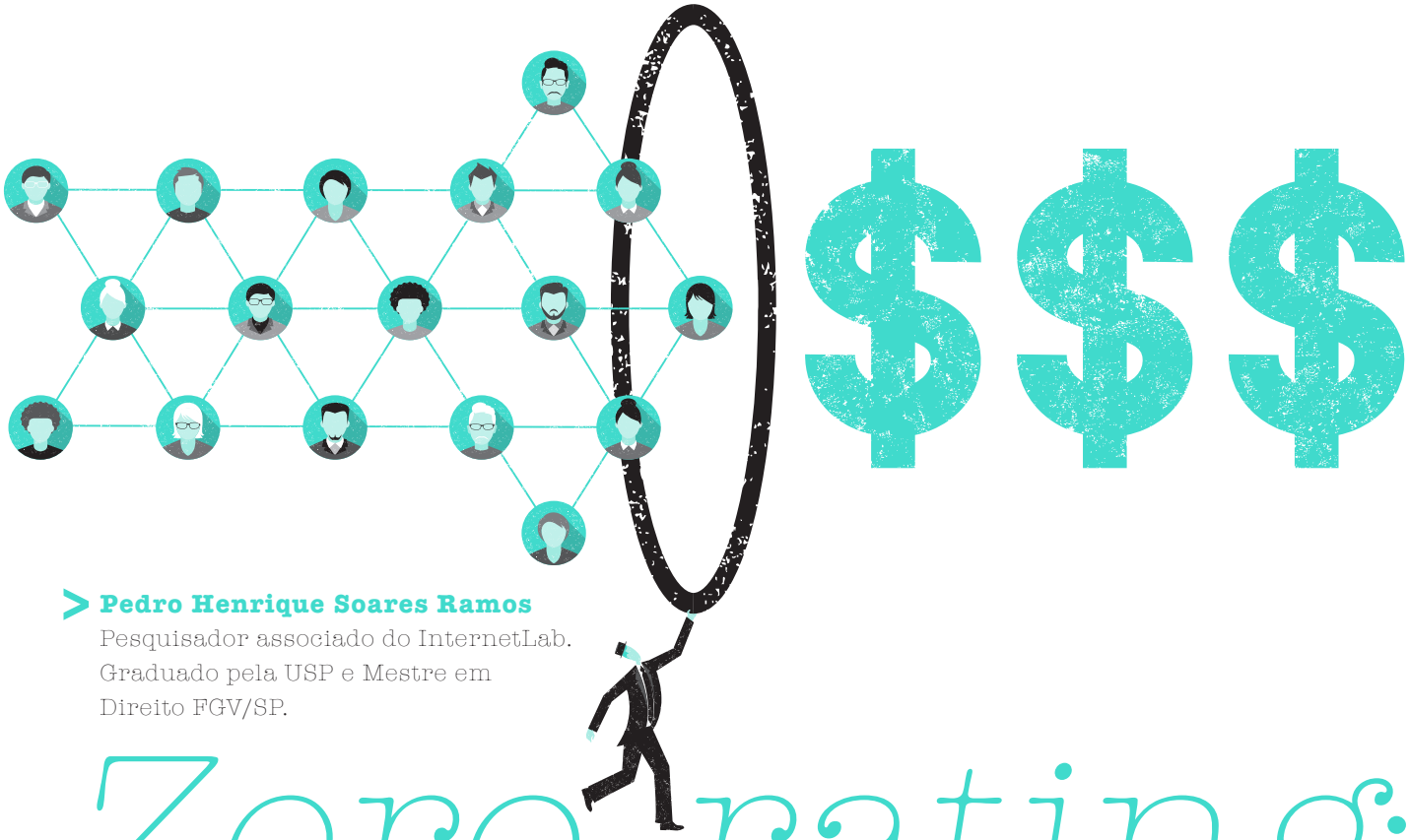
Flávia Lefèvre aprofunda a discussão sobre o acesso patrocinado à luz do Marco Civil e dos dez princípios de governança e uso da Internet definidos pelo CGI.br, bem como da Declaração Multissetorial de São Paulo do encontro NETmundial, analisando também os impactos econômicos dessa prática.

Arzak Khan, do Observatório de Políticas de Internet do Paquistão, descreve as limitações de acesso e liberdade de escolha impostas pela iniciativa Internet.org do Facebook em seu país, através de uma parceria entre o Facebook e uma das principais provedoras de acesso móvel no país, a Telenor. Nas palavras de Khan, "o esforço Zuckerberg-Telenor não só prejudica o crescimento, a liberdade e a expansão da Web no Paquistão como também arrisca criar uma Internet em dois patamares cerceando milhões de pessoas no mundo em desenvolvimento justamente no lado errado da exclusão digital".

Seth Schoen, tecnologista senior da EFF analisa as vulnerabilidades das tecnologias atuais de certificação criptográfica oferecidas pelo mercado, e descreve uma nova opção para a obtenção de certificados: a iniciativa Let's Encrypt. Liderada pela EFF e apoiada por várias entidades e empresas do ramo, a Let's Encrypt deve lançar ainda em 2015 um novo método quase automático de obtenção e renovação gratuitas de certificados SSL/TLS, com o objetivo de universalizar a criptografia nos serviços Web de modo simples, rápido e sem custos para o usuário.

Por fim, publicamos a carta aberta a Mark Zuckerberg, assinada por mais de 60 entidades de vários países, manifestando desacordo com a iniciativa Internet.org. Ao final da carta, as entidades concluem: "O Facebook, nas suas intenções declaradas de conectar bilhões à Internet, deveria apoiar e defender fortemente as salvaguardas dos princípios da neutralidade da rede, privacidade, segurança, e outros direitos dos usuários nas negociações com os governos e os reguladores nacionais, ao mesmo tempo que deveria aplicar estes padrões às suas iniciativas de negócios".

Boa leitura!



Pedro Henrique Soares Ramos
Pesquisador associado do InternetLab. Graduado pela USP e Mestre em Direito FGV/SP.

Zero-rating: uma introdução ao debate

:: INTRODUÇÃO

O objetivo deste artigo é apresentar um panorama geral de como os estudos acadêmicos têm abordado os efeitos econômicos e sociais de estratégias *zero-rating* no mercado *mobile*, e como essa discussão tem afetado o posicionamento dos principais *stakeholders* no Brasil. Este ensaio está dividido em três partes: na primeira, vamos rapidamente contextualizar o que é *zero-rating*, sua relação com a neutralidade da rede e algumas de suas espécies. Em seguida, elencaremos os principais modelos de análise que têm sido utilizados para o estudo sobre *zero-rating* na literatura acadêmica, especialmente nas áreas de Direito, Economia e Ciências Sociais. Finalmente, vamos organizar um mapa das discussões no Brasil, expondo a posição dos atores e seus principais argumentos em favor ou contra planos de *zero-rating* no país.

:: O QUE É *ZERO-RATING*

Zero-rating refere-se a uma série de estratégias comerciais desenvolvidas por operadoras em parceria com provedores de aplicações que visam oferecer gratuidade no tráfego de dados para

determinada aplicação e serviço específico - em outras palavras, trata-se de um modelo de negócio no qual a operadora, após o cliente esgotar sua franquia de dados, permite que ele continue usando um determinado serviço, sem custos.

Ao contrário do mercado de banda larga, é comum que operadoras ofereçam a seus usuários planos de acesso à internet com limites de volume de tráfego mensais – por exemplo, em um plano de 100 MB, o usuário somente poderá utilizar internet 3G em seu dispositivo móvel até o limite de 100 megabytes de tráfego download e upload por mês. Por meio de estratégias de *zero-rating*, operadoras permitem que o cliente, após esgotar sua franquia de dados, continue usando um determinado serviço sem custos, independente da contratação de uma nova franquia de dados.

Na visão atualmente majoritária da academia, estratégias de *zero-rating* têm entrado diretamente em conflito com a neutralidade da rede, princípio de arquitetura de rede que endereça a provedores de acesso o dever de tratar os pacotes de dados que trafegam em suas redes de forma isonômica, não os discriminando em razão de seu conteúdo ou origem. Planos de *zero-rating*, ao permitir que determinadas aplicações trafeguem de forma gratuita e que outras sejam bloqueadas ao término da franquia, feririam essa isonomia, fortalecendo, no caso dos provedores de acesso, seu papel de gatekeepers da rede, com a capacidade de escolher quais conteúdos serão ou não disponíveis para usuários de forma diferenciada.

Zero-rating refere-se, naturalmente, a um gênero de estratégias comerciais: em vários países e em estudos específicos, identifica-se diferentes espécies dessa modalidade, como por exemplo:

- **(i) tarifação zero para aplicações e serviços de emergência** – mesmo ao término da franquia de dados, o usuário deveria ter acesso a aplicações que possam auxiliar serviços públicos, como envio de mensagens para polícia e pronto-socorro, e mesmo serviços de localização do dispositivo do usuário;

- **(ii) acesso patrocinado** – nesses casos, o provedor de aplicação paga diretamente a operadora pelo tráfego gerado por seus usuários (tarifação reversa), por meio de uma tabela de preços pública e isonômica, em formato semelhante ao que ocorre no formato 0800 da telefonia tradicional;

- **(iii) tarifação zero por escolha da própria operadora** – são iniciativas de *zero-rating* em que a operadora, por meio de decisões estratégicas internas, seleciona uma aplicação específica para que o tráfego gerado pelo acesso a essas aplicações não seja cobrado do usuário; não há, nesse caso, uma oportunidade para *quaisquer serviços* serem elegíveis à tarifação zero, mas somente aqueles escolhidos pela operadora.

Há consenso acadêmico sobre os benefícios sociais relacionados com a modalidade (i) acima. No caso (ii), há uma posição majoritária de que essas estratégias não ferem a neutralidade da rede, em que se pesem argumentos sobre seus eventuais efeitos econômicos (van Schewick, 2015). Logo, a grande discussão atual gira em torno do cenário (iii), em que a posição de *gatekeeper* do provedor de acesso fica não só evidente como potencializada.

:: *ZERO-RATING* NA ACADEMIA

A discussão acadêmica sobre o assunto ainda é embrionária. Entre os trabalhos publicados, observa-se poucas iniciativas empíricas; a maior parte dos trabalhos e artigos procura realizar discussões à nível mais teórico, adotando perspectivas como os efeitos do *zero-rating* para os usuários e sua relação com o acesso à rede, os efeitos dessas iniciativas na competição e as consequências adversas dessas estratégias para o desenvolvimento tecnológico de países em desenvolvimento. Discutiremos um pouco desses trabalhos e perspectivas nas próximas páginas.

:: ESTUDOS EMPÍRICOS SOBRE OS EFEITOS DE ESTRATÉGIAS *ZERO-RATING*

Poucos estudos empíricos têm sido dedicados para entender quais as consequências de planos de *zero-rating* para o desenvolvimento do mercado *mobile*. Em Ramos (2014), conduzimos um estudo para identificar o que há de comum entre países em que planos de *zero-rating* estabeleceram-se primeiro e com mais sucesso, e quais as possíveis consequências dessas práticas.

Para responder a essas perguntas, analisamos países em que Facebook, Google, Twitter e Wikimedia Foundation desenvolvem ou desenvolveram, entre 2010 e o primeiro semestre de 2014, estratégias de *zero-rating* em parceria com operadoras locais. Os resultados do estudo apontaram que: (i) há uma posição dominante dos quatro grandes provedores de conteúdo analisados entre os *sites* mais acessados desses países, o que permite assumir que dar acesso gratuito a usuários desses países tenderá a satisfazer melhor as expectativas que esses usuários possuem sobre quais *sites* gostariam de acessar na internet; (ii) o número de planos de telefonia móvel ativos nos países analisados é bastante alto, mas a penetração da internet ainda é baixa (em geral, abaixo de 50%), e o preço de um plano de internet no celular é muito caro, custando uma média de 9,76% do PIB *per capita* (em países como no Congo, esse custo pode chegar a 126% do PIB *per capita*); (iii) há relevantes barreiras para o desenvolvimento de uma indústria tecnológica local; e (iv) dentre todos os países analisados, poucos começaram a promover

1. É difícil assumir que estratégias de *zero-rating* proliferaram por causa das características apontadas anteriormente, ainda que pareça claro que essas particularidades contribuíram para a expansão dessas estratégias. Em países com as características citadas, estratégias *zero-rating* podem servir como importantes portas de entrada de usuários mais pobres para a internet, funcionando como iniciativas de *marketing* eficientes para operadoras *mobile* (ainda que esses discursos sejam comuns no campo teórico e também em discursos dos principais *players* do mercado, não foram localizados estudos empíricos suficientes para fundamentar essas afirmações; em países desenvolvidos, há evidências recentes de que programas como o *Sponsored Data* da AT&T não estão tendo sucesso comercial, como aponta Becker, 2014).

discussões regulatórias mais sofisticadas sobre o papel da tecnologia no desenvolvimento local e a importância de regras de neutralidade da rede[1].

Em novembro de 2014, o relatório da Digital Fuel Monitor (2014) sobre a competitividade no setor *mobile* comparou diversos países pertencentes à União Europeia e à OCDE para investigar o impacto do *zero-rating* nesses países. O relatório traz três resultados importantes: (i) dentre os 41 países analisados, estratégias de *zero-rating* foram implementadas a partir do segundo semestre de 2014 em 32 desses países, beneficiando ao menos 75 aplicações *mobile* diferentes; (ii) entre essas operadoras, o custo de planos de acesso 3G e 4G aumentaram de forma expressiva ao longo de 2014, especialmente entre operadoras que oferecem serviços *zero-rated* de vídeo, por meio de parceiros ou empresas de seu mesmo grupo econômico (em um dos casos, uma operadora *zero-rated* triplicou o preço de seus planos de acesso 4G), e (iii) entre os países que não adotaram o modelo, tem sido observada uma tendência das operadoras locais em aumentar o limite da franquia de seus usuários, sem alteração dos preços – a operadora KPN da Holanda, por exemplo, dobrou o limite de franquia de seus planos, o que gerou uma redução, pela metade, do preço médio por gigabyte na banda larga *mobile*.

O estudo da Digital Fuel Monitor conclui que a oferta de *zero-rating*, aliada ao aumento dos preços da banda larga móvel, possui consequências adversas para a competitividade e para o acesso à rede, reduzindo a capacidade de escolha dos usuários (que, caso não queiram usar determinado serviço *zero-rated*, enfrentarão custos altos de banda larga) e a competitividade em relação a outras aplicações (enfrentarão altas barreiras de acesso para competir com aplicações *zero-rated*). Ainda, o relatório afirma que o estudo sugere que, caso o *zero-rating* seja proibido, pode haver incentivos econômicos para que operadoras reduzam o custo de seus planos de banda larga *mobile*, com o objetivo de incentivar o uso geral da internet por seus usuários, beneficiando inclusive serviços oferecidos pela própria operadora.

:: *ZERO-RATING* E A PERSPECTIVA DO USUÁRIO

Mas, afinal, planos de *zero-rating* são benéficos para os usuários? Ou os usuários são prejudicados com a proliferação desse tipo de iniciativa? Essas são questões difíceis de responder, na medida em que contrapõem dois diferentes referenciais analíticos. O primeiro referencial parte da premissa de que "qualquer acesso gratuito é benéfico, ainda que seja limitado a uma ou poucas aplicações"[2]. Por essa perspectiva, usuários de planos *zero-rating* estão sendo beneficiados com a possibilidade de acessar o seu conteúdo favorito gratuitamente, o que significa que a internet é, para esses usuários, mais valiosa e útil. Especialmente no caso de redes sociais e *sites*

2. Esse é, direta e indiretamente, o referencial adotado pelos *white-papers* produzidos pela Internet.org, disponíveis em http://goo.gl/VaicFM e http://goo.gl/yUu8NL. Acesso em 15 fev. 2015.

de conteúdo educativo, dar a usuários a capacidade de acessarem esses conteúdos gratuitamente pode expandir suas capacidades, promover a participação social e política e dar acesso a mais informação.

Por sua vez, o segundo referencial parte da premissa de que "o acesso a somente um ou poucos conteúdos selecionados pode reduzir as capacidades dos usuários". Essa é a perspectiva adotada por Susan Crawford (in Talbot, 2014), quando esta afirma que "*for poorer people, Internet access will equal Facebook. That's not the Internet — that's being fodder for someone else's ad-targeting business [...] that's entrenching and amplifying existing inequalities and contributing to poverty of imagination — a crucial limitation on human life*". Essa abordagem considera que o *zero-rating* traz pelo menos três consequências negativas para os usuários. A primeira é a possibilidade de que governos utilizem o *zero-rating* para aumentar o filtro de informações na rede e influenciar o consumo de conteúdo dos usuários, especialmente em países em desenvolvimento sujeitos a regimes autoritários.

A segunda consequência seria a criação de barreiras de exclusão social e a potencial divisão entre a "internet dos ricos" e a "internet dos pobres": esta última seria a periferia do sistema, com acesso limitado a recursos e que, a longo prazo, tenderia a aumentar barreiras de exclusão social, na medida em que os mais pobres seriam cada vez mais diferentes dos ricos no que se refere a acesso a informação, ferramentas de comunicação e interação social (Ramos, 2014). Com a cobrança diferenciada, poderia ser reproduzida a mesma separação social que ocorre nas cidades brasileiras hoje: periferias com acesso limitado a equipamentos culturais e serviços de qualidade, e anéis de riqueza em que seriam construídas barreiras de estratificação social com o objetivo de afastar a presença e entrada da periferia nessas praças.

Finalmente, a proliferação de modelos de *zero-rating* pode criar efeitos de *walled- gardens*, em que os usuários reduzem o interesse em sair das aplicações gratuitas e explorar os demais conteúdos da rede, reduzindo a possibilidade de que esses usuários venham, no futuro, a aprofundar-se em determinados temas e construir seus próprios conteúdos (Surman et al., 2014).

:: *ZERO-RATING* E DESENVOLVIMENTO: UMA ANÁLISE CONCORRENCIAL

O tema do *zero-rating* também está intimamente ligado aos estudos que analisam a competição no setor de tecnologia. Esses trabalhos apontam que estratégias de *zero-rating* podem potencialmente levar a uma maior concentração de mercado e à persistência de situações de monopólio que podem gerar consequências adversas à indústria local de conteúdo e aplicações, aumentando as barreiras para inovadores que desejam competir com players já estabelecidos e cujo mercado encontra-se resguardado por estratégias de *zero-rating*.

Ao permitir que provedores de acesso tenham a capacidade de *escolher* qual conteúdo ou aplicação ficará sujeita à gratuidade de tráfego – logo, podendo escolher os *vencedores* e *perdedores* de determinado setor do mercado –, a dinâmica da inovação altera-se profundamente (Berners-Lee, 2015; Van Schewick, 2014). Essa tem sido a principal lente teórica adotada no debate acadêmico, inclusive em carta enviada no início de 2015 à FCC por diversos pesquisadores estadunidenses[3]. Nesse cenário, as aplicações de maior sucesso não serão necessariamente aquelas que possuem a melhor tecnologia e desenvolvem o melhor produto, mas sim as aplicações que conseguirem a melhor condição de acesso junto a provedores de acesso[4]. Destarte, se determinada *startup* resolve competir em um setor em que já existe um concorrente que possui um acordo de *zero-rating* com um provedor de acesso, essa *startup* deverá enfrentar a barreira de que, pela perspectiva do usuário, a aplicação oferecida por esta é *paga*, enquanto a do concorrente é *gratuita*.

:: *ZERO-RATING* E CICLOS DE DEPENDÊNCIA TECNOLÓGICA

Outra lente de análise para o tema parte da perspectiva da dependência tecnológica entre países desenvolvidos e países em desenvolvimento[5]. Na medida em que grandes provedores de conteúdo precisam aumentar suas bases de dados para a oferta de serviços de publicidade, é racional que essas empresas busquem uma atuação mais forte em grandes mercados consumidores localizados em países em desenvolvimento. Todavia, quando essas empresas iniciam suas operações nesses países, estas se veem em condições econômicas adversas para o desenvolvimento de operações locais, tendo em vista que a penetração da internet é baixa, os custos de acesso são ainda altos e celulares ainda são a principal porta de entrada para a internet. Uma das formas que provedores de aplicação encontram para desenvolver suas operações locais e, ao mesmo tempo, o desenvolvimento do ecossistema local, são parcerias como *zero-rating*, oferecendo assim planos de acesso patrocinado a usuários de operadoras locais.

3. A carta, assinada por 36 pesquisadores, incluindo Jack Balkin, Yochai Benkler, Nicholas Economides, Brett Frischmann, Lawrence Lessig, Barbara van Schewick e Tim Wu, afirma que "*rules banning paid prioritization would prohibit providers of broadband Internet access from charging edge providers for prioritized or otherwise enhanced access to their Internet access customers. By "paid prioritization" we mean payments from edge providers for priority, guaranteed bandwidth, or zero-rating (not counting an edge provider's traffic towards a user's monthly bandwidth cap), as well as any other technical or economic practice that gives edge providers that pay an Internet access provider an advantage over edge providers that do not pay*". Disponível em http://goo.gl/zQDAU6. Acesso em 15 fev. 2015. 4. Esse cenário reduziria bastante a incerteza do mercado de tecnologia. Como coloca Van Schewick, (2010), investimentos de *venture capital* só são viáveis em mercados em que há enorme incerteza sobre quais *players* poderão ou não prosperar, e regulações ou falhas de mercado que reduzem essa incerteza tendem a diminuir o desenvolvimento desses setores. 5. A perspectiva teórica aqui adotada (e melhor detalhada em Ramos, 2014) remete diretamente à escola da "teoria da dependência", popularizada na América Latina nos anos 1950 e 1960 (nesse sentido, ver Prebisch, 1950; e Cardoso, 1973). Conforme colocado por teóricos desse movimento, a principal consequência adversa de ciclos de dependência é a redução da capacidade de países em desenvolvimento (periferia) de gerar seu próprio progresso tecnológico, tendo em vista sua dependência tecnológica em relação a países desenvolvidos (centro) – como colocado por Vernego (2006), "*technology – the Promethean force unleashed by the Indus- trial Revolution – is at the center of stage. The Center countries controlled technology and the systems for generating technology. Foreign capital could not solve the problem, since it only led to limited transmission of technology, but not the process of innovation itself*". Ainda que a profilaxia sugerida por autores dessa escola – e.g., substituição de importações e empresas estatais – tenha se provado como incapaz de superar barreiras de desenvolvimento, o diagnóstico de dependência permanece atual, com diversos trabalhos retomando essa problemática (Ghosh, 2001; Conway e Heynen, 2008).

Como uma consequência macro dessa estratégia, há potenciais desincentivos para a inovação e conteúdo local, bem como menores incentivos para o investimento de *venture capital* nesse setor, o que pode levar à maior dependência dos usuários locais por conteúdo e aplicações externas. Em última instância, a persistência de microciclos de dependência tecnológica, que podem ocorrer em virtude de iniciativas de *zero-rating*, pode levar a ciclos em que países em desenvolvimento, incapazes de desenvolver sua própria indústria de inovação, serão utilizados como combustível para o financiamento da inovação em países desenvolvidos, levando a baixas taxas de transferência tecnológica entre os países.

:: *ZERO-RATING* NO BRASIL

No Brasil, estratégias de *zero-rating* não são recentes. As primeiras estratégias desse tipo remetem à pré-história da internet móvel no País, com os chamados *portais WAP*, que permitiam a oferta de conteúdo multimídia em aparelhos de celular pré-smartphones, com baixíssimo uso de dados da rede (HCI Blog, 2004). Na era 3G, operadoras como a Claro mantiveram parcerias *zero-rating* com a Facebook e Twitter até o primeiro semestre de 2015[6], em parceria que atualmente é oferecida pela Oi em alguns de seus planos. A TIM já desenvolveu parcerias nesse sentido com aplicações de GPS como Moovit e Waze, e atualmente possui parceria com o aplicativo WhatsApp (de titularidade da Facebook).

:: O MAPA DAS DISCUSSÕES NO BRASIL

Com a aprovação do Marco Civil, o *zero-rating* tornou-se uma das primeiras (senão a primeira) grandes discussões hermenêuticas sobre o Marco Civil. Setores ligados a operadoras defenderam em comunicados e artigos de imprensa que essas iniciativas não estão compreendidas na regra do art. 9º, encontrando respaldo na liberdade de modelos de negócio estabelecida pela lei (De Luca, 2014).
Por outro lado, outros comentários têm apontado para a clara inadequação entre esses planos e a redação aprovada, não encontrando espaço para o entendimento de que o *zero-rating* estaria permitido. O debate foi amplificado recentemente, com o anúncio sobre a parceria entre o governo federal e a Facebook a respeito do projeto Internet.org que, entre algumas de suas iniciativas, também desenvolve, em parceria com operadoras locais, iniciativas de *zero-rating* em países em desenvolvimento.

6. Com a extinção dos planos de Facebook e Twitter grátis em abril de 2015, a Claro aumentou franquia de dados dos planos 3G e 4G de seus usuários, levando a uma redução de até 60% no custo por megabyte trafegado, como ocorreu com a operadora KPN na Holanda. Como coloquei em artigo para o Brasil Post à época (Ramos, 2015), a lição que parece ficar empiricamente apresentada aqui (e que já era apontado por estudos como o da Digital Fuel Monitor) é que o *zero-rating* pode favorecer a manutenção de preços altos no custo por *megabyte* ao usuário, e a sua não-existência em determinado mercado tende a reduzir barreiras de acesso tanto para usuários quanto para provedores de aplicações. Ainda, se esses planos não tem sido estratégias de *marketing* eficientes para as operadoras, essa mudança parece sinalizar que, se os usuários tiverem a escolha um plano de *zero-rating* para sua aplicação favorita e ter mais franquia de dados para todas as aplicações, os usuários podem estar preferindo a última opção.

O mapeamento organizado pelo InternetLab[7] traz alguns resultados que ajudam a entender melhor o posicionamento do mercado de internet a respeito do *zero-rating*. Por meio da análise das contribuições realizadas à plataforma de consulta pública do Ministério da Justiça, é possível identificar ao menos duas posições majoritárias sobre o assunto.

A primeira posição foi defendida por empresas e representantes do setor de telecomunicações como a FEBRATEL, SINDITEBRASIL, SINDISAT, TELCOMP, TELEBRASIL, ABRAFIX, ACEL, ABINEE, Claro, Tim e Cisco. Para esse grupo, que a obrigação de não discriminação de dados prevista no artigo 9º do Marco Civil abrange tão somente as atividades relacionadas com o tráfego de pacotes de dados, e não alcançam discriminações entre pacotes de dados que possam ocorrer em nível comercial. Defensores desse posicionamento argumentam que planos de zero rating proporcionam um aumento do acesso à internet, principalmente entre as classes sociais menos favorecidas, e que não necessariamente levam a efeitos negativos para a concorrência. Posicionamento semelhante também foi defendido pela Brasscom, associação que possui entre seus membros grandes provedores de aplicações como Google, Facebook, Microsoft, IBM, SAP, TOTVS e Locaweb.

A segunda posição interpreta o artigo 9º do Marco Civil de forma diversa: para estes, o Marco Civil prescreve a provedores de acesso o dever de tratar pacotes de dados de forma isonômica em qualquer modalidade, seja este no nível lógico, de infraestrutura ou de ofertas comerciais.
Para essa posição, a existência de planos de *zero-rating* possui efeitos concorrenciais adversos, e também gera efeitos nocivos para usuários, na medida em que contribuem para replicar uma divisão entre o pleno acesso a internet para quem pode pagar e o acesso limitado a algumas aplicações para as populações mais carentes.

Ao contrário da primeira posição, em que seus defensores estão claramente mais concentrados no setor de telecomunicações e entre os grandes provedores de aplicações, os defensores dessa segunda posição estão mais difusamente distribuídos entre diversos setores, como o governo (por meio de pareceres das consultorias do Senado, Câmara e da SEAE/MF), academia (CTS/FGV), associações representativas de pequenos provedores de aplicações (ABStartups) e representantes da sociedade civil (e.g., AccessNow, Artigo 19, IDEC, Instituto Telecom, Intervozes, PROTESTE).

:: CONCLUSÕES E APONTAMENTOS PARA FUTUROS ESTUDOS

Como vimos acima, a discussão acadêmica é embrionária; embora haja uma tendência em apresentar evidências sobre os efeitos adversos de

7. Disponível em http://www.internetlab.org.br

iniciativas de *zero-rating*, há ainda base empírica pouco sólida para confirmar ou não algumas das hipóteses levantadas, especialmente àquelas relacionadas à perspectiva do usuário, cujas pesquisas encontram dificuldade no levantamento de dados confiáveis que possam fundamentá-las.

Ao mesmo tempo, o debate público é enviesado: nos debates regulatórios, há uma clara tendência de polarização de acordo com os interesses institucionais de cada setor. Todavia, *zero-rating* não é uma discussão binária, nem uma luta entre usuários e corporações, ou entre *startups* e telecoms. Os custos e benefícios envolvidos não são exclusivamente alocados em um único *stakeholder*, e é papel de aplicadores do Direito entender a característica multifacetada dessa discussão, de forma a interpretá-la para preservar benefícios e reduzir custos dos atores envolvidos. Tensões entre livre-iniciativa e justiça distributiva, o papel de corporações na criação ou na redução de desigualdades, a promoção de um modelo de desenvolvimento com papel atuante do Estado e a participação de grupos políticos e representativos de empresas no jogo político possuem influência importante no debate, e não devem ser desconsiderados por instrumentalistas do Direito no momento de desenvolver regulações específicas ou de aplicar no Judiciário decisões a favor ou contra determinada prática de mercado. ●

Referências bibliográficas

- BECKER, S. *Here's Why No One Is Buying into AT&T's Sponsored Data Plan*. Wall St. Cheat Sheet, 2014. Disponível em http://goo.gl/bAhrH7. Acesso em 31 ago. 2014

- CARDOSO, F. H. *Associated-dependent development: theoretical and practical implications. in Authoritarian Brazil: origins, policies and future*. New Haven: Yale University Press, 1973.

- CONWAY, D.; HEYNEN, N. *Dependency theories: from ECLA to André Gunder Frank and beyond*. The Companion to Development Studies. London: Hooder, 2008.

- DE LUCA, C. *Marco Civil provocará muitas batalhas jurídicas. Quer saber quais?*. IDG Now!, 2014. Disponível em http://goo.gl/cyLm8H. Acesso em 16 jan. 2015.

- DIGITAL FUEL MONITOR. *EU28 & OECD mobile internet access competitiveness report Q4 2014*. Helsinki, 2014. Disponível em http://goo.gl/xhWTpy. Acesso em 16 jan. 2015.

- GHOSH, B. N. *Dependency Theory Revisited*. Aldershot: Ashgate Pub Ltd, 2001.

- HCI BLOG. *Introduction to WAP*. HCI Blog, 2004. Disponível em http://goo.gl/jYZjc2. Acesso em 13 dez. 2013.

- PREBISCH, R. *Economic Development in Latin American and its principal problems*. Lake Success: UN Department of Economic Affairs, 1950.

- RAMOS, P. H. S. *Towards a developmental framework for net neutrality: the rise of sponsored data plans in developing countries. Telecommunications Policy Research Conference*, 2014.

- ____. *Dilma, Zuckerberg e o fim do Facebook grátis na Claro*. Brasil Post, 2015.

- SCHEWICK, B. V. *Internet Architecture and Innovation*. Cambridge: MIT Press, 2010.

- ____. *Network Neutrality and Zero-rating*. FCC, 2015. Disponível em http://goo.gl/rnOVfy. Acesso em 23 jun 2015.

- SURMAN, M.; GARDNER, C.; ASCHER, D. *Local content, smartphones and digital inclusion*. Innovations, v. Special Edition, 2014.

- TALBOT, D. *In Developing Countries, Google and Facebook Already Defy Net Neutrality*. MIT Techonology Review, 2014. Disponível em http://goo.gl/35r9hw. Acesso em 23 jan. 2014.

- VERNEGO, M. *Technology, Finace, and Dependency: Latin American Radical Political Economy in Retrospect*. Review of Radical Political Economics, v. 38, n. 4, 2006.

Flávia Lefèvre Representante da sociedade civil no CGI.br e colaboradora da PROTESTE Associação de Consumidores.

Zero-rating, planos de serviço limitados e o direito de acesso à Internet

Durante disputado processo para a aprovação do Marco Civil da Internet (MCI) no Congresso Nacional em 2012 e 2013, um dos principais e mais polêmicos temas foi a garantia da neutralidade da rede e seus possíveis impactos para as empresas provedoras de serviço de conexão à Internet, para seus planos de negócios e para os consumidores. A discussão continua, pois estamos na fase de debates para edição do Decreto Presidencial que regulamentará alguns dispositivos da Lei 12.965/2014, estando entre eles as exceções à garantia da neutralidade, previstas no art. 9º, que trata das obrigações de tratamento não discriminatório dos pacotes de dados lançados na rede.

Muito da discussão se deu e ainda se dá quanto ao alcance que se atribuirá a esta garantia, de acordo com a qual o responsável pela transmissão, comutação e roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação. Dispõe também o MCI que na provisão de conexão à Internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear os pacotes de dados.

Diante desses comandos surgem posições divergentes com relação à prática comercial adotada por muitas empresas fornecedoras do serviço de conexão à Internet denominada de

zero-rating ou acesso patrocinado. Esta prática é muito utilizada pelas operadoras móveis nos planos que estabelecem franquias com volumes limitados de dados a serem utilizados mensalmente pelo consumidor. Nestes casos o provedor de conexão deixa de descontar o volume de dados correspondentes à aplicações ou conteúdos específicos. A princípio, esta prática não violaria a neutralidade, desde que o consumidor mantivesse a possibilidade de acessar também outras aplicações e conteúdos disponíveis na Internet, mesmo depois de esgotada a franquia, ainda que com a velocidade do provimento reduzida; assim não se poderia falar em discriminação vedada pelo MCI.

:: PLANOS DE SERVIÇO LIMITADOS E *ZERO-RATING*

Ocorre que a prática do *zero-rating* no Brasil está associada a planos franqueados, com limites baixos de volumes de dados por mês – de 200 MB a 600 MB – e, ao fim da franquia, o provedor de conexão mantém o acesso apenas a determinados aplicativos, com o bloqueio de todo o imenso universo disponível na Internet. Porém, se o *zero-rating* não viola a neutralidade enquanto a franquia está válida, a partir do momento em que a franquia se esgota e o provedor disponibiliza o acesso apenas a determinados aplicativos ou conteúdos e bloqueia todo o resto do que está disponível na Internet a obrigação de tratamento não discriminatório e a proibição de bloqueio estão sendo desrespeitadas.

E este entendimento foi também o das operadoras, que, durante o período de tramitação do projeto de lei que resultou no MCI, publicaram uma espécie de cartilha para ser distribuída aos parlamentares, onde apontavam como um dos principais problemas da lei o teor do art. 9º do então projeto, mas, ao mesmo tempo e contraditoriamente, se diziam a favor da neutralidade. Afirmaram o seguinte: "O artigo 9º do projeto do Marco Civil da Internet define, em seu caput, que os provedores de acesso têm o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por serviço. Como consequência dessa determinação, a oferta de serviços diferenciados pela velocidade é a única modalidade que pode ser comercializada. Neste tipo de oferta todos os pacotes recebem da rede o mesmo tratamento e apenas a velocidade com que eles são entregues ao usuário pode variar, em função da velocidade contratada. Todos os demais tipos de oferta, alguns deles atualmente comercializados, incluindo, a oferta baseada em volume de dados consumido pelo usuário, estariam vedados pelo Marco Civil".

Editado o Marco Civil da Internet em abril de 2014, que passou a vigorar a partir de junho do mesmo ano, apesar das assertivas transcritas acima, as empresas continuaram a comercializar planos franqueados, com volumes de dados mensais pífios, mas ao final da franquia, reduziam a velocidade

do provimento e mantinham o acesso à Internet. Porém, a partir de janeiro deste ano, alegando que este modelo de negócios praticado até então não se mostrava mais lucrativo, mudaram a prática; passaram a adotar o *zero-rating* para dar acesso aos aplicativos e conteúdos fornecidos por empresas com as quais estabelecem algum tipo de parceria, como é o caso do Facebook, Whatsapp e Twitter, bloqueando qualquer outro conteúdo ou aplicação.

:: OS PRINCÍPIOS, FUNDAMENTOS E OBJETIVOS DO MARCO CIVIL DA INTERNET

Para analisar a legalidade ou não desta prática comercial, antes de tratar propriamente da neutralidade pelo aspecto técnico e de seus efeitos no campo social e econômico, temos de considerar que o MCI desenhou um novo cenário para o serviço de acesso à Internet. Deixou expresso que o acesso à Internet é essencial para o exercício da cidadania e, por isso, introduziu uma série de garantias e definiu para o Estado diretrizes para a promoção da racionalização da gestão e expansão do uso da Internet no Brasil, tendo como fundamentos o reconhecimento da escala mundial da rede, os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais, a pluralidade e a diversidade, a defesa do consumidor e a finalidade social da rede, entre outros.

Os princípios trazidos pelo MCI foram a garantia da liberdade de expressão, comunicação e manifestação do pensamento, a preservação e garantia da neutralidade de rede, assim como sua estabilidade, segurança e funcionalidade, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas. O MCI estabeleceu ainda que a disciplina do uso da Internet no Brasil tem por objetivo a promoção do direito de acesso à Internet a todos, de modo a se promover o acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos.

Ou seja, ao determinar que o acesso à Internet é direito de todos, introduziu a garantia de que o serviço é de interesse público e essencial e de caráter universal, o que significa que deve estar disponível tanto para os mais ricos quanto para os mais miseráveis dos cidadãos, de forma contínua e com condições mínimas de qualidade.

Vale ressaltar que o MCI teve como fonte a Resolução 2009/003 do Comitê Gestor da Internet no Brasil (CGI.br), por meio da qual se estabeleceram os Princípios para a Governança e uso da Internet no Brasil, estando entre eles o seguinte: "O acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos". A fixação de tais princípios decorreu de consenso construído entre os vários setores representados no CGI.br: governamental, comunidade científica e tecnológica, sociedade

civil e setor empresarial e, por isso, as empresas não podem ignorá-los.

Temos também de ter em vista um dos objetivos trazidos com o MCI e relevante para a discussão a respeito do *zero-rating*, qual seja, a adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados. Portanto, ao tratar de acesso à Internet temos de reconhece-lo como serviço de interesse público e essencial, sendo mandatório admitir que o estado está obrigado a assegurar a sua prestação, devendo regular as contratações que se dão em larga escala e que não podem se desenvolver exclusivamente com base nas regras do mercado.

:: A NEUTRALIDADE

Nesse cenário, um dos principais instrumentos para se atingir o acesso universal à Internet, além da infraestrutura, é a garantia da neutralidade da rede, na medida em que os benefícios decorrentes do acesso à Internet resultam principalmente pela ampliação do acesso aos conteúdos de toda natureza, educacional, cultural, entre outros.

A neutralidade é uma ferramenta jurídica para garantir tratamento isonômico e não discriminatório na Internet, a fim de preservar o caráter aberto da arquitetura de redes e valores como a democracia, liberdade de expressão, fluxo livre de informação, privacidade, ambiente concorrencial, inovação, direitos do consumidor entre outros direitos fundamentais.

Os aspectos técnicos para a verificação do cumprimento das obrigações de não discriminação na rede vão depender da abrangência do conceito de neutralidade que se configurar nos ambientes de debate – órgãos reguladores e Poder Judiciário. De qualquer forma, o certo é que existem muitas definições a respeito da neutralidade, amoldadas cada uma delas aos objetivos perseguidos por cada país. E, no caso do Brasil, a definição a respeito da neutralidade terá de ser construída de acordo com os fundamentos, princípios e objetivos estabelecidos pelo MCI, como vimos anteriormente.

Nesse sentido, a primeira afirmação que podemos fazer com absoluta segurança é a de que a prática do *zero-rating* não se enquadra em nenhuma das hipóteses de quebra da neutralidade estabelecidas pelo MCI, já que não decorre de questões de natureza técnica e nem tem implicações emergenciais; trata-se de modelo de negócio voltado para atender interesses comerciais. Mas a disputa permanece quanto a se concluir se esta prática configura ou não quebra da neutralidade. Sendo assim, voltamos a resgatar o Decálogo de Princípios do CGI.br que, ao tratar da neutralidade, deixou fixado o seguinte: "filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento".

Também traz grandes contribuições para a análise da prática do *zero-rating* o consenso estabelecido na Declaração de São Paulo, resultado do Encontro multissetorial NETmundial[1], ocorrido no Brasil em abril de 2014 envolvendo mais de 12 países, que trata de princípios para a governança da Internet, estando entre eles:

Espaço unificado e não fragmentado: a Internet deve continuar como um espaço unificado e não fragmentado com vistas a que continue a ser uma rede de redes globalmente coerente, interconectada, estável, não fragmentada, escalável e acessível, baseada em um conjunto comum de identificadores únicos, permitindo o livre fluxo de informações de ponta a ponta independentemente de seu conteúdo.

Arquitetura aberta e distribuida: a Internet deve ser preservada como um ambiente fértil e inovador baseado em uma arquitetura de sistema aberto, com colaboração voluntária, gestão coletiva e participação, apoiando a natureza ponta a ponta da Internet aberta, e buscando especialistas técnicos para resolver problemas técnicos no local apropriado de uma maneira consistente com esta abordagem aberta e colaborativa.

Ambiente favorável para a inovação sustentável e a criatividade: a capacidade de inovar e criar está no âmago do notável crescimento da Internet e trouxe grande valor para a sociedade global. Para a conservação de seu dinamismo, a governança da Internet deve continuar a permitir a inovação livre de barreiras através de um ambiente de Internet favorável, consistente com outros princípios deste documento. Empreendedorismo e investimentos em infraestrutura são componentes essenciais de um ambiente favorável.

Entendemos que a prática do *zero-rating* associada a planos franqueados com acesso restrito a determinados conteúdos e aplicações e bloqueio a todo o resto da Internet viola a neutralidade, trazendo graves prejuízos para a sociedade brasileira, tanto pelo aspecto econômico, quanto aspecto social.

Sendo assim, pela perspectiva dos princípios de governança da Internet aceitos internacionalmente e de acordo com o MCI, entendemos que a prática do *zero-rating* associada a planos franqueados com acesso restrito a determinados conteúdos e aplicações e bloqueio a todo o resto do que se encontre disponível na Internet viola a neutralidade, trazendo graves prejuízos para a sociedade brasileira, tanto pelo aspecto econômico, quanto aspecto social.

A prática do *zero-rating* associada aos planos com limite de volume de dados e restrição de acesso à Internet ao final da franquia cria condições para que a Internet se torne um espaço voltado preponderantemente à interesses comerciais e contrário à verdadeira efetiva inclusão digital.

1. http://netmundial.br/pt/about

:: IMPACTOS ECONÔMICOS DECORRENTES DO *ZERO-RATING*

Para avaliar os impactos econômicos decorrentes da prática do *zero-rating* do modo como vem sendo comercializada pelos provedores de acesso, importante considerar que empresas de infraestrutura de telecomunicações, com Poder de Mercado Significativo, e que atuam como provedores de acesso à Internet, se associam a empresas fornecedoras de conteúdos e aplicações, potencializando os efeitos anticoncorrenciais e desestimuladores para a inovação por pequenas e médias empresas.

Dados divulgados pela Alexa[2] neste ano revelam os dez sítios eletrônicos mais frequentados no Brasil, na seguinte ordem: Google.com.br; Facebook.com; google.com; youtube.com; uol.com.br; globo.com; live.com; yahoo.com; mercado livre.com.br e wikipedia.org. Associando-se o poder de mercado das empresas fornecedoras de conteúdos e aplicações ao *market share* das principais operadoras de telecomunicações e provedoras de acesso à Internet no Brasil, com a adoção da prática do *zero-rating*, é impossível deixar de reconhecer que se trata de concentração indesejada nas mãos de grandes grupos econômicos transnacionais, cujo efeito é a verticalização da prestação dos serviços de acesso à Internet e fornecimento de aplicações e conteúdos, capaz de afetar a inovação, a liberdade de expressão, o livre fluxo de informações, a diversidade cultural, o desenvolvimento econômico das classes de baixa renda e, como consequência, o comprometimento da democracia.

Participação dos Grupos no mercado – 1º Trimestre 2015[3]

	Receita (%)		Market Share (Acessos)		
	Bruta	Líquida	Tel. Fixos	Celulares	B.Larga
Telefónica/Vivo	25,9%	25,6%	23,4%	28,9%	16,7%
América Móvil	24,2%	25,7%	26,1%	25,4%	31,6%
Oi	21,4%	19,5%	35,8%	17,8%	26,6%
Tim	13,2%	12,9%	1,2%	26,7%	-
Sky	6,1%	7,3%	-	-	-
GVT	4,4%	4,1%	10,4%	-	12,5%
Nextel	2,9%	3,0%	-	0,64%	-
Outros	1,8%	2,0%	3,0%	0,6%	11,9%
Total Brasil	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**

2. http://www.alexa.com/topsites/countries/BR 3. http://www.teleco.com.br/operadoras/grupos.asp

E a justificativa para a prática do *zero-rating* no Brasil no sentido de que se trata de planos voltados para consumidores de baixa renda, que não têm como contratar planos ilimitados, também não se sustenta, pois nos países em que se permite esta prática os preços subiram ao invés de cair, como não poderia deixar de ser tendo em vista os danos decorrentes de condutas concentradoras. Mas nos países em que se proibiu o *zero-rating* os preços caíram.

O domínio de mercado das empresas de aplicações e conteúdos tem trazidos outros efeitos danosos para o desenvolvimento da Internet, especialmente nos mercados emergentes. O Facebook gera uma tal concentração do tráfego de dados, a ponto de os usuários confundirem Internet com o próprio aplicativo. Matéria publicada na Quartz[4] traz pesquisa revelando que milhões de usuários não têm a menor ideia de que estejam na Internet.

Porcentagem de respostas concordando com a frase: "O Facebook é a Internet"[5]

Nigéria	65%
Indonésia	61%
Índia	58%
Brasil	55%
EUA	5%

Estes dados revelam um problema econômico e não apenas mera confusão semântica. Considerando-se que há dezenas de milhões de usuários no Brasil sujeitos aos efeitos da prática do *zero-rating* e aderentes às principais plataformas de aplicação como Facebook, teremos efeitos decisivos no modo de evolução da Internet como um todo, na medida em que *startups*, organizações da sociedade civil, editoras, governos e todos os agentes que atuam no mercado, para se comunicarem em larga escala, terão de reverenciar estes grandes grupos econômicos, que poderão condicionar a formação da consciência de milhões e milhões de pessoas de acordo com interesses comerciais, como resultado da concentração do mercado de informação. Isto sem falar nos aspectos de segurança e proteção da privacidade pois as cinco empresas de aplicação mais acessadas no Brasil e no mundo, não por coincidência, participam do sistema de vigilância massiva e arbitrária realizada pela Agência de Segurança Nacional dos Estados Unidos – a NSA.

:: DIREITOS DO CONSUMIDOR E *ZERO-RATING*

O *zero-rating* impacta também direitos básicos do consumidor, especialmente o direito de escolha e o impedimento de venda casada. Considerando o poder de mercado das principais empresas fornecedoras de aplicação e conteúdos, quem

4. http://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-Internet 5. Dados: Geopoll, Jana, SurveyMonkey.

Assim, no momento de contratar o acesso à Internet, o consumidor que não puder pagar por um plano ilimitado estará sujeito ao pacote de aplicações ofertado pelo provedor e, ao fim da franquia, terá acesso a uma parte ínfima do universo da Internet.

determina o que deixará de ser descontado da franquia são os interesses econômicos das empresas que se associam e não o interesse e necessidades do consumidor.

Assim, no momento de contratar o acesso à Internet, o consumidor que não puder pagar por um plano ilimitado estará sujeito ao pacote de aplicações ofertado pelo provedor e, ao fim da franquia, terá acesso a uma parte ínfima do universo da Internet. Mas este bloqueio à Internet contraria as garantias inerentes aos serviços públicos essenciais. O Código de Defesa do Consumidor trata dos serviços públicos e determina que, quando forem essenciais devem ser prestados de forma contínua.

Ou seja, esgotado o volume de dados correspondente à franquia, a velocidade do provimento poderá até ser reduzida, mas o acesso irrestrito à Internet deve ser mantido, levando em conta a definição constante do MCI, qual seja: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes.

:: *ZERO-RATING* E INTERESSE PÚBLICO

Mas a prática do *zero-rating*, como já ponderamos acima, não é lesiva por si só. Poderia ser utilizada para atender o interesse público caso os governos e entidades da administração pública formulassem contratos com os provedores de modo a garantir que o acesso a serviços públicos não fosse descontado da franquia. Por exemplo, não haveria cobrança quando o usuário acessasse sítios eletrônicos para entregar declaração de imposto de renda, pagar tributos, lavrar boletins de ocorrência, utilizar serviços de saúde pública, se inscrever em programas sociais, participar de consultas públicas etc. Ou seja, o acesso estaria sendo patrocinado pelos poderes públicos, com vistas a ampliar a fruição de serviços públicos e o exercício da cidadania.

:: A NEUTRALIDADE E O MERCADO EUROPEU

Em 30 de junho deste ano anunciou-se largamente que o Parlamento Europeu, o Conselho e a Comissão Europeia chegaram a um acordo[6] sobre elementos essenciais para um mercado único de

6. http://europa.eu/rapid/press-release_MEMO-15-5275_en.htm

telecomunicações, definindo o fim da cobrança de roaming na Europa até junho de 2017 e também introduzindo regras para garantir o caráter aberto da Internet naquele mercado.

O documento consagra regras para garantir o princípio da neutralidade da rede na legislação, impedindo o bloqueio ou estrangulamento de conteúdos *on-line*, aplicações e serviços, de modo que em toda a União Europeia, contribuindo para um mercado único, com vistas a reduzir o cenário de fragmentação. O acordo especifica expressamente que todo europeu tem de ter acesso à Internet aberta e todos os provedores de conteúdo e de serviços devem tratar igualmente o tráfego, proibindo a priorização paga. A gestão do tráfego foi permitida desde que seja razoável, de acordo com requisitos técnicos justificados, e que deve ser independente da origem ou destino dos pacotes de dados.

Há menção expressa quanto ao *zero-rating* no sentido de que esta prática não pode implicar em bloqueio de conteúdos concorrentes e que, nestes termos, pode apresentar efeitos benéficos, promovendo uma maior variedade de ofertas para os usuários de baixa renda, incentivando-os a usar mais serviços digitais. Entretanto, há ponderações no sentido de se evitar que esta prática comercial leve à situações em que o poder de escolha dos consumidores fique reduzido, impondo às autoridades reguladoras o dever de acompanhar e assegurar o cumprimento das regras.

:: PAÍSES QUE PROIBIRAM O *ZERO-RATING*

Há países, porém, que proibiram expressamente essa prática, como é o caso do Canadá, Chile, Holanda e Noruega, basicamente sob o fundamento de que a prática, além de implicar em discriminação por conteúdo ou serviço e violar a neutralidade, propicia vantagens indevidas entre fornecedores de serviços equivalentes.

A INFRAESTRUTURA DE SUPORTE AO SERVIÇO DE ACESSO À INTERNET

A justificativa utilizada por aqueles que defendem a prática de associar o *zero-rating* a planos franqueados tem sido a insuficiência de infraestrutura no Brasil frente à crescente demanda por redes com alta capacidade de tráfego e que, por isso, não teríamos como garantir à todos os brasileiros o acesso irrestrito à Internet. Mas os formuladores de políticas públicas para a Internet devem seguir as diretrizes do MCI que garantem o acesso à Internet a todos, em caráter universal, de modo que as ferramentas regulatórias para estimular investimentos em infraestrutura deveriam estar sendo aplicadas, como está previsto na Lei Geral de Telecomunicações, no sentido de que os serviços considerados essenciais não podem ser explorados exclusivamente no regime privado. Isto porque o regime público viabiliza que o Poder Público possa estabelecer metas de universalização e utilizar os recursos do Fundo de Universalização

dos Serviços de Telecomunicações (FUST), que atualmente arrecada a cada ano mais de R$ 2,5 bilhões, para serem investidos na ampliação das redes de banda larga, que, associados a investimentos privados, poderão estar a favor da democratização do acesso à Internet, já que hoje a infraestrutura além de ser escassa está altamente concentrada nas localidades que concentram a renda do país – regiões Sul e Sudeste.

Porém, admitir a prática do *zero-rating* do modo como vem sendo praticada no Brasil significa um estímulo ao não investimento, pois ao se permitir o bloqueio do acesso a Internet e sua restrição a aplicações e conteúdos que dependem de baixa capacidade de tráfego para serem utilizados, alivia-se a obrigação do estado e das empresas de promoverem investimentos para a ampliação da infraestrutura pela redução da demanda. E esta solução bate de frente com os objetivos do MCI.

> Ou seja, o MCI reconheceu expressamente que a neutralidade está relacionada a outros direitos, que devem ser avaliados na análise do cumprimento ou não da obrigação de não discriminação ou degradação do tráfego.

:: A NEUTRALIDADE, O DIREITO DO CONSUMIDOR E AMBIENTE CONCORRENCIAL NO MARCO CIVIL

Há quem diga que a neutralidade, como prevista no MCI, deve ser vista exclusivamente pelo aspecto técnico e que outras abordagens jurídicas relativas aos direitos do consumidor e garantia de ambiente concorrencial não deveriam ser consideradas na análise do cumprimento das obrigações de tratamento não discriminatório aos pacotes de dados pelos provedores de acesso à Internet. Entretanto, o certo é que o MCI é uma lei voltada para a proteção de direitos humanos e civis, justamente diante do fato de que a Internet, apesar de ser um espaço público, como uma cidade, um parque ou o meio ambiente, surgido da interconexão de redes em escala mundial, está sujeita ao poder de poderosos grupos econômicos transnacionais, que veem na Internet uma oportunidade infinita de lucros, bem como ao poder de governos autoritários que encaram este valioso palco para as mais diversas e livres manifestações do pensamento e comunicação como uma ameaça aos seus domínios.

Sendo assim e considerando os fundamentos, princípios e objetivos declarados no MCI e o

próprio texto do art. 9º, que trata da neutralidade, entendemos que restringir o alcance do MCI a questões técnicas será um erro de adequação, pois significa reduzir o ganho social e econômico que foi a aprovação da lei. E a redução defendida por alguns ao nosso ver contraria a própria lei, na medida em que encontramos no art. 9º disposições no sentido de que nas hipóteses de discriminação ou degradação do tráfego, o provedor de acesso deve se abster de causar dano aos usuários, agir com proporcionalidade, transparência e isonomia, oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais. Ou seja, o MCI reconheceu expressamente que a neutralidade está relacionada a outros direitos, que devem ser avaliados na análise do cumprimento ou não da obrigação de não discriminação ou degradação do tráfego.

Restringir o alcance da garantia da neutralidade a aspectos exclusivamente técnicos expurgando reflexões mais amplas e de natureza jurídica, significa ignorar a realidade de que os agentes econômicos que atuam na cadeia da Internet estão cada vez mais concentrados, prestando os serviços de forma vertical, associando-se para explorar a infraestrutura de telecomunicações e comercializar serviços de acesso à Internet e fornecimento de aplicações e conteúdos, com o objetivo de impedir a concorrência efetiva e manter altos preços de forma cartelizada, colocando em risco o caráter democrático da rede. E esta visão restrita nos colocará na situação de por em risco que a nossa "Constituição da Internet" perca sua dimensão social e econômica e deixe de ter relevância no cenário mundial como referência geopolítica para a regulamentação dos direitos da Internet. ●

Arzak Khan fundador e diretor do Internet Policy Observatory do Paquistão.

A Internet.org arrisca o futuro da Web no Paquistão[1]

O esforço de Zuckerberg-Telenor para trazer a Internet para o mundo em desenvolvimento é contraproducente. A Internet.org, parceria entre o presidente da Facebook Mark Zuckerberg e a operadora de telecomunicações norueguesa Telenor, procura oferecer o acesso à Internet para dois terços da população mundial que ainda não está conectada e trazer para todos as mesmas oportunidades que o mundo conectado tem nos dias de hoje. O projeto foi lançado em julho de 2014 na Zâmbia, em seguida na Tanzânia, Quênia, Colômbia, Gana, Índia, Filipinas, Guatemala, Indonésia, Bangladesh e Malavi.

Agora o projeto está chegando ao Paquistão, onde nasci. Através do aplicativo Internet.org, os 37 milhões de clientes da Telenor no Paquistão têm acesso via Internet gratuita a 17 sites, dentre os quais uma das mídias sociais, o popularíssimo serviço Facebook, juntamente com a BBC, a Wikipedia e outros serviços de notícias, saúde, educação, finanças e informação. Os objetivos da Internet.org baseiam-se em um problema real que milhões de pessoas sem acesso à Internet no Paquistão enfrentam devido a baixos níveis de renda, custos elevados, falta de capacitação do usuário e, acima de tudo, uma precária infraestrutura de telecomunicações.

1. Publicado originalmente pela Al Jazeera America em http://america.aljazeera.com/opinions/2015/6/internetorg-risks-the-webs-future-in-pakistan.html

Os paquistaneses que porventura se conectem pela primeira vez usando a Internet.org correm o risco de ficar sem saber o que é a Internet de verdade, que pode dar-lhes oportunidades ilimitadas de desenvolvimento socioeconômico, e acabar perdendo todo o interesse pelo que venha a ser a Internet.

Apesar das aparentemente nobres intenções do esforço conjunto, a iniciativa tem mais percalços do que benefícios. Primeiro, tanto a Internet.org quanto a Telenor estão comercializando enganosamente para as pessoas essa iniciativa como "a Internet", enquanto o livre acesso à rede propiciado não é a Internet de verdade, mas sim um limitado pacote de sites Web aprovados pela Facebook com significativas falhas de privacidade e segurança. Segundo, essa iniciativa não ajuda a resolver as questões de conectividade dos países em desenvolvimento como o Paquistão e ainda aprofunda sua gravidade ao oferecer uma plataforma para acesso restrito à Internet onde as pessoas de recursos econômicos mais escassos contam com parcas oportunidades de ingresso na economia cibernética global. Assim sendo, o esforço em questão pouco ajuda a resolver a exclusão digital.

Os paquistaneses merecem o direito de saborear a Internet de verdade, e não a que lhes é servida pela Internet.org. O sucesso da Internet se deve a sua abertura, igualdade de oportunidades e inovação. Plataformas como o Facebook não teriam sido criadas se Zuckerberg só tivesse acesso à Internet através de uma iniciativa como essa. Além disso, a Internet já é vista como um meio importante, capaz de ajudar países como o meu a desenvolver economias de sucesso. Mas o Paquistão é prejudicado por uma infraestrutura de banda larga precária, por velocidades baixas e indisponibilidade de acesso. Os paquistaneses que porventura se conectem pela primeira vez usando a Internet.org correm o risco de ficar sem saber o que é a Internet de verdade, que pode dar-lhes oportunidades ilimitadas de desenvolvimento socioeconômico, e acabar perdendo todo o interesse pelo que venha a ser a Internet.

Apesar do acesso limitado, a Internet já se tornou, num curto período de tempo, um poderoso veículo de mudança no Paquistão. Dos 191 milhões de paquistaneses, 30 milhões têm Internet, metade dos quais através dos seus telefones celulares, segundo o relatório de pesquisa da empresa Ansr.io. A Internet deu a essas pessoas

a genuína liberdade de expressão sem censura. Paradoxalmente, a Internet.org veio colocar tal liberdade em risco.

Sua existência tem consequências que podem ser prejudiciais em regimes repressores como o do Paquistão, onde os governos querem pautar a censura à Internet em nome da segurança nacional e de valores sociais e religiosos. Através dessa iniciativa, a Facebook coloca-se estranhamente numa posição na qual os governos conseguem exercer pressão para bloquear certos tipos de conteúdo ou os usuários que os acessam. Isso pode ser especialmente prejudicial para usuários politicamente ativos em ambientes restritivos. Além disso, a segurança e a privacidade de usuários individuais também corre risco constante de sofrer ataques maliciosos e espionagem por parte do governo.

O objetivo de fornecer acesso à Internet de maneira universal e a custos razoáveis a todas as pessoas na face da Terra é grande demais e importante demais para ser resolvido apenas por uma empresa, um grupo ou um governo. Para alcançá-lo, é necessária uma abordagem coesiva multissetorial, capaz de demonstrar – além do compromisso com o interesse público – justeza e transparência. Quanto a esse esforço específico, através da Internet.org a Facebook parece estar mais interessada em expandir sua base de usuários e seu império de publicidade no mundo em desenvolvimento, tudo em nome de propiciar acesso gratuito à "Internet". Essa nefasta agenda de desenvolvimento não é muito diferente daquelas que eram seguidas nos tempos do colonialismo, do imperialismo e em seguida do capitalismo, nos quais os governos e as corporações mais engenhosos exploravam os países pobres com falsas promessas de desenvolvimento.

Juntamente com todos os povos dos outros países em desenvolvimento, os paquistaneses merecem o direito a saborear a Internet de verdade, e não aquela entregue pela Internet.org. O esforço Zuckerberg-Telenor não só prejudica o crescimento, a liberdade e a expansão da Web no Paquistão como também arrisca criar uma Internet em dois patamares cerceando milhões de pessoas no mundo em desenvolvimento justamente no lado errado da exclusão digital. ●

> O sucesso da Internet se deve a sua abertura, igualdade de oportunidades e inovação. Plataformas como o Facebook não teriam sido criadas se Zuckerberg só tivesse acesso à Internet através de uma iniciativa como essa.

A autoridade certificadora Let's Encrypt: uma oportunidade para criptografar toda a Web

> **Seth Schoen** tecnólogo senior da Electronic Frontier Foundation (EFF).

Em uma Internet cada vez menos segura e confiável, vemos ainda muito pouco uso de tecnologias de segurança como o protocolo HTTPS para acesso seguro a sites Web. Há várias dificuldades na adoção mais ampla de HTTPS e outras técnicas, inclusive obstáculos devido ao sistema de certificação digital. Uma iniciativa da Electronic Frontier Foundation, Mozilla, Universidade de Michigan e parceiros pretende criar uma nova autoridade certificadora, chamada Let's Encrypt, para melhorar esta situação tornando mais acessível o uso de tecnologias essenciaisde segurança.

Os cientistas da computação têm tradicionalmente alertado para não depositarmos confiança na infraestrutura de rede fora de nosso controle físico. Tem-se a impressão que os dados simplesmente aparecem em nosso navegador depois que digitamos o endereço de um site Web, ou que nossos chats ou e-mails simplesmente aparecem em dispositivos de nosso amigo. Na realidade – como o jornalista Andrew Blum destaca em *Tubes: A Journey to the Center of the Internet* – eles são levados através do espaço físico por hardware físico que existe em algum lugar e que é possuido e gerido por alguém[1]. Na maioria das vezes não podemos ver como os nossos dados foram transportados ou o percurso dos mesmos até chegar aos nossos amigos; não podemos ver ou controlar o que aqueles que operam o hardware ao longo do caminho estão fazendo[2].

Os operadores de infraestrutura e outros que controlam partes do caminho dos nossos dados estão em condições de causar muitos danos que sequer podemos perceber. Eles podem ver nossa comunicação, podem gravá-la em bases de dados enormes, podem associá-la conosco de modo que o que fizemos ou dissemos na Internet passe a ser pesquisável. Eles podem roubar nossas senhas e passar-se por nós. Eles também podem alterar o que comunicamos, escondendo coisas de nós, impedindo-nos de dialogar sobre certas ideias,

1. Ver Andrew Blum, *Tubes: A Journey to the Center of the Internet* (Ecco, 2013). 2. É importante notar que estas preocupações não se aplicam apenas aos atos volitivos de nossos próprios prestadores de serviços de Internet comerciais. As ameaças à comunicação são muito diversificadas. A sabotagem no tráfego da Internet pode ser realizada por outras pessoas em nossas redes wi-fi (digamos, em um café ou em uma escola), por alguém que pode invadir nossos roteadores wi-fi (que normalmente têm software desatualizado que raramente recebem atualizações depois de fabricados), por provedores de serviços Internet que anunciam rotas espúrias, por aqueles que controlam partes da infraestrutura de nomeação DNS, por espiões que grampeiam cabos de fibra óptica, e por governos que obrigam os provedores a conceder-lhes acesso ao hardware de rede ou secretamente exploram suas vulnerabilidades.

removendo ou reescrevendo enlaces ou parágrafos em nossos textos, infectando os nossos downloads de software com malware, ou colocando seus próprios anúncios no corpo das páginas Web que visitamos.

Temos soluções técnicas baseadas em criptografia para responder à ideia que a infraestrutura de rede não pode ser confiável e devemos proteger-nos dela, mas essas soluções estão em um estado fragmentário. Eles são frequentemente frágeis e estão longe de estar implantadas universalmente. Mesmo a maioria das principais redes sociais, provedores de webmail e serviços de bate-papo até há pouco tempo não forneciam qualquer tipo de criptografia. Isso significa que era trivial para um operador de rede, um "grampeador" da Internet, ou até mesmo alguém em sua rede wi-fi gravar e procurar tudo o que você comunicou nesses espaços – e, em muitos casos, assumir o controle de suas contas. Ainda hoje, muitos serviços populares e a maioria das redes de publicidade não utilizam criptografia, permitindo que as comunicações de seus usuários sejam alvos fáceis para espionagem[3].

:: HTTPS

A tecnologia de criptografia mais usada e mais universalmente disponível capaz de abordar algumas dessas ameaças é HTTPS, a versão segura do protocolo HTTP. HTTPS está disponível em todos os navegadores Web, mas funciona apenas com os sites configurados para isso. Embora o HTTPS tenha sido desenvolvido há duas décadas, os sites habilitados para HTTPS ainda são uma minoria da Web hoje, e são ainda mais raros nos países em desenvolvimento e em sites Web pessoais e não comerciais.

A maravilha da tecnologia de criptografia de chave pública, concebida na década de 1970, é que os usuários não precisam ter qualquer relação prévia para configurar uma conexão segura, mesmo se alguém estiver capturando tudo o que está sendo comunicado[4]. A tecnologia de chave pública é usada em TLS, a camada criptográfica por trás do HTTPS[5]. No entanto, um risco de captura por um interceptador ainda permanece – o assim chamado "man-in-the-middle attack"[6] –, a menos que os dois lados da comunicação possam confirmar que estão usando as mesmas

3. Os usuários não têm que identificar-se em um site (ou mesmo estar cientes que o site existe) para que este seja usado para espionagem. Reportagens do *The Intercept* e do *Washington Post* com base em documentos fornecidos por Edward Snowden mostraram que as agências de inteligência criam sistemas de rastreamento de usuários que interceptam os cookies de redes de publicidade em conexões HTTP não criptografadas para identificar dispositivos móveis e assim localizar usuários da Internet, e até mesmo direcionar ataques contra eles. 4. Esta propriedade da segurança é baseada em problemas matemáticos com uma estrutura assimétrica ou de alçapão ("trapdoor"), que são fáceis de resolver dado algum conhecimento secreto, mas muito difícil de resolver sem ele. Entre outras possibilidades, isto significa que o conhecimento de como criptografar uma mensagem pode ser distinto do conhecimento de como decifrá-la; o primeiro pode, então, ser tornado público, enquanto o último é mantido em segredo. 5. O protocolo TLS (Transport Layer Security) era anteriormente conhecido como SSL (Secure Sockets Layer), um termo que ainda está em uso generalizado. O TLS também pode ser usado para proteger os serviços de Internet e protocolos que não sejam HTTP, e os certificados descritos neste artigo também servem para serviços além do HTTP. Este artigo irá discutir apenas o uso de TLS para proteger HTTP, mas os certificados emitidos pela Let's Encrypt também podem ser usados com outros protocolos de Internet. 6. Forma de ataque em que os dados trocados entre duas partes, por exemplo entre o usuário e o seu banco, são de alguma forma interceptados, registrados e possivelmente alterados pelo atacante sem que as vítimas percebam. Durante o ataque "man-in-the-middle", a comunicação é interceptada pelo atacante e retransmitida por este de uma forma discricionária. Os participantes legítimos da comunicação não percebem que os dados podem estar adulterados e podem fornecer informações ou executar instruções por ordem do atacante. Fonte: *https://pt.wikipedia.org/wiki/Ataque_man-in-the-middle*

chaves de criptografia. Nós às vezes referimo-nos a isso como a garantia "que você está efetivamente visitando o site que você pensa que está" ou "que ninguém está personificando o site", mas a natureza dessa ameaça é específica da criptografia; não se trata necessariamente de "personificar" um site no sentido de criar uma versão do mesmo falsificada do zero, mas sim intermediar criptograficamente uma conexão supostamente segura. Isso significa enganar simultaneamente ambos os lados para estabelecer conexões criptografadas com o interceptador, enquanto ambos os lados da comunicação acreditam erroneamente que estabeleceram conexões criptografadas entre si[7]. Esta ameaça é importante porque pode permitir que um invasor comprometa completamente a segurança do TLS, mas não tem equivalente exato no mundo offline.

A prevenção desses ataques "man-in-the-middle", garantindo que o software dos usuários saiba qual chave de criptografia realmente pertence a determinado site é o objetivo principal das autoridades certificadoras da Internet, as organizações em que os navegadores Web e outros softwares confiam para garantir tais asserções. Para estabelecer uma conexão segura com um serviço, um aplicativo de software do lado do usuário normalmente recebe cópias de certificados digitais emitidos por autoridades certificadoras confiáveis, e verifica que os certificados concordam que a chave de criptografia que o site está aparentemente usando de fato pertence ao site[8].

:: AUTORIDADES CERTIFICADORAS

As autoridades certificadoras aceitas pelos principais navegadores Web são centenas, e estão localizados em dezenas de países. Por convenção, a maioria das autoridades está habilitada a emitir certificados para qualquer nome de domínio da Internet[9], e os navegadores confiam plenamente nas assertivas dessas autoridades (por exemplo, as autoridades não têm de estar na mesma jurisdição que os locais para os quais elas emitem certificados). Isso significa que o sistema de autoridade certificadora só é tão forte quanto o seu elo mais fraco[10]: se uma autoridade certificadora

7. Um atacante do tipo "man-in-the-middle" poderia permitir comunicação entre as partes sem interferência aparente; ao fazer isso, o atacante pode no entanto ler o conteúdo dessas comunicações, o que seria impedido pela criptografia. Uma analogia é uma agência de correios que às vezes consegue abrir envelopes, examinando (e talvez alterando) os seus conteúdos e em seguida fechá-los de modo que pareçam intactos para os destinatários dos envelopes. A vulnerabilidade a um ataque criptográfico "man- in-the-middle" é semelhante à impossibilidade de detectar quando e se os selos foram violados; isso não significa que todas as comunicações serão sempre interceptadas, mas que alguns atacantes poderiam interceptá-las sem ser percebidos. 8. Os certificados também podem conter outras afirmações sobre a identidade do mundo real de alguma entidade, por exemplo, afirmando que um site é operado por uma determinada empresa ou organização, em um endereço físico específico. Esse tipo de verificação é menos importante para a segurança em geral. A maioria dos usuários finais raramente ou nunca consulta essa informação, e a capacidade dos navegadores em estabelecer ou não uma conexão segura é determinada apenas pela verificação de que as chaves criptográficas são válidas. O navegador não verifica se o certificado diz que google.com.br é operado pela Google Inc., de Mountain View, Califórnia, mas apenas se a chave criptográfica de curva elíptica 045cf96e6579eb74ed905a60fdee882a1 290e8c5c2e85ecfe14b047085193df9d b0c61a803a894729b6d22583ef83da80b 7d396809b54600f4bb21d742ad079448 pertence de fato ao operador do domínio google.com.br. 9. Existem meios técnicos para restringir os nomes de domínio para os quais uma certificadora pode emitir certificados, mas estes meios são usados raramente. 10. Hoje em dia, sites especialmente preocupados com a segurança podem reduzir o risco com tecnologias como "public-key pinning" (HPKP), extensão do HTTP que alerta os navegadores para rejeitarem alterações inesperadas de um certificado; no entanto, cada site tem que optar por ativar essa proteção.

é atacada ou induzida a emitir certificados falsos, seus certificados serão aceitos pelos navegadores, mesmo quando não houver relação prévia entre essa autoridade e o site para o qual ela emite certificados. (Em um incidente notório em 2011, a autoridade certificadora holandesa DigiNotar foi penetrada, aparentemente por um hacker iraniano ativista pró-governo[11]; em consequência emitiu certificados fraudulentos para o Gmail e outros serviços, que os navegadores dos usuários iranianos automaticamente aceitaram, mesmo que não houvesse relação entre esses sites e a DigiNotar.)

Embora existam algumas autoridades certificadoras de governos ou empresas que operam principalmente para o uso interno dessas organizações, a maioria das autoridades certificadoras existentes cobram um preço para emitir certificados, que tem-se revelado um negócio rentável. (Por exemplo, a fortuna do filantropo Mark Shuttleworth, que foi responsável pela criação do sistema operacional Ubuntu, é um resultado do sucesso de sua empresa certificadora, a Thawte.) As autoridades certificadoras têm custos fixos elevados, especialmente com sua infraestrutura física, serviços jurídicos e de auditoria, testes de segurança e pessoal. Criar uma nova autoridade certificadora do zero é considerado um empreendimento que pode custar centenas de milhares de dólares.

O sistema de autoridade certificadora só é tão forte quanto o seu elo mais fraco: se uma autoridade certificadora é atacada ou induzida a emitir certificados falsos, seus certificados serão aceitos pelos navegadores, mesmo quando não houver relação prévia entre essa autoridade e o site para o qual ela emite certificados.

A obtenção de um certificado também tem sido uma tarefa cara e complicada. O cliente precisa pagar uma autoridade certificadora e lidar com uma série de tarefas especializadas para solicitar um certificado e provar sua posse de um nome de domínio. Em nossa experiência, mesmo um administrador de sistemas experiente vai consumir mais de uma hora nessa tarefa se não for uma parte de suas responsabilidades regulares. Pessoas tecnicamente menos sofisticadas muitas vezes não conseguem completar o processo.

Muitos sites e serviços também têm sido levados a crer que não precisam de um certificado porque não lidam com pagamentos ou números de cartões de crédito, ou porque eles terceirizam pagamentos

11. Ver os detalhes do caso em https://www.eff.org/pt-br/deeplinks/2011/09/post-mortem-iranian- diginotar-attack

para algum outro serviço online. Sites Web que aceitam pagamentos com cartão de crédito diretamente devem exigir conexões HTTPS para este fim, com um certificado que seu navegador aceite como confiável, como resultado das regras estabelecidas no Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (Payment Card Industry Data Security Standard, PCI DSS). Mas outros sites frequentemente não são oficialmente obrigados a usar HTTPS; como resultado, eles podem desativar o protocolo, ou mesmo sugerir que seus usuários ignorem os avisos de segurança do navegador. A forte associação entre HTTPS e transações financeiras tem sido difícil de quebrar, já que muitos administradores não levam em conta que seus sites não financeiros também devem proteger a confidencialidade de seus usuários.

Ativistas da privacidade, especialistas em segurança da Web e até mesmo o governo dos Estados Unidos propuseram uma utilização mais universal do HTTPS por uma gama mais ampla de sites Web[12]. A versão 2010 da ferramenta de ataque fácil de usar Firesheep (que permite que usuários de uma rede wi-fi violem contas de outros usuários online com um único clique, se as vítimas estiverem usando uma conexão HTTP insegura) ajudou a sublinhar os riscos para os serviços que permitem login em uma conta. Operadores de redes sociais e de webmail em geral reagiram ao Firesheep, tornando disponível ou obrigatório o HTTPS para seus sites.

Mas sites de notícias e de referência, fóruns não-comerciais, redes de publicidade, e até mesmo fontes de download de software têm sido mais resistentes a adotá-lo, mesmo que seus usuários também estejam em risco de censura, rastreamento e ataques de malware.

:: LET'S ENCRYPT

Um grupo de especialistas em privacidade e segurança na Internet da Universidade de Michigan, Mozilla e a Electronic Frontier Foundation uniram-se para criar uma nova autoridade certificadora chamada Let's Encrypt (Vamos Criptografar). A Let's Encrypt planeja estar disponível ao público em meados de setembro; a base tecnológica está sendo desenvolvida em público, incluindo o software cliente-servidor e o protocolo de rede a ser usado para comunicação mútua[13].

A ideia central da Let's Encrypt é que o nível básico de validação de identidade pela autoridade certificadora pode ser realizado automaticamente. (Esta verificação básica, chamada Validação de Domínio, confirma que a entidade que solicita um certificado na realidade tem controle sobre o nome de domínio que é objeto do referido certificado – por exemplo, verificando a capacidade da entidade de fazer alterações em serviços hospedados sob esse nome de domínio.) Já que a validação e consequente emissão de

12. Ver, por exemplo, http://www.w3.org/2001/tag/doc/web-https e https://https.cio.gov. 13. Ver https://www.letsencrypt.org, site oficial da Let's Encrypt, que inclui enlaces para o código-fonte e o rascunho do padrão ACME.

certificado pode ser realizada sem intervenção humana, não há quase nenhum custo marginal associado à emissão de um certificado para um novo domínio. Isto significa que este serviço pode ser prestado em grande escala em um modelo sem fins de lucro, sem custo para o usuário final que recebe o certificado.

A ênfase em automação também significa que os administradores de sistemas dos usuários não terão que executar a tarefa manual demorada e inconveniente de obter, instalar e renovar certificados. O software cliente da Let's Encrypt cuidará da tarefa de gerar chaves criptográficas, automaticamente autenticando o detentor do nome de domínio especificado, obtendo o certificado e até mesmo instalando o mesmo no software de servidor Web Apache ou Nginx. (Contribuições de código para integrar o software cliente com outros softwares de servidor Web serão bem-vindas).

Desta forma eliminamos os obstáculos de custo, tempo e esforço que são barreiras para que sites e serviços mudem para HTTPS. Nosso objetivo é permitir que um administrador de sistemas leve menos de um minuto para obter e instalar um certificado confiável, sem nenhum custo, executando um único comando em um servidor. Os navegadores mais comuns aceitarão estes certificados automaticamente como resultado de um acordo alcançado entre IdenTrust (uma autoridade certificadora já existente) e a entidade operadora da Let's Encrypt. Usuários de navegadores Web não têm que mudar ou atualizar nada para que os certificados Let's Encrypt sejam aceitos; eles simplesmente navegam na Web como de costume e estarão automaticamente protegidos.

Para obter um certificado, o usuário da Let's Encrypt executa nosso software cliente livre (ou qualquer software de terceiros compatível com nosso protocolo ACME) em um servidor Web, selecionando os nomes de domínio para os quais será obtido o certificado, em geral a partir de uma lista gerada automaticamente. O software cliente conecta-se a nossa autoridade certificadora usando o protocolo ACME e solicita um certificado; a autoridade desafia o cliente a provar que detém os nomes de domínio, o que é feito automaticamente, fazendo alterações solicitadas no servidor Web. Quando a autoridade aprova, já emite o certificado, e o software cliente o instala automaticamente. (Na maioria dos casos, o software cliente irá renovar automaticamente o certificado quando este expirar e instalará automaticamente a versão atualizada. Isso vai reduzir a incidência dos erros irritantes no navegador Web que aparecem quando certificados expiram e não são imediatamente renovados.) Todo esse processo pode ser concluído em um minuto ou menos.

Eventualmente esperamos ter parcerias com empresas de hospedagem Web populares

e CDNs ("content-delivery networks"[14]) para gerar e instalar automaticamente os certificados disponíveis para todos os seus clientes, e esperamos também que o software cliente Let's Encrypt seja incluído em todos os principais sistemas operacionais de servidor Web. (Os nossos serviços continuarão a ser de uso livre para os clientes em qualquer escala, sejam pessoas físicas ou grandes corporações. Estamos financiados por doações de nossos parceiros e de indivíduos que entendem que o nosso serviço constitui uma parte importante para tornar a Internet mais segura.)

:: TRANSPARÊNCIA

Preocupações consideráveis têm sido levantadas que autoridades certificadoras possam ser atacadas por hackers (como aconteceu com DigiNotar, Comodo, e outros) ou sejam forçadas pelos governos a emitir certificados fraudulentos para facilitar a interceptação (como foi sugerido por

14. Designação de grandes sistemas distribuidos de servidores instalados em múltiplos datacentros na Internet para entregar conteúdo a usuários finais com alta disponibilidade e desempenho. Hoje os CDNs fornecem uma grande parte do conteúdo da Internet, incluindo textos, gráficos, software, serviços de e-comércio, mídia em tempo real, mídia sob demanda, redes sociais e outras aplicações. Fonte: https://en.wikipedia.org/wiki/Content_delivery_network

Soghoian e Stamm[15]; o caso Lavabit também aumentou as preocupações que os governos usariam seu poder para obter chaves criptográficas sensíveis, embora a ordem judicial, nesse caso, tenha sido direcionada a um serviço específico, não a uma autoridade certificadora)[16]. Hoje as autoridades certificadoras têm um poder considerável, uma vez que qualquer autoridade pode emitir um certificado para qualquer site, facilitando a vigilância sobre seus usuários[17]. Existem inúmeras certificadoras que operam em uma ampla variedade de jurisdições, e nenhuma é formalmente obrigada a dizer ao público quais certificados foram emitidos. O setor insiste que autoridades certificadoras devem sujeitar-se a um processo de auditoria, mas este geralmente concentra-se na análise dos controles de políticas, burocráticos e organizacionais em vez da auditagem técnica. Os processos de auditoria também examinam os procedimentos gerais da certificadora, em vez de sua decisão de emitir certificados específicos.

Nós não consideramos que Let's Encrypt seja um alvo particularmente atraente para qualquer hacker ou coerção legal; algumas autoridades certificadoras existentes provavelmente são mais vulneráveis a isso do que nós. Mas os sites devem ser capazes de defender-se contra a emissão de certificados fraudulentos, e o público deve ser capaz de verificar que as certificadoras estão fazendo seu trabalho corretamente.

Felizmente existem novos meios técnicos já disponíveis para responsabilizar as certificadoras e aumentar a transparência das suas operações. Entre estes, o CAA permite que sites informem as certificadoras que não têm contrato com eles para não emitir certificados para estes sites; o HPKP permite que os sites informem o navegador Web sobre quais certificadoras estão autorizadas a emitir certificados para os mesmos; e o sistema de Transparência de Certificados do Google permite que as certificadoras mantenham um registro público de todos os certificados já emitidos, que não pode ser retroativamente alterado[18].

15. Ver Christopher Soghoian e Sid Stamm, "Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL" (em https://s3.amazonaws.com/files.cloudprivacy.net/ssl-mitm.pdf) (sugerindo, com base na literatura da indústria de vigilância, que "agências do governo exigem – via mandato judicial ou outro processo legal – que uma certificadora emita certificados para serem usados por agentes policiais e de inteligência para secretamente interceptar e sequestrar a comunicação segura de indivíduos"). 16. Lavabit era um provedor de webmail seguro baseado nos EUA. Em julho de 2013, o governo dos EUA exigiu judicialmente que o provedor entregasse suas chaves criptográficas secretas. O Lavabit não levantou objeções formais às demandas a tempo e acabou tendo que cumprir a demanda por ordem judicial e revelar suas informações de chaves secretas. Os tribunais, de acordo com resumo da EFF sobre o caso, "não decidiram conclusivamente se ou como o governo pode obrigar um provedor de e-mail a fornecer suas chaves de criptografia privadas ao governo"; ver https://www.eff.org/cases/lavabit (descrevendo o envolvimento da EFF no caso). 17. As preocupações sobre o abuso do poder das autoridades certificadoras para fins de vigilância foram levantadas quando o China Internet Network Information Center (CNNIC) solicitou em 2009 ser reconhecido por desenvolvedores dos navegadores Web como uma certificadora confiável; analistas temiam que o governo da República Popular da China usaria seu controle sobre o CNNIC para forçar a emissão de certificados fraudulentos e espionar as conexões HTTPS. Essa ansiedade reflete uma percepção da República Popular da China como uma praticante particularmente agressiva do vigilantismo (e a certificadora do CNNIC acabou sendo removida da lista de certificadoras confiáveis de alguns navegadores em 2015 depois de um escândalo envolvendo uma delegação indevida de autoridade para uma empresa egípcia). No entanto, certificadoras já existiam em dezenas de jurisdições, e muitas são controladas diretamente por entidades governamentais ou por empresas estatais de telecomunicações. É concebível, como Soghoian e Stamm descrevem, que qualquer governo poderia tentar obrigar secretamente qualquer certificadora dentro de sua jurisdição a emitir certificados falsos.

Estas tecnologias reduzem o poder das certificadoras de emitir certificados fraudulentos e não detectáveis como tal, e o nível de confiança que os usuários da Internet são forçados a ter sobre as mesmas. Isso é uma boa coisa.

O Observatório SSL da EFF e o projeto ZMap da Universidade de Michigan também catalogam os certificados em uso nos servidores visíveis publicamente[19]. Além de definir os procedimentos internos de detecção de fraudes, a Let's Encrypt compromete-se a cooperar com as tecnologias que aumentem a transparência das atividades de certificadoras, além de publicar registros detalhados de todos os certificados emitidos por nós e por que decidimos emitir cada um deles. Também incentivaremos sites a usar tecnologias como HPKP para defenderem-se contra certificados fraudulentos. Esperamos estabelecer um exemplo para o resto do setor de certificação, fazendo o que pudermos para garantir que os ataques contra certificadoras não tenham êxito, ou sejam detectados de imediato.

:: CONCLUSÃO

O TLS e sua infraestrutura de chave pública, constituídos por um grande número de autoridades certificadoras, são sistemas complexos criados às pressas na década de 1990. Eles têm sofrido pressão considerável e falharam de várias maneiras, mas o escrutínio de peritos ao longo dos últimos anos tornou-os cada vez mais seguros e resilientes. O maior problema com TLS e HTTPS hoje não é alguma falha técnica; é o fato de não serem utilizados pela maioria dos sites e assim exporem as comunicações de seus usuários a uma Internet cada vez mais hostil e amplamente vigiada.

Nossa tecnologia será baseada em software livre e padrões abertos da Internet disponíveis para adoção e aperfeiçoamento de todos.

A Let's Encrypt vai ajudar a corrigir isso, tornando rápido, fácil e sem custos para os *sites* em qualquer escala obter certificados que os navegadores mais usados aceitam, e que são renovados automaticamente, de modo que os administradores de sistemas possam considerar esse problema resolvido e dedicar seu tempo a outros desafios. Nossa tecnologia será baseada em software livre e padrões abertos da Internet disponíveis para adoção e aperfeiçoamento de todos. Até o final deste ano, a Let's Encrypt estará fazendo uma contribuição para uma Internet mais segura e universalmente criptografada. ●

18. Ver https://en.wikipedia.org/wiki/DNS_Certification_Authority_Authorization, https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning e http://www.certificate- transparency.org. 19. Ver https://www.eff.org/observatory e https://scans.io.

> Divulgada em 18 de maio de 2015

Carta aberta a Mark Zuckerberg sobre a Internet.org, neutralidade da rede, privacidade e segurança

Caro Mark Zuckerberg,

Nós, abaixo assinados, compartilhamos uma preocupação comum sobre o lançamento e expansão da plataforma Internet.org da Facebook e suas implicações para a Internet aberta ao redor do mundo. Nessa Internet aberta, todos os conteúdos, aplicações e serviços são tratados igualmente, sem discriminação alguma. Estamos especialmente aborrecidos pelo fato que o acesso das pessoas pobres é usado como justificativa para tais violações da neutralidade da rede.

Na sua concepção atual, a Internet.org viola os princípios da neutralidade da rede, ameaçando a liberdade de expressão, igualdade de oportunidades, segurança, privacidade e inovação. Além disso, é nossa convicção que a Facebook está definindo de forma inapropriada a neutralidade da rede em declarações públicas e construindo um jardim murado onde as pessoas mais pobres só podem aceder a um conjunto limitado de sites Web e serviços inseguros. Além disso, estamos profundamente preocupados com o fato que a Internet.org tem sido comercializada de forma enganosa como provimento de acesso à Internet como um todo, quando na verdade ela só permite acesso a um número limitado de serviços conectados à Internet que são aprovados pela Facebook e provedores locais de acesso.

Apoiamos o objetivo de levar o acesso a preços acessíveis aos dois terços do mundo que atualmente carecem de acesso à Internet. Muitos de nós têm trabalhado durante anos em iniciativas para reduzir a brecha digital, como a instalação de facilidades

de acesso à Internet em bibliotecas públicas e telecentros, apoiando iniciativas de provimento de banda larga comunitária, empreendimentos locais de telecomunicações, investimento público em infraestrutura de banda larga, projetos de sites Web e serviços mais acessíveis a pessoas com dispositivos de acesso móvel, e mais. No entanto, temos sempre defendido o provimento de acesso não discriminatório à Internet plenamente aberta, sem privilegiar determinados aplicativos ou serviços em detrimento de outros e sem comprometer a privacidade e a segurança dos usuários.

Estas são diferenças fundamentais em relação à Internet.org.

Em um vídeo de 4 de maio, a Facebook anunciou novas regras relativas à Internet.org e argumentou que a neutralidade da rede e a Internet.org não estão em conflito. No entanto, na página Web relacionada, as novas regras declaram explicitamente que "sites Web devem ser apropriadamente integrados com a Internet.org para permitir o zero-rating."

Abaixo articulamos nossas preocupações sobre a atual estrutura e implementação da Internet.org:

Neutralidade da Rede: a neutralidade da rede apoia a liberdade de expressão e a igualdade de oportunidades ao permitir que as pessoas procurem, recebam e enviem informações e interajam como iguais. Ela requer que a Internet seja mantida como uma plataforma aberta sobre a qual os provedores de redes tratem todos os conteúdos, aplicações e serviços de forma isonômica, sem discriminação. Um aspecto importante da neutralidade da rede afirma que todos devem ser capazes de inovar sem permissão de ninguém ou qualquer entidade.

Instamos a Facebook a afirmar seu apoio a uma verdadeira definição de neutralidade da rede na qual todos os aplicativos e serviços são tratados igualmente e sem discriminação — especialmente no mundo em desenvolvimento, onde os próximos três bilhões de usuários da Internet estarão online — e para abordar as falhas significativas de privacidade e segurança inerentes à versão atual da Internet.org.

Zero-rating: É a prática adotada por provedores de serviço de oferecer um conjunto específico ou aplicações de uso livre sem afetar o plano contratado, ou que não descontam da franquia de dados. Esta prática é inerentemente discriminatória — é por isso que foi proibida ou restringida em países como o Canadá, Holanda, Eslovênia e Chile.

Zero-rating é atualmente o modelo básico da Internet.org: a Facebook faz parcerias com provedores de serviços Internet em todo o mundo para oferecer acesso a determinadas aplicações da Internet sem nenhum custo adicional para os usuários. Estes acordos põem em perigo a liberdade de expressão e a igualdade de oportunidades, permitindo que os fornecedores de serviços Internet decidam quais serviços serão privilegiados em detrimento de outros, interferindo assim com o livre fluxo de informação e os direitos das pessoas em relação às redes.

Nomenclatura: A Internet.org enganosamente chama essas aplicações de zero-rating de "a Internet", quando na verdade os aplicativos só oferecem acesso

a uma pequena parte da mesma. O projeto atua como um "jardim murado", em que alguns serviços são favorecidos em detrimento de outros — novamente, uma violação da neutralidade da rede.

Liberdade de expressão: O projecto revela outros riscos para a liberdade de expressão. A capacidade de censura de gateways de Internet está bem estabelecida — alguns governos exigem que provedores de serviços Internet bloqueiem o acesso a sites ou serviços. A Facebook parece colocar-se em uma posição semelhante, onde os governos poderiam pressionar a empresa a bloquear determinados conteúdos, ou ainda, quando os usuários precisarem identificar-se para acesso, bloquear usuários individuais. A identificação de tais usuários desta maneira pode até mesmo levar a sua detenção. A empresa não deve assumir esta responsabilidade adicional e de risco através da criação de um único posto de controle centralizado para o livre fluxo de informações.

Privacidade: Estamos também profundamente preocupados com as implicações da Internet.org para a privacidade. A política de privacidade da Facebook não fornece proteções adequadas para novos usuários da Internet, alguns dos quais podem não entender como seus dados serão utilizados, ou podem não ser capazes de dar consentimento adequado para certas práticas. Dada a falta de declarações em contrário, é provável que a Internet.org colete dados dos seus usuários quando eles utilizam os aplicativos e serviços que fazem parte do programa, e há uma falta de transparência sobre como os dados são utilizados pela Internet.org e seus parceiros de telecomunicações. A Internet.org também concentra o uso da Internet em um conjunto restrito de aplicativos e serviços, tornando mais fácil para os governos e agentes maliciosos a bisbilhotagem do tráfego dos usuários.

Segurança: A implementação atual da Internet.org ameaça a segurança dos usuários e da Internet como um todo. A atualização de 4 de maio para o programa proíbe o uso de TLS (Transport Layer Security), SSL (Secure Socket Layer), ou criptografia HTTPS pelos serviços participantes. Isto em si coloca os usuários em risco, porque o seu tráfego Web será vulnerável a ataques mal-intencionados e à bisbilhotagem do governo.

Internet em dois níveis: O "boom" econômico que a Internet criou em países desenvolvidos precisa ser compartilhado igualmente com as próximas três bilhões de pessoas, e não estrangulado pela nova Internet de dois níveis da Facebook. O modelo da Internet.org — dando aos usuários uma degustação de conectividade antes de incentivá-los a comprar planos de dados caros — não reconhece a realidade econômica para milhões de pessoas que não podem pagar por esses planos. Estes novos usuários poderiam ficar presos em um caminho separado e desigual para conectividade com a Internet, que servirá para alargar em vez de estreitar a brecha digital.

A Facebook, nas suas intenções declaradas de conectar bilhões à Internet, deveria apoiar e defender

fortemente as salvaguardas dos princípios da neutralidade da rede, privacidade, segurança, e outros direitos dos usuários nas negociações com os governos e os reguladores nacionais, ao mesmo tempo que deveria aplicar estes padrões às suas iniciativas de negócios.

Assinam:

• **18MillionRising.org** - EUA • **Access** - Global • **Ageia Densi Colômbia** - Colômbia • **Baaroo Foundation** - Holanda • **Bits of Freedom** - Holanda • **Center for Media Justice** - EUA • **Centre Africain D'Echange Culturel (CAFEC)** - República Democrática do Congo • **Coding Rights** - Brasil • **Coletivo Intervozes** - Brasil • **Colnodo** - Colômbia • **ColorofChange.org** - EUA • **Community Informatics Network** - Global • **Data Roads Foundation** - Global • **Digital Rights Foundation** - Paquistão • **Digitale Gesellschaft** - Alemanha • **European Digital Rights (EDRi)** - União Européia • **Fight for the Future** - EUA • **Förderverein freie Netzwerke e.V. / freifunk.net** - Alemanha • **Free Press Unlimited** - União Européia • **Fundacion Karisma** - Colômbia • **Fundacion para la Libertad de Prensa** - Colômbia • **Future of Music Coalition** - EUA • **Global Voices Advocacy** - Global • **Greenhost** - Holanda • **i freedom Uganda** - Uganda • **ICT Watch - Indonesia** - Indonésia • **Initiative für Netzfreiheit** - Áustria • **Instituto Bem Estar Brasil** - Brasil • **Instituto Beta para Internet e Democracia - IBIDEM** - Brasil • **Instituto NUPEF** - Brasil • **Integrating Livelihoods through Communication Information Technology for Africa** - Uganda International • **Modern Media Institute** - Islândia • **Internet Policy Observatory Pakistan** - Paquistão • **IPANDETEC** - Panamá • **IT for Change** - Índia • **ITPol Denmark** - Dinamarca • **Just Associates Southern Africa** - África • **KICTANet** - Quênia • **Korean Progressive Network Jinbonet** - Coréia do Sul • **Media Alliance** - EUA • **Media Matters for Democracy (Pakistan)** - Paquistão • **Media Mobilizing Project** - EUA • **MediaNama** - Índia • **Movimento Mega** - Brasil • **Open Wireless Network of Slovenia** - Eslovênia • **OpenMedia** - Global • **Paradigm Initiative Nigeria** - Nigéria • **Popular Resistance** - EUA • **Protege Qv** - Camarões • **Red en Defensa de los Derechos Digitales (R3D)** - México • **RedPaTodos** - Colômbia • **RIght 2 Know Campaign** - África do Sul • **RootsAction.org** - EUA • **Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)** - Canadá • **SavetheInternet.in** - Índia • **Savvy System Designs** - EUA • **Southeast Asia Freedom of Expression Network/Safenet** - Sudeste da Ásia • **TEDIC** - Paraguai • **The Agency League of Musicians** - EUA • **The Heliopolis Institute** - Egito • **The Media Consortium** - EUA • **Unwanted Witness** - Uganda • **Usuarios Digitales** - Equador • **Vrijschrift** - Holanda • **WITNESS** - Global • **xnet** - Espanha • **Zimbabwe Human Rights NGO Forum** - Zimbabue •

O Instituto Nupef é uma organização sem fins de lucro dedicada à reflexão, análise, produção de conhecimento e formação, principalmente centradas em questões relacionadas às Tecnologias da Informação e Comunicação (TICs) e suas relações políticas com os direitos humanos, a democracia, o desenvolvimento sustentável e a justiça social.

Além de realizar cursos, eventos, desenvolver pesquisas e estudos de caso, o Nupef edita a poliTICs, a Rets (Revista do Terceiro Setor) e mantém o projeto Tiwa – provedor de serviços internet voltado exclusivamente para instituições sem fins lucrativos – resultado de um trabalho iniciado há 21 anos, com a criação do Alternex (o primeiro provedor de serviços internet aberto ao público no Brasil). O Tiwa é um provedor comprometido prioritariamente com a privacidade e a segurança dos dados das entidades associadas; com a garantia de sua liberdade de expressão; com o uso de software livre e de plataformas abertas não-proprietárias.

instituto nupef

Rua Sorocaba 219, 501 | parte | Botafogo | CEP 22271-110 | Rio de Janeiro | RJ | Brasil
Telefone/fax +55 (21) 3259-0370 | www.nupef.org.br