Governança da Internet: e agora?

*Por **Louis Pouzin**, um dos "pais" da Internet, criou a primeira rede de computação por datagramas, modelo adotado mais tarde no padrão TCP/IP. É membro do Conselho Consultivo da poliTICs*

Data da publicação:

Maio de 2014

A governança da Internet tem sido o tópico de infindáveis discussões desde que a preparação para a Cúpula Mundial sobre a Sociedade da Informação (CMSI/WSIS) começou em 2001. A maioria dos Estados insiste em pesos iguais nas decisões que afetam não apenas questões técnicas como também políticas públicas, além de impactos econômicos e sociais, nos níveis nacional e internacional. Entretanto, o governo dos EUA ainda não retrocedeu na sua determinação de continuar com as operações de espionagem e vigilância em massa e continua exercendo controle unilateral sobre a Internet por meio de uma empresa californiana, a Internet Corporation for Assigned Names and Numbers (ICANN), criada em 1998 com esse propósito específico[1].

A retórica e a imaginação podem continuar por vários anos, sem qualquer desfecho previsível. Embora ideias e pontos de vista possam ir ganhando flexibilidade e se tornando negociáveis, com o passar do tempo o grupo dominante segue expandindo o seu poder até o ponto de ficar tão entrincheirado que a negociação passa a ser irrelevante. Discutir sem poder tomar nenhuma providência é jogar um jogo perdido. Os cidadãos do mundo inteiro vão ficar parados, esperando serem digitalizados e monetarizados? O objetivo último da cibercolonização.

O QUE É POSSÍVEL FAZER?

A menos que seja do interesse do governo dos EUA, toda e qualquer ação que precise de um aval dele será impedida. Isso é a realpolitik rotineira. Portanto, ações possíveis são aquelas que podem ser implementadas sem a concordância do governo dos EUA - como, por exemplo:

• aplicar leis nacionais/regionais à privacidade de dados pessoais;

• aplicar leis nacionais/regionais aos sonegadores;

• impor penalidades à dominação abusiva do mercado;

• excluir monopólios ilegítimos dos principais contratos;

• equilibrar investimentos/receitas entre operadores, provedores de conteúdo, prestadores de serviços de Internet e mídia;

• proteger plantas naturais contra patentes ilegítimas;

• criar registros de domínios nacionais/regionais independentes da ICANN;

• abrir a competição entre vários serviços de nome de domínio raiz (“DNS roots”);

• usar software de código aberto;

• promover criptografia para e-mails ponta-a-ponta que seja fácil de usar;

• manter registros e normas para identificadores em entidades de normatização (ISO[2]);

• estimular pesquisa/desenvolvimento sobre o futuro da Internet (exemplo: RINA[3]).

...mais?

Alguns leitores podem pensar numa lista de compras. Ao enfrentar uma hiperpotência, um primeiro nível de defesa seria aumentar o custo da espionagem e das operações predatórias. Um segundo nível seria conquistar parcelas de independência de forma a atingir algum potencial de barganha. Num prazo mais longo, o objetivo é aumentar a resistência dos países e prepará-los melhor contra intrusões agressivas.

Muitas das ações que têm sido sugeridas não precisam de mais detalhes, pois são autoexplicativas. Vamos elaborar as que podem não ser.

• proteger plantas naturais contra patentes ilegítimas

Exemplo: uma variedade de pimenta indígena resistente a insetos cresce em algum país menos desenvolvido. Um grupo multinacional de produtos químicos acrescenta ingredientes inúteis às sementes e registra uma patente. Daí em diante, passa a processar os agricultores daquele país por cultivarem, sem licença, a pimenta cuja patente o grupo alega deter.

• criar registros de domínio nacional/regional independentes da ICANN

Os nomes de domínios de topo (TLDs) – como .com, .net, .org – são conhecidos até por quem não usa a Internet. Os TLDs com o código do país – como .cn, .de, .fr, .it, .us – também são bastante conhecidos, enquanto outros – como .bz, .gl, .tp, .vi – são menos conhecidos. Os novos TLDs que estão sendo introduzidos agora – como .bike, .construction, .guru, .photography, .singles – são bastante desconhecidos.

O governo dos EUA impôs a ICANN como monopólio encarregado de designar todos os domínios de topo, inclusive os domínios de topo de país (ccTLDs). Essa decisão unilateral não tem base internacional legítima. Uma boa razão para tal status anticompetição foi dotar a ICANN de uma fonte permanente de renda a partir das anuidades pagas pelos usuários para terem seus domínios.

Como em geral ocorre com os monopólios – e, neste caso, com o apoio do governo dos EUA –, a prioridade máxima da ICANN é ganhar mais dinheiro para sustentar seu estilo opulento e para comprar novos amigos. Essa posição de entidade reguladora dos TLDs e de beneficiária financeira é um caso gritante de conflito de interesses. É premente a necessidade de a ICANN colocar a casa em ordem e submetê-la à competição com os demais atores que cuidam dos interesses dos usuários.

Desde 1996, antes da criação da ICANN, surgiram registros independentes que funcionaram durante alguns anos, e alguns ainda existem, como é o caso de Name.Space, Cesidian Root, OpenNic, Name.Coin etc.[4] Há, de fato, um grande número de registros privados que funcionam a partir de instituições convencionais e continuam, em grande

parte, invisíveis. Seja por uma questão de ignorância, de desinformação, ou do monopólio da ICANN, esses registros independentes encontram-se limitados a nichos de mercado. Já que não há instrumento jurídico internacional protegendo o monopólio da ICANN, o mercado pode descambar para outras direções caso os Estados ou as instituições de grande porte mudem suas políticas ou não as implementem.

• abrir concorrência entre vários DNS-raiz

No campo do nome de domínio, o termo “raiz” (root em inglês) designa um arquivo contendo uma coleção de parâmetros de TLD. Esse arquivo é duplicado nos “servidores de nomes” consultados pelos navegadores ou outros aplicativos na tentativa de conseguir um endereço IP associado a um TLD. Em resumo, é semelhante ao processo de procurar o nome de um assinante num catálogo telefônico. O conceito de raiz é técnico – um repositório de parâmetros de TLDs. O registro (de nomes) é uma organização que gerencia os usuários de domínios e seus identificadores. Um registro pode usar sua própria raiz (OpenNic), ou a raiz de outra organização (o PIR, Public Internet Registry para .org, usa a raiz da ICANN).

A ICANN preconiza a existência de uma única raiz global (ou seja, controlada pelo governo dos EUA). Conforme mencionado mais cedo, existem registros independentes e várias outras raízes muito antes da criação da ICANN, mas nada disso tem cabimento num império monopolista. É curioso observar que o Google e o OpenDNS, que não são registros, usam suas próprias raízes, que são cópias da ICANN.

Uma análise mais profunda de um ambiente com várias raízes vale a elaboração de um outro artigo em separado.

• promover criptografia para e-mails ponta-a-ponta que seja fácil de usar

Após as revelações de Edward Snowden, já não é mais possível tratar da segurança com negligência benigna. Não são todas, mas muitas organizações vão se esforçar um pouco mais para integrar a segurança a seus procedimentos. A indústria do ramo da segurança vai au mentar a pressão comercial em cima disso. A criptografia é o ingrediente básico da segurança das comunicações; ela é usada rotineiramente em ambientes fechados, mas praticamente nunca em ambientes abertos. O e-mail é o serviço dominante para trocas privadas e profissionais. Se a criptografia for malfeita ou for lenta, não será adotada pelo público. Além disso, é necessário que se implemente um conjunto limitado de protocolos padronizados em todos os servidores de e-mail. Desta forma, haveria possibilidade de sucesso para campanhas que incentivem os usuários a adotar medidas de segurança.

• manter registros e normas para identificadores em entidades de normatização (ISO)

Segundo projeções, nos próximos anos o número de objetos na Internet terá uma ordem de grandeza três a cinco vezes maior que o número de seres humanos. Serão necessárias ferramentas para o registro, a recuperação e a troca de identificadores. Parece inadequado e irreal usar ferramentas DNS para o manuseio desse tipo de dados. Um exemplo bom e prático é o GS1 para códigos de barra e o RFID.[5] Funcionam bem porque foram cuidadosamente projetados para atender às necessidades de um comércio específico: a distribuição internacional de bens de consumo de produção em massa que se costumam encontrar nos supermercados. Os automóveis, os produtos químicos, os hospitais, o vinho, por exemplo, teriam outras necessidades, diferentes. Se o mercado de gestão dos identificadores cair nas mãos de um monopólio mundial, esse monopólio vai impor seus próprios padrões proprietários, independentemente das necessidades do ramo, e vai distorcer os processos de manufatura e distribuição com vistas ao seu próprio lucro.

É bom tomar cuidado, estimulando o consenso entre os ramos do mercado para a criação de normas de gestão dos identificadores que estejam ancoradas numa organização internacional de boa reputação, como a ISO.

• estimular pesquisa/desenvolvimento sobre o futuro da Internet (RINA)

Do jeito que está atualmente, a Internet é um sistema experimental cheio de remendos, baseado em conceitos de 40 anos atrás. Escrever nas paredes é “obsoleto”. A pesquisa sobre o futuro da Internet foi reintroduzida nos últimos dez anos, principalmente na forma de projetos separados, sem enfoque numa meta operacional específica. Uma equipe da Universidade de Boston conseguiu lançar uma novidade em termos de projeto de rede: “Padrões de Arquitetura de Rede”, de John Day.[6] O sistema se chama RINA, recursive internetwork architecture. Equipes europeias foram contratadas pelo programa de pesquisa da Comissão Europeia para expandir a plataforma inicial no desenvolvimento de aplicações. Eis uma boa oportunidade para que os designers da nova geração fechem as lacunas de segurança da Internet legada[7].

• acabou-se a confiança

Isso é fato, embora a confiança seja subjetiva. “Quem quer a paz deve estar preparado para a guerra” diz a velha máxima. Não sabemos como o povo norte-americano vai se ajustar à vigilância em massa, que as pessoas levaram décadas achando que só existia em países como a China, a Rússia, a ex-Alemanha Oriental e outros. A logística parece ter chegado a um ponto do qual não dá mais para voltar. É possível que chegue ao poder um regime totalitário mais orwelliano do que nunca. Precisamos convencer os nossos governos e concidadãos a nos afastarmos desse modelo, e dessa tecnologia. Ninguém quer viver numa sociedade assim, não é mesmo?

---
1. N.E.: Este texto foi escrito em fevereiro de 2014, antes do anúncio da intenção da National Telecommunications and Information Administration (NTIA) dos EUA de ceder o controle do arquivo da zona-raiz do DNS a u m organismo pluralista a partir de 2015, a ser definido.

2. Sobre a Organização Internacional para Padronização (ISO), ver http://pt.wikipedia.org/wiki/Organiza%C3%A7%C3%A3o_Internacional_para_Pa...

3. Iniciais de Recursive InterNetwork Architecture. Ver http://csr.bu.edu/rina/about.html

4. Name.Space: http://name.space.xs2.net. Cesidian Root: http://cesidianroot.net. Open NIC: http://www.opennicproject.org. Name.Coin: https://www.namecoin.org. Para mais informações sobre DNS alternativos, ver http://en.wikipedia.org/wiki/Alternative_DNS_root

5. Sobre GS1: http://www.gs1.org. Sobre RIFD: http://pt.wikipedia.org/wiki/Identifica%C3%A7%C3%A3o_por_radiofrequ%C3%A...

6. Ver http://rina.tssg

7. N.T.: Legacy Internet, no original em inglês – termo utilizado para descrever a internet global em funcionamento com base no protocolo Ipv4, sistema em uso desde a década de 80.

Categoria:

- poliTICs 17