

poli**TIC**S

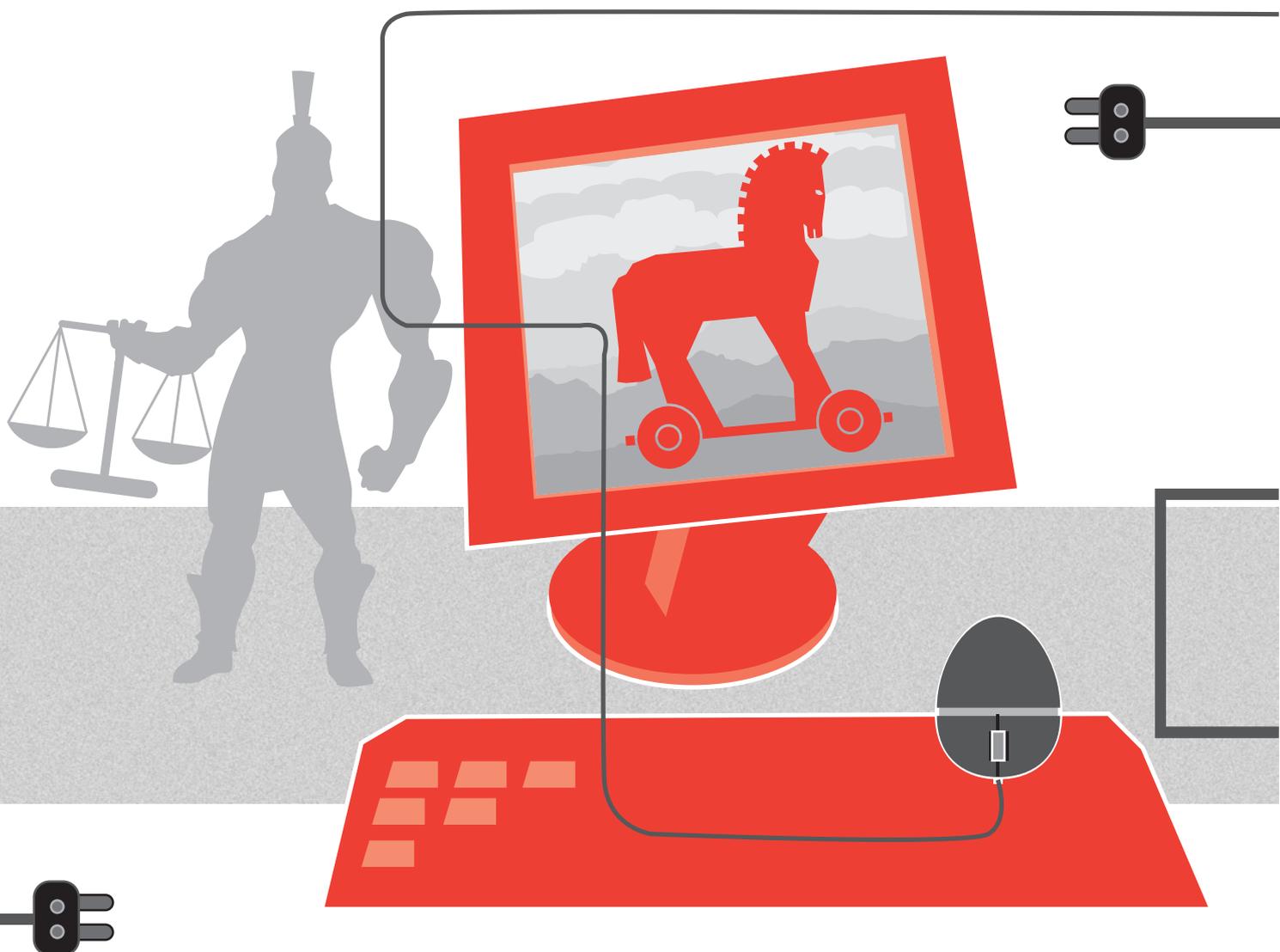
Uma publicação do Instituto Nupef • agosto / 2011 • www.politics.org.br

Lei Azeredo: o Cavalo de Troia legislativo



> **Sergio Amadeu da Silveira** Professor da UFABC, conselheiro do Comitê Gestor da Internet no Brasil, eleito como um dos representantes do Terceiro Setor.

A internet e o novo cavalo de Troia



:: PRESSUPOSTOS...

Deleuze anunciou que vivemos em uma sociedade de controle. As estruturas de confinamento típicas de um mundo disciplinar estariam sendo suplantadas por mecanismos distribuídos de acompanhamento e modulação dos comportamentos. O capitalismo industrial exigiu e se beneficiou com a formação das instituições disciplinares. O capitalismo informacional não consegue se ampliar simplesmente com a introjeção do medo que a permanente vigilância acarreta. O capitalismo baseado nas tecnologias da comunicação e informação precisa de um outro tipo de liberdade vigiada, busca uma liberdade modulada. A nova fase da biopolítica não passa apenas pela garantia da disciplina dos corpos, da saúde posicionada para o trabalho adequado à reprodução do capital, agora ela precisa incentivar a ultraindividualização, necessita que os indivíduos sejam acompanhados e parametrizados em suas variações de humor, de perspectiva e de objetivos.

A internet é a maior expressão deste período histórico. Trata-se de uma rede sociotécnica que dá aos indivíduos a sensação de completa liberdade de uso, de possibilidades de criação, de múltipla existência no ciberespaço, de navegação anônima, de impossibilidade de observação e acompanhamento dos corpos virtualizados. O indivíduo tem medo da câmara alocada no alto da via pública, mas acredita piamente que o acesso a um determinado site não pode ser acompanhado.

Desse modo, é ignorada a origem cibernética da rede mundial de computadores. A internet é uma rede de comunicação e controle. Completamente baseada em protocolos, ou seja, regras rígidas que permitem que uma rede se comunique com a outra, que um computador possa encontrar o outro em uma malha de milhões de pontos de conexão. Seria praticamente impossível rastrear e encontrar uma pessoa com um pequeno rádio de pilha analógico, ouvindo uma transmissão qualquer. Mas é muito provável e factível que possamos localizar um jovem conectado a partir de seu pequeno netbook ou dispositivo móvel com precisão georeferenciada crescente. A interatividade só pode ser garantida se os interagentes forem visíveis um para o outro, não importa onde estejam nos pontos de conexão distribuídos da internet.

Para burlar os mecanismos de controle técnico é preciso estar consciente da existência deles e estar preparado para utilizá-los de outro modo. O indivíduo pode evitar que seu fluxo de informação seja rastreado utilizando um proxy anônimo ou uma rede de proxies anônimos – capaz de ocultar a informação de identificação do computador de origem. Todavia, sem técnicas de ocultamento, praticamente todas as conexões podem ser monitoradas por agentes do Estado, por crackers, por coporações de análise de comportamento, de acompanhamento de redes sociais e de marketing. Entretanto, apesar de ser uma rede de controle técnico, sua arquitetura

distribuída e o desenho de seus protocolos asseguram uma grande liberdade de comunicação. Os protocolos da internet não são construções neutras. Em sua maioria, foram escritos para garantir a liberdade de expressão e de navegação sem a necessidade de identificação pessoal. Foram formulados sob ideias liberais, libertárias, estiveram sob forte influência dos valores disseminados pela contracultura norte-americana dos anos 1960.

:: OS ÚLTIMOS ACONTECIMENTOS INTERNACIONAIS ...

O caso Wikileaks e a aprovação da Lei Sarkozy na França são dois marcos importantes no cenário atual de embates em torno da comunicação em rede. Eles permitem perceber a unidade de ação de agrupamentos nascidos no mundo industrial e que perderam força no mundo das redes: os burocratas dos aparatos de segurança de Estados nacionais, principalmente dos países hegemônicos na OTAN, interessados no policiamento do mundo, de um lado, e a indústria de copyright, de outro. Tais articulações têm em comum a tentativa de retirar da internet as qualidades que a fizeram mais democrática do que as demais mídias de massa. A cultura da liberdade que caracteriza a rede mundial incomoda esses segmentos e os lança em uma jornada de combate à atual dinâmica da internet.

A indústria de copyright perdeu, com o advento da internet, o controle dos canais escassos de disseminação de conteúdos artísticos e de bens culturais que caracterizaram as mídias industriais. Mais do que isto, a digitalização intensiva dos bens simbólicos deixou claro que textos, sons e imagens podem existir e coexistir distantes de suportes físico-localizados, bem como, podem ser recombinaados sem grandes dificuldades. Milhões de pessoas passaram a usar as facilidades das redes digitais e levaram até elas as práticas de compartilhamento que já realizavam no mundo pré-internet, agora sem as barreiras impostas pelos limites e dificuldades criadas pela logística dos suportes. O crescimento da rede representou mais do que o aumento do compartilhamento de arquivos digitais – implicou na ampliação da diversidade cultural. Indivíduos puderam acessar os sites de inúmeros criadores sem a necessidade de intermediação. Isto reduziu a audiência per capita de cada artista ou grupo cultural, mas aumentou a diversificação da fama. As associações de copyright reagiram com agressividade extrema e nisso se encontram com os segmentos retrógrados da burocracia vigilantista dos Estados nacionais.

A tentativa do governo dos Estados Unidos de sufocar o Wikileaks e retirar o seu site da rede, bem como bloquear suas contas para o recebimento de doações financeiras, redundou em um grande

fracasso. Milhares de apoiadores do Wikileaks, dispersos em todos os continentes, replicaram em seus servidores as informações que o Departamento de Estado norte-americano tanto queria evitar que fossem divulgadas. Isto confirmou o que Alexander Bard e Jan Söderqvist afirmaram ser uma característica das redes distribuídas: o fato que “todo ator individual decide sobre si mesmo, mas carece da capacidade e da oportunidade para decidir sobre qualquer dos demais atores” (UGARTE, 2008, 26). Além disso, a abusiva e obscura tentativa de calar o líder do Wikileaks, Julian Assange, levou o grupo hacktivista Anonymous a organizar uma grande ação de protesto que derrubou da rede os sites da Visa, Mastercard e PayPal. Angariando pelo IRC e pelo Twitter milhares de apoiadores, o Anonymous mostrou que um grande número de requisições de acesso a uma determinada aplicação de um site pode ser uma legítima forma de protesto.

Unindo os pensamentos retrógrados do planeta, as vozes da velha comunidade de segurança espalharam seus temores sobre a denominada “excessiva liberdade na rede”, guarida para terroristas. Tais vozes são logo amplificadas pelos detentores das velhas mídias, também incomodados com a grande liberdade de ação na rede. Uma matéria da Revista Época deixa claro o

incômodo: “apesar do evidente teor adolescente nas manifestações, eles trazem um ingrediente novo para o universo hacker – a motivação política. Sua prioridade é desestabilizar forças políticas, econômicas ou militares, numa lógica em tudo similar à do terrorismo. No lugar de atentados suicidas e ameaças a bomba, o foco dos hackers é a informação. Eles afirmam que as organizações e os Estados, ainda que estabelecidos de forma democrática, devem sofrer ataques em prol de um bem maior, a transparência.”¹

Propor a violação da privacidade e submeter os indivíduos a constante vigilância de robôs e “aranhas”² que rastreiam a rede em busca de palavras-chave, fluxos de informações suspeitas, tipos de aplicação, passam a ser alardeadas como práticas necessárias no combate aos terroristas, incluindo nesta categoria os ativistas que lutam pela liberdade de expressão na rede. Como um dos grandes marcos desta prática de destruição dos direitos civis na internet e de subordinação de todos os demais direitos às necessidades da análise de espectro e dos fluxos de informação, temos a Lei Hadopi. Essa lei implantou na França um certo “estado de sítio digital”. Para saber se as pessoas estão fazendo download ou compartilhando arquivos digitais cerceados pelo copyright, o presidente Sarkozy aprovou uma lei que obriga os provedores a observar o que seus clientes estão fazendo na rede.

1. Revista Época - 27/06/2011 - A guerra virtual começou / Autor(es): Bruno Ferrari, Daniella Cornachione e Leandro Loyola. 2. Aranhas são programas que fazem buscas na internet de maneira metódica, automatizada e sistemática. Ver em https://secure.wikimedia.org/wikipedia/en/wiki/Web_crawler

Nesse caso concreto, o que está em jogo não é a busca de indícios de terrorismo, mas as provas de violação de copyright.

A lei de Sarkozy é também conhecida como *three strikes*. Se o internauta for pego pela Comissão Hadopi baixando música sem pagamento de licenças, receberá um e-mail alertando que sua atividade ilegal foi detectada (primeira batida). Se continuar, receberá uma carta (segunda batida). Por fim, será desconectado da internet por um ano (terceira batida). Nos primeiros nove meses de aplicação da Hadopi foram monitorados 18 milhões de usuários que trocaram arquivos. A partir desta quantidade de usuários, a empresa selecionada Trident Media Guarda rastreou um milhão de endereços IP e enviou mais de um milhão de solicitações para os provedores de acesso, que entregaram informações sobre a atividade de aproximadamente 900.000 usuários. Destes, 470 mil internautas receberam o primeiro aviso da Comissão Hadopi. O segundo aviso foi enviado para 20 mil pessoas e 10 franceses já foram desconectados com o terceiro aviso. A ironia é que o primeiro desconectado é um professor de 54 anos que nunca baixou música pela internet e provavelmente teve sua máquina usada por invasores. Além de economicamente dispendiosa, a Lei Sarkozy é invasiva e ineficaz, uma vez que apenas 4% dos franceses pesquisados pela ZDNet afirmaram deixar de fazer download devido à lei.³

:: O BRASIL E O CAVALO DE TROIA LEGISLATIVO

No Brasil, no final de junho de 2011, a confluência de interesses dos setores de segurança ligados aos bancos com segmentos conservadores da burocracia estatal e com os representantes da indústria do copyright trabalharam para criar um clima de terror que justificasse a aprovação do chamado AI-5 Digital, uma proposta de lei de crimes na internet organizada pelo ex-Senador Eduardo Azeredo, do PSDB de Minas Gerais. A partir de ataques de baixo impacto a sites do governo, promovido por um grupo de crackers⁴ que se autodenominavam "luzlsec brasil", articulou-se uma onda de reportagens iniciada pela Revista Época, empresa da Rede Globo, que buscava superdimensioná-los a ponto de justificar a urgente aprovação da lei de crimes na rede, sem a qual o país estaria indefeso. A artificialidade do clima era tamanha que a Folha de São Paulo resolveu divulgar que a conta de e-mail da então candidata a presidente da República, Dilma Rousseff, tinha sido invadida em 2010. Estranha divulgação, um ano depois, em 2011. Também chama a atenção que o provedor de acesso que teria sido supostamente invadido, o UOL, é da mesma empresa que controla a Folha de São Paulo. Como um verdadeiro estouro da boiada, os veículos de comunicação da velha mídia iniciaram reportagens sobre hackers (como se todos fossem crackers) e crimes na internet.

3. Informações disponíveis no site <http://torrentfreak.com/france-tracks-down-18-million-file-sharers-110714/>. Acesso 10/08/2011. 4. Cracker é o termo usado para designar quem pratica a quebra (ou cracking) de um sistema de segurança, de forma ilegal ou sem ética.

Apesar da onda, um conjunto de deputados ligados à defesa da liberdade na rede conseguiu barrar a tentativa de votação *in limine* do projeto de Azeredo. O ministro da Ciência e Tecnologia, Aloizio Mercadante, sensibilizado com o risco da lei paralisar um importante segmento que desenvolve tecnologia no país, foi até o Fórum Internacional de Software Livre, em Porto Alegre, reunir-se com as comunidades hackers de desenvolvedores de código aberto. Na contramão da onda sensacionalista da imprensa, o ministro Mercadante afirmou estar interessado em organizar um Transparência HackDay em seu ministério. O movimento de dados abertos dos governos tem sido defendido e apoiado no Brasil pelos hackers que estão ajudando diversos gestores públicos a dispor dados em formato

acessível pelas máquinas dos cidadãos, o que tem aumentado o *accountability* e a transparência.

Há três anos, o mesmo Azeredo tentou aprovar o seu projeto de criminalização de práticas na rede afirmando ser ele imprescindível para se combater a pedofilia. Todavia, ficou claro que isto não era precedente e que o combate à pedofilia (que já era crime no nosso código penal) exigia muito mais grupos especializados de atuação policial do que um novo aparato legal. O projeto Azeredo tem uma agenda oculta que está principalmente consolidada nos artigos 285-A, 285-B e 22. Os dois primeiros artigos visam criminalizar o acesso não autorizado a um sistema informatizado sem a concordância do seu legítimo titular, bem como, pretende agravar a pena daqueles que transferem arquivos obtidos

■ Para burlar os mecanismos de controle técnico é preciso estar consciente da existência deles e estar preparado para utilizá-los de outro modo.

com tal violação. Aparentemente, os artigos visam os crackers, mas no fundo pretendem transformar qualquer pessoa que quebre um dispositivo DRM⁵, que retire, por exemplo, uma música de um CD, cuja licença proíba expressamente que ela seja levada a qualquer outro sistema informatizado, e a insira em seu próprio computador. A lei Azeredo é um “Cavalo de Troia” legislativo. Traz dentro de sua redação inúmeras possibilidades de interpretação – inclusive por isso teve sua aprovação recomendada pela Aliança Internacional de Propriedade Intelectual, no seu relatório de 2010.

O artigo 22 do PL é completamente obscuro. Pretende tratar da guarda de logs de acesso às redes. Ao invés de definir claramente que quem deve guardar os registros de acesso são apenas os administradores de sistemas autônomos (aproximadamente algo em torno de 1100 no país), afirma que todos os provedores públicos e comerciais devem fazê-lo por três anos, ou seja, estão incluídos aí desde o IG, Terra, UOL até uma empresa, telecentro ou universidade que forneça conexão aos seus alunos. Vários complementos indispensáveis à aplicação do artigo 22 são jogados para uma regulamentação posterior, através da qual Azeredo pretende construir no Executivo, entre outros pontos de sua agenda oculta, a necessidade de se vincular a identidade civil dos internautas à navegação na rede. Trata-se de mais uma aplicação do método “Cavalo de Troia”. Todavia, seu discurso

conservador já deixa claro que a aprovação da guarda de logs é apenas a primeira ação no sentido de implantação da navegação vigiada – por isso escreveu em seu último relatório, agora como deputado na Comissão de Ciência e Tecnologia:

“Ressalte-se, ainda, que a Constituição Federal, em seu art. 5º, inciso IV, veda o anonimato, vinculando tal vedação à liberdade de pensamento e manifestação. Trata-se de um dos princípios fundamentais da nossa sociedade, cujo respeito aos valores é necessário ao pleno equilíbrio dos direitos e deveres de todos os cidadãos. Conclui-se, portanto, que, ao direito de conectar-se a um sistema deve-se contrapor o dever social de identificação, sob pena de que o anonimato venha a permitir àqueles de má-fé praticarem diversas modalidades de crimes e infrações.”

Azeredo é porta-voz dos banqueiros que querem inverter o ônus da prova e socializar o prejuízo dos ataques de crackers às instituições financeiras. Também é porta-voz da indústria do copyright, que tal como na França de Sarkozy quer que a navegação seja identificada para que se possa ameaçar aqueles que compartilham arquivos digitais, principalmente em redes P2P.

O Brasil, no ano de 2010, assumiu uma postura de destaque no processo de regulação social da internet. O Ministério da Justiça, de modo pioneiro, usando a plataforma da rede de cultura

5. Sigla para Digital Rights Management

digital do Ministério da Cultura, lançou uma proposta de projeto de lei para regulamentar civilmente a internet no Brasil. Antes de enviar a proposta para o Congresso, o Ministério da Justiça decidiu construí-la com a colaboração da sociedade. Em duas rodadas de consultas o pré-projeto de Marco Civil recebeu mais de duas mil contribuições de todos os setores da sociedade. A última versão definia claramente quais os direitos que os cidadãos deveriam ter na comunicação em redes digitais. É uma proposta de lei para regulamentar a liberdade na rede. Uma contraposição avançada e claramente contrária à proposta de Azeredo ou de Sarkozy. O Marco Civil brasileiro pode ser um exemplo para o mundo e um anteparo ao obscurantismo que assola países como a França e a Espanha.

O que aconteceu com o Marco Civil? Até a primeira semana de agosto de 2011 não havia sido enviado para o Congresso Nacional. Como o processo colaborativo que gerou sua redação terminou em meio às eleições para a sucessão presidencial, o governo Lula resolveu deixar para a gestão seguinte o envio do Marco Civil para o Congresso. Entretanto, a Casa Civil do Ministro Palocci e os novos ministros não conseguiram ou não quiseram enviar a proposta para o Legislativo. O não envio do Marco Civil é que permitiu o fortalecimento do projeto de lei do ex-senador Azeredo. Os próximos lances serão derradeiros. Estão em jogo as possibilidades de reagir contra a onda vigilante que quer

transformar as possibilidades de controle técnico da rede em controle cultural, tecnológico e político. O Brasil pode ser o país da virada na construção de uma opinião pública transnacional favorável à manutenção da cultura da liberdade na rede, derrotando assim a implantação de uma cultura da permissão.

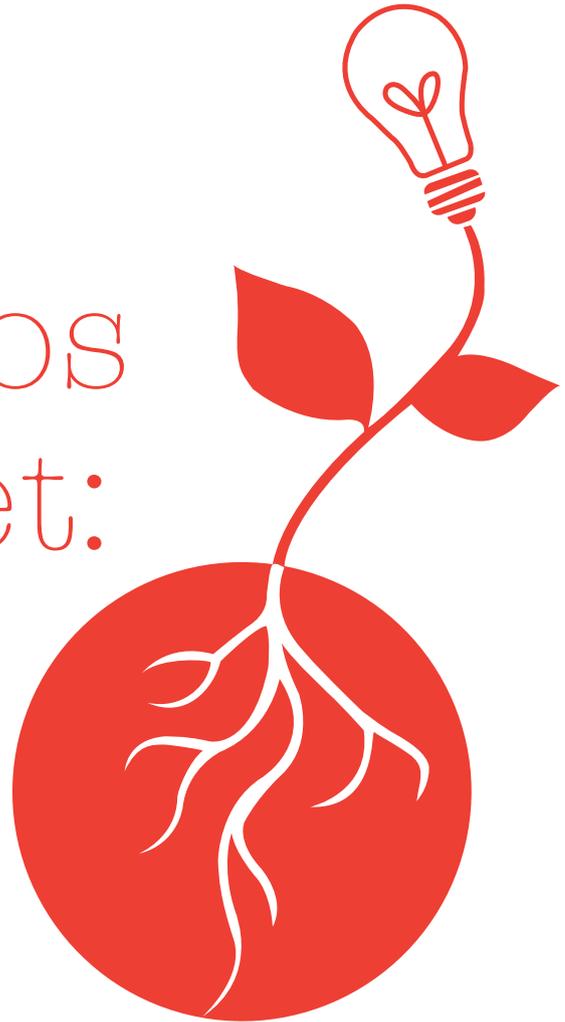
- * Nota dos editores: O Marco Civil da internet foi enviado ao Congresso no dia 24 de agosto, durante o processo de edição deste número da poliTICs. ●

//REFERÊNCIAS: BIBLIOGRÁFICAS

- ARQUILLA, John; RONFELDT, David (ed.). **In Athena's Camp: preparing for conflict in the Information Age.** Washington, D.C.: RAND, 1997.
- BENKLER, Yochai. **The wealth of networks: how social production transforms markets and freedom.** New Haven: Yale University, 2006.
- CASTELLS, Manuel. **Comunicación y poder.** Madrid: Alianza Editorial, 2009.
- DELEUZE, Gilles. **Conversações.** São Paulo: Editora 34, 1992.
- GALLOWAY, A. **Protocol : how control exists after decentralization.** Cambridge, MA.: MIT, 2004.
- STALLMAN, R. **The Anonymous WikiLeaks protests are a mass demo against control.** The Guardian, Friday 17 December 2010. Disponível: <http://www.guardian.co.uk/commentisfree/2010/dec/17/anonymous-wikileaks-protest-amazon-mastercard> Acesso:15/02/2011.
- UGARTE, David. **O poder das redes.** Porto Alegre : PUC-RS, 2008.

> **Avri Doria** Pesquisadora da Luleå University of Technology e presidente do Comitê Executivo do NCUC (Non-Commercial Users Constituency), na ICANN.

Nomeação de domínios na internet: O DNS, Raízes Alternativas e o Futuro



:: A POSSIBILIDADE DE RAÍZES ALTERNATIVAS ¹

Raízes alternativas, também chamadas de 'alt roots', são um tópico frequentemente pronunciado em voz baixa. São tanto uma ameaça quanto uma promessa. Envolver-se com raízes alternativas é o suficiente para ser afastado da Força-Tarefa de Engenharia da internet (IETF, sigla em inglês) ou da Corporação da internet para Atribuição de Nomes e Números

(ICANN, sigla em inglês) e também o suficiente para tornar-se um herói em alguns círculos.

Quinze anos atrás, antes da criação da ICANN, havia muitas propostas sobre novas raízes. O medo destas novas propostas foi suficiente para fazer muitos governos despertarem para a importância do Sistema de Nomes de Domínios (DNS, sigla em inglês). Há cerca de cinco anos, fui ao Conselho

¹. O artigo refere-se às propostas de criação de sistemas de nomes de domínio alternativos. Para uma excelente introdução ao assunto, ver http://pt.wikipedia.org/wiki/Servidor_Raiz

de Arquitetura da internet (IAB, sigla em inglês) e recomendei que a IETF começasse a trabalhar em uma resposta técnica para o problema de raízes alternativas, já que esperava que raízes alternativas emergissem em vários países. Fui informada que com certeza a IETF não poderia fazê-lo, pois isso significaria dar permissão para aqueles que quisessem dividir a raiz. Também fui lembrada que a IAB já havia falado sobre esta questão na recomendação RFC2826 e havia desencorajado qualquer esforço nesta direção.

Há cerca de três anos, insisti que os nomes de domínio internacionalizados (IDNs) de ccTLDs e de gTLDs, grafados em caracteres e idiomas locais, deveriam ser inseridos na raiz ao mesmo tempo para que governos não obtivessem uma vantagem comercial sobre a indústria de nomes de domínio em seus países. Depois que as pessoas superaram o choque após eu ter falado algo a favor de interesses comerciais, eu fui chamada em particular e informada que a ICANN tinha que apressar-se e lançar ccTLDs internacionalizados porque os russos, e talvez até os chineses, poderiam separar-se e criar suas próprias raízes se a ICANN não fizesse o que eles queriam imediatamente e não desse a eles seus ccTLDs em seus caracteres e idiomas nacionais.

Há dois anos, eu era parte de um grupo de autores da Força-Tarefa de Pesquisa da internet (IRTF, sigla

em inglês), Grupos de Pesquisa de Redes Tolerantes a Atrasos (DTNRG, sigla em inglês), que sugeri que um Identificador Uniforme de Recursos (URI) do tipo DTN (ou seja, seguindo os padrões para uma rede tolerante a atraso²) poderia ser utilizado para definir nomes sob uma autoridade que não a ICANN para endereços em uma rede. Redigimos um rascunho para a internet utilizando o componente de Autoridade do URI³ para elaborar um esquema de definição de nomes fora do espaço da ICANN⁴ com o uso de padrões DTN. Este trabalho está pendente mas está sendo utilizado experimentalmente.

Há cerca de um ano atrás, organizadores da Pirate Bay iniciaram uma tentativa de criação de um novo “sistema de DNS aberto, descentralizado e grátis!”⁵ utilizando tecnologia ponto a ponto (P2P, sigla em inglês). Esta é uma das mais recentes tentativas para a criação de novos sistemas DNS ou raízes alternativas que têm sido propostos nos últimos dez anos. Acho que tornou-se dormente ou desapareceu após uma quantidade razoável de atenção da mídia.

Há cerca de seis meses, durante um debate sobre o gTLD .xxx na ICANN, um dos distinguidos sábios da internet argumentou que seria importante evitar a aprovação de nomes que países pudessem filtrar, porque isto poderia levar à divisão da raiz, algo que deveria ser evitado a todo custo. A divisão em múltiplas raízes seria o que defensores da raiz unitária chamam de raízes alternativas.

2. Rede tolerante a atraso (DTN) é uma arquitetura de rede de computadores que procura contornar os problemas de conectividade em redes heterogêneas entre as quais pode ocorrer conectividade intermitente. Exemplos de tais redes são as redes móveis, ou de ambientes extremos (guerras, resgates, acidentes, etc), ou redes planejadas no espaço. Para mais informação, ver http://pt.wikipedia.org/wiki/Delay-tolerant_networking 3. Ver <http://www.ietf.org/rfc/rfc2396.txt> 4. Ver <http://tools.ietf.org/id/draft-irtf-dtnrg-dtn-uri-scheme-00.txt> 5. Ver http://dot-p2p.org/index.php?title=Main_Page

■ O que mantém a internet coesa como um sistema único é um conjunto de protocolos que operam na rede, permitindo que diversas redes se comuniquem. O que também a mantém coesa é um esquema de endereçamento comum, definido pelo Protocolo de Internet (IP).

Outros argumentam que aqueles rejeitados pela ICANN para novos gTLDs, após gastarem centenas de milhares de dólares em processos e tudo aquilo que se vincula a eles, podem ser seduzidos a se juntarem a raízes alternativas se estas puderem demonstrar que podem ser utilizadas de maneira confiável e lucrativa. Em julho deste ano, em uma de minhas aulas na Summer School on Internet Governance (SSIG, Escola de Verão Sobre Governança na Internet)⁶ mencionei que acreditava que eventualmente existiriam raízes alternativas ou até novos sistemas de nomeação na internet.

Após a aula um aluno chegou até mim para verificar se eu estava sugerindo a destruição do DNS e portanto o fim da internet, pois o que eu disse havia soado assim para ele. Eu assegurei a ele que, ao contrário de estar advogando a destruição do DNS e da internet, eu estava defendendo a sobrevivência da internet e acreditava que o DNS unitário da ICANN era não somente desnecessário, mas também um monopólio cuja duração como tal estaria limitada.

:: FRAGMENTAÇÃO DA INTERNET

O argumento mais frequente contra a ideia de raízes alternativas ou sistemas de nomeação alternativos é que isto irá fragmentar a internet. Acho que este argumento é falso, mas devem ser tomadas precauções ao criar sistemas alternativos de nomes para evitar problemas para a internet. Todavia, isto sempre será uma preocupação quando algo novo for criado na internet: deve-se sempre aderir a princípios de projeto que assegurem que a internet continue a ser o sucesso que é em qualquer escala.

O que mantém a internet coesa como um sistema único é um conjunto de protocolos que operam na rede, permitindo que diversas redes se comuniquem. O que também a mantém coesa é um esquema de endereçamento comum, definido pelo Protocolo de Internet (IP). Se a criação de um novo esquema de endereçamento comum, o IPv6⁷,

6. Ver <http://www.euro-ssig.eu/>

não fragmentou a internet, é difícil pensar que um novo sistema de nomeação o faria. Dizer que uma raiz alternativa pode matar a internet é tão razoável quanto dizer que a produção de uma nova agenda telefônica irá destruir a rede telefônica. Claro, se alguém criar uma nova agenda telefônica sem cautela isso pode confundir as coisas, mas quem iria utilizar uma agenda telefônica incorreta? Da mesma forma, se uma raiz alternativa não fornecesse informação correta ou tornasse impossível alcançar/entrar em contato com sistemas que poderiam ser alcançados de outra forma, quem iria utilizá-la? Todos que pensam sobre raízes alternativas entendem que qualquer coisa que for criada tem que funcionar sem tornar a internet menos estável.

:: O QUE FAZ O SISTEMA DE NOMES DE DOMÍNIOS (DNS)?

Dando um passo atrás, é importante lembrar o que o DNS faz. Sua função primária é criar um conjunto de nomes fáceis para fazer referências aos endereços de IP que se referem a várias máquinas e serviços na internet. Como discutido acima, DNSs são semelhantes a uma agenda telefônica automatizada, na medida em que quando uma pessoa busca um nome ela encontra um endereço de IP. Não há nada mágico sobre o DNS, é um conjunto de perguntas e respostas sequenciais,

para traduzir um nome a partir de uma forma que seja compreensível para o entendimento humano, para outra forma: os pseudo-números utilizados em endereços de IP como um meio de identificar sistemas e seu local na rede. O fato de que temos os nomes é importante, não apenas por serem de fácil uso para quem navega na internet, mas para fornecer um meio através do qual o mesmo nome possa direcionar a um novo endereço quando alguém move um recurso no sistema para um local diferente na rede. Então precisamos de nomes e precisamos que os nomes sejam referências confiáveis. Mas por que isso teria que significar que precisamos somente de uma autoridade que atribua estes nomes?

:: OPINIÃO DO IAB SOBRE RAÍZES ALTERNATIVAS

Como mencionado acima, o IAB discutiu a questão através do documento RFC2826⁸ e recomendou fortemente que raízes alternativas nunca fossem estabelecidas. O sumário da RFC diz:

“Para que permaneça uma rede global, a internet requer a existência de um espaço de nome público único. O espaço de nomes é um espaço hierárquico derivado de uma raiz única global. Existe um limite técnico inerente ao projeto do DNS. Portanto não é tecnicamente factível existir mais de uma raiz no DNS público.

7. Sobre o IPv6 e a exaustão do IPv4, ver <http://pt.wikipedia.org/wiki/IPv6> 8. Ver <http://tools.ietf.org/html/rfc2826>

Esta única raiz tem de ser apoiada por um conjunto de servidores raiz coordenados administrados por uma autoridade de nomeação única.

“Em outras palavras, lançar múltiplas raízes públicas de DNS irá levantar uma possibilidade fortíssima de que usuários de diferentes ISPs (provedores de internet, sigla em inglês) que clicarem no mesmo enlace de uma página Web possam terminar em diferentes destinos, contra a vontade dos criadores dessas páginas.

“Isto não impede redes privadas de operar seus próprios espaços de nome privados, mas se estas desejarem utilizar nomes unicamente definidos para a internet, elas terão que buscar esta informação na hierarquia de nomeação do DNS global, e em particular dos servidores raiz coordenados da hierarquia de nomeação do DNS global.”

Nunca pensei que estes dois primeiros parágrafos fossem muito convincentes. Quando o protocolo de DNS estava sendo introduzido pela primeira vez nos anos 1980, eu não fui capaz de entender por que em uma internet cuja essência era sua natureza distributiva, o DNS deveria ser o único lugar que requereria um ponto único de controle. Mas eu era apenas uma engenheira de rede junior na época e certamente não tinha a solução. Ainda hoje eu acredito que deveria ser possível criar um sistema compatível com a raiz única DNS, mas que acomode outras raízes. E não estou sozinha nesta crença.

:: O QUE SERIA NECESSÁRIO PARA CRIAR UMA RAIZ ALTERNATIVA?

Dizer que uma coisa é tecnicamente possível é relativamente fácil. Fornecer os requerimentos para tal tecnologia é mais difícil. Construir de fato um novo sistema que cumpra estes pré-requisitos para tal tecnologia é mais complicado. Alguns dos requisitos básicos para qualquer sistema de raiz alternativa podem incluir:

- Não se sobrepor a nenhum outro sistema de domínio. Isto pode ser conseguido listando-se explicitamente a autoridade para um nome como parte do nome (infelizmente esta função, a etiqueta Class, está quebrada na arquitetura atual de DNS), ou por coordenação rigorosa entre as várias raízes para não utilizar um nome já utilizado por outra raiz.
- Compatibilidade retroativa, para que o sistema existente continue a funcionar. Isto pode ser uma extensão do tópico anterior referente a espaços de nomes que não se sobrepõem. Isto pode ser alcançado através da inclusão de outras raízes, especialmente a raiz da ICANN, ou referências a outras raízes na raiz alternativa.
- Segurança.
- Privacidade.
- Escalabilidade.

Sei que várias pessoas já desenvolveram raízes alternativas e conheço ao menos uma que está trabalhando em outra raiz alternativa.

:: POR QUE NÃO TEMOS RAÍZES ALTERNATIVAS

Na verdade devem existir dúzias de raízes alternativas que surgiram nos últimos anos. Algumas ainda existem, mas muitas estão inoperantes. No entanto, nenhuma destas alcançou algum grau de aceitação na internet. A questão é o porquê disto. A maioria das especulações afirma que nenhuma destas raízes ofereceram algo que os usuários não estavam obtendo de uma raiz única da ICANN. Com nenhuma motivação para mudar, por que mudar?

Além disso, como na maioria de situações de monopólio, a ICANN tem notoriedade e fez um excelente trabalho em relação à sua defesa de uma raiz única. Quase todos que perguntam sobre uma raiz alternativa repetem os chavões sobre como isto pode significar o fim da internet. Mas qualquer um que tenha observado os argumentos a favor de uma raiz única, que não sejam aqueles comprometidos com a religião de uma raiz única, já percebeu que nenhum dos argumentos para uma única raiz é necessário. Se o processo for feito corretamente, a internet iria não somente sobreviver às raízes alternativas e sistemas de nomeação, mas poderia até se beneficiar destas inovações.

:: ALÉM DO DNS EM DIREÇÃO A OUTRAS ARQUITETURAS DE NOMEAÇÃO

Uma possível razão para não estender o atual sistema DNS para apoiar a raízes alternativas é a

fragilidade do atual DNS. Com a adição do suporte a registro do IPv6, do DNS seguro (DNSSEC⁹), de nomes de domínio em línguas e caracteres outros que não do inglês (os nomes de domínio internacionalizados) e agora com a adição de um número indeterminado de novos nomes (os novos gTLDs) que podem ser filtrados, alguns especialistas estão indecisos em relação a quantas mudanças mais o DNS pode suportar. Esta pode ser a debilidade real do DNS: não é que as raízes alternativas serão confusas, é que elas podem agregar mais tensão sobre um sistema antigo e frágil.

Por esta, entre outras razões, existem várias tentativas de criar outros sistemas de nomeação para operar paralelamente ao DNS e talvez até eventualmente substituir o atual. Uma destas tentativas é o Serviço de Nomeação de Objeto (ONS¹⁰) que vem sendo implementado como um modelo centralizado em níveis no existente DNS e como um sistema par-a-par (P2P, do inglês peer-to-peer) utilizando tabelas de dispersão. No ONS haverá várias raízes pares em vez de uma única raiz. O ONS está utilizando esta abordagem porque busca um modo de fazer a nomeação na chamada "internet das Coisas", que existe em uma multidão de redes – algumas que são parte da internet e algumas que não são parte da internet tal como entendida hoje. O ONS permite que a rede cresça para além da

9. Ver <http://pt.wikipedia.org/wiki/DNSSEC> 10. Ver <http://www.epcglobalinc.org/standards/ons>

internet como a conhecemos para tornar-se uma rede sintética ainda maior, uma internet maior.

O ONS é apenas um dos modelos desenvolvendo um sistema de nomeação baseado em P2P. Outro é a estrutura GUNet¹¹ para assegurar conexões entre pares. Muitas pessoas estão olhando para o modelo de rede P2P e desenvolvendo possíveis novos sistemas de nomeação da internet.

:: ENTÃO, O QUE FAZER DEPOIS DISSO

Haverá raízes alternativas? Sim, elas existem desde o início e não há razão para pensar que irão desaparecer.

Surgirão raízes alternativas que podem se tornar mais do que um hobby para desenvolvedores? Isto ainda não é certo. Não somente existe a necessidade de haver uma razão para que usuários queiram utilizá-las, e uma forma automática para estes usuários modificarem os sistemas para acessar estas raízes alternativas; haverá também a necessidade de estes sistemas mostrarem que não somente são compatíveis com o sistema da ICANN, mas também que são tão confiáveis quanto ele. Por mais desejável que seja de um ponto de vista político termos algo que substitua a ICANN, esta provou ser um agente regulador competente para serviços de nomes de domínios, que são fornecidos por entidades de registro muito profissionais e confiáveis. Ademais, pode-se esperar que a ICANN não moverá uma palha para ajudar estas raízes

alternativas a surgirem. Por isso, para uma raiz alternativa realmente chegar à internet, ela deverá provar que sua implementação e utilização valem a pena. Este não é um caminho fácil; desde o final dos anos 1980 várias tentativas têm sido propostas para raízes alternativas, e até hoje nenhuma delas teve sucesso.

:: HAVERÁ UM SUBSTITUTO PARA O SISTEMA DNS?

Certamente, em algum momento, o DNS atual será substituído. O sistema tem sido um componente crucial da internet desde o final dos anos 1980. Ele cresceu e foi estendido para suportar funções além das que foram concebidas no momento de sua criação.

O DNS irá durar mais 10 anos? Certamente, existe um exército de engenheiros dedicados e brilhantes para mantê-lo em funcionamento.

O DNS pode durar mais 20 anos? Esta pergunta é difícil, tenho minhas dúvidas. Quando se considera o número de novos endereços que precisarão um nome associado devido à introdução do IPv6 com sua abundância de endereços, é difícil imaginar que o sistema atual de DNS continuará sendo adequado para a tarefa por mais uma ou duas décadas.

Uma coisa certa é que implementar um novo sistema de nomeação na internet não será um processo trivial. Não apenas o sistema de nomeação

11. Ver <https://gnunet.org/>

precisa ser desenvolvido com sucesso, mas também precisa ser aceito pela comunidade técnica da internet e precisa ser implementado. A experiência na internet mostra que qualquer sistema novo, por exemplo o IPv6 ou um novo protocolo de roteamento, necessita de ao menos uma década a partir do momento em que o protótipo estiver completo até estar pronto para o uso. É provável que muitos sistemas de nomeação, e muitos novos protocolos de nomeação, irão surgir nos próximos anos –

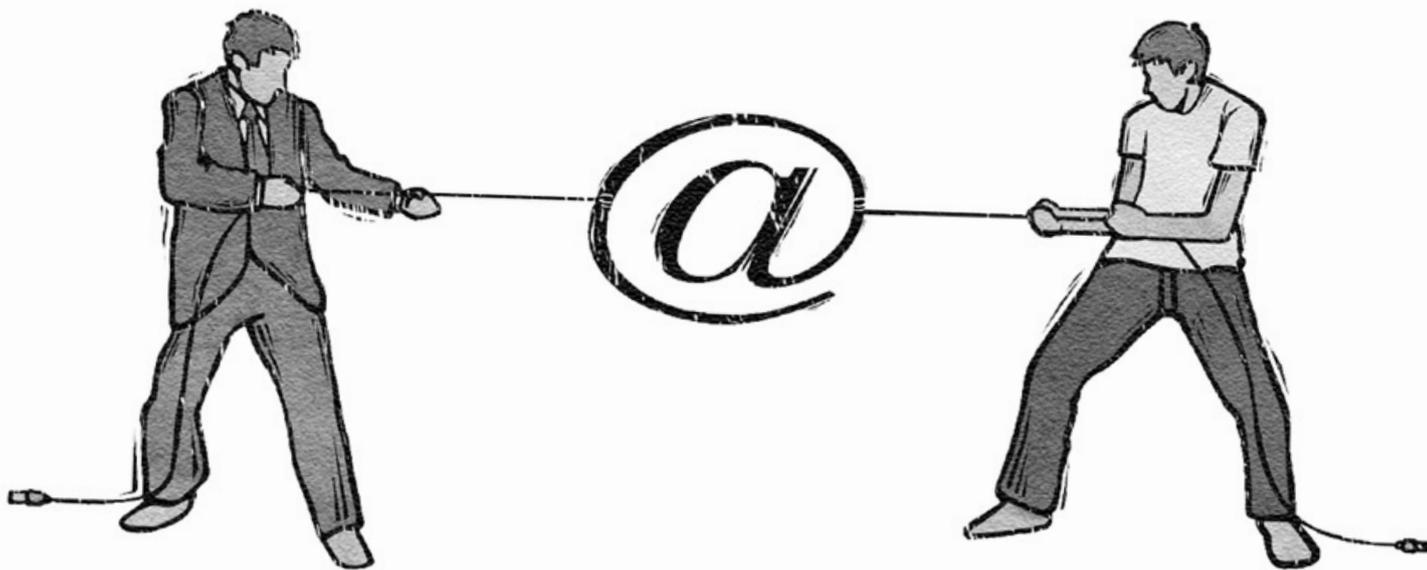
a não ser que as potências da engenharia da internet e organizações de governança se unam em uma nova estrutura e arquitetura de nomeação. E um requisito para este novo sistema é provavelmente sua habilidade em apoiar múltiplas autoridades de nomeação.

Algum dia a internet irá suportar um sistema de nomeação com uma estrutura de raízes dispersas que serão pares entre si. Como iremos chegar lá e como será esta situação, são questões que ainda estão em aberto. ●

■ Para uma raiz alternativa realmente chegar à Internet, ela deverá provar que sua implementação e utilização valem a pena. Este não é um caminho fácil .



> **Wolfgang Kleinwächter** Professor de Políticas e Regulação da Internet na Universidade de Aarhus. Atualmente preside o Europe Cross Border Internet Expert Group.



A febre dos princípios da internet:

como o direito indicativo é utilizado para regular a internet

Nenhum governo percebeu quando Tim Berners-Lee, do CERN¹, em Genebra, publicou um pequeno resumo de seu projeto da WorldWideWeb no alt.hypertext-newsgroup - no dia 6 de agosto de 1991. O mundo estava mais preocupado com o fim da Guerra Fria e a internet estava sendo ignorada pelos líderes políticos.

Vinte anos depois, cada vez mais governos estão lutando para controlar as consequências da invenção de Berners-Lee. O ano de 2011 poderá ficar para os livros de história da Internet como o ano dos 'Princípios Governamentais para a Internet'.

A Internet subiu a escada de prioridades políticas e agora já alcançou o G-8. Quando os líderes de oito

1. Sigla de European Organization for Nuclear Research. <http://public.web.cern.ch>

poderosas nações – Obama, dos E.U.A.; Medvedev, da Rússia; Sarkozy, da França; Merkel, da Alemanha; Cameron, do Reino Unido; Berlusconi, da Itália; Harper, do Canadá; Kan, do Japão; e Baroso da União Europeia – se juntaram em um resort francês em Deauville no fim de maio de 2011, as políticas da internet eram uma questão de prioridade em sua agenda.

Três das quinze páginas da Declaração de Deauville tratavam da internet. E como destaque, os líderes do G-8 concordaram em ‘um número de princípios-chave, incluindo liberdade, respeito à privacidade e propriedade intelectual, governança multissetorial, cibersegurança e proteção contra o crime’.

A Declaração enfatiza que tal acordo teria sido atingido ‘pela primeira vez no nível das lideranças’.

Mas não foi apenas o G-8 que descobriu que a internet é uma questão de alta política em 2011.

O Conselho da Europa, a OCDE², a OSCE³ e a OTAN⁴ lançaram iniciativas para a elaboração e adoção de princípios da internet. O Presidente norte-americano Barack Obama propôs dez princípios em seu documento de estratégias publicado em maio de 2011; a Comissária Europeia Neelie Kroes ofereceu sete princípios quando propôs o ‘Internet Compact⁵’ no final de julho de 2011. O Brasil, a Índia e a África do Sul – em nome do G-77 – propuseram na 65^a Assembléia Geral da

ONU, em setembro de 2010, o lançamento de uma ‘nova plataforma intergovernamental da internet’. E mais, uma reunião do G-20, que também inclui a China, está marcada para novembro de 2011 em Cannes.

Por que tem surgido tanta euforia sobre os princípios da internet e qual será o resultado deste ativismo governamental e intergovernamental?

:: OS ANOS OITENTA: A ‘NETIQUETA’

Vamos voltar na história. A internet nunca foi uma zona sem-lei. No entanto, ela se desenvolveu principalmente à sombra de regulamentos governamentais específicos. Ao contrário da invenção da telecomunicação e da radiotransmissão – que logo após sua adoção foram empurradas para uma estrutura regulamentar de leis nacionais – ninguém introduziu uma Lei Nacional para a Internet ou uma Convenção Internacional da Internet após o protocolo TCP/IP ter aberto as portas para o desenvolvimento de uma rede de redes, a internet.

Os mecanismos autorreguladores introduzidos pela própria comunidade da internet – um pequeno grupo de *nerds* nos anos setenta e oitenta – foram considerados suficientes para gerenciar a rede emergente. O procedimento RFC, introduzido em 1969, proveu as regras necessárias para garantir a estabilidade e flexibilidade requeridas e para

2. Organização para Cooperação e Desenvolvimento Econômico – <http://www.oecd.org/> 3. Organização para a Segurança e Cooperação na Europa – <http://www.osce.org> 4. Organização do Tratado do Atlântico Norte – <http://www.nato.int> 5. Ver em <http://blogs.ec.europa.eu/neelie-kroes/tag/internet-compact/>

manter sob controle quaisquer problemas que pudessem surgir.

Um exemplo disso foi a 'netiqueta', que introduziu algumas normas éticas como princípios básicos para a conduta adequada na internet em relação a usuários individuais. a netiqueta' foi desenvolvida no início dos anos oitenta quando o e-mail em forma de mensagem de texto, a Telnet⁶, a Usenet⁷, o Gopher⁸, o Wais⁹, e o FTP¹⁰ de órgãos educacionais e de pesquisa dominavam o tráfego na internet.

A WWW foi certamente um marco para a internet. Em dois anos o número de usuários explodiu - e chegou a 300 milhões em 1995. Os pioneiros da internet perceberam rapidamente que eles teriam de fazer algo em relação às suas regras internas.

Sally Hambridge, da Intel, publicou em outubro de 1995 um novo RFC - o famoso RFC 1855 - que resume e descreve o conjunto de princípios para uma 'netiqueta para a internet'. "Hoje em dia", escreveu Hambridge, "a comunidade dos usuários da internet inclui pessoas que são novas neste ambiente. Estes 'novatos' não tem familiaridade com a cultura e não precisam saber sobre transporte e protocolos. Para incluir estes novos usuários na cultura da internet rapidamente, este Guia oferece um mínimo de princípios de conduta que organizações e indivíduos podem adotar e adaptar para seu próprio uso".

O RFC 1855 inclui um conjunto de normas como o famoso 'princípio de robustez', mais conhecido como lei Postel, do RFC 761: "Seja conservador no que você envia; seja liberal com relação ao que você aceita receber". Mas o RFC 1855 também inclui regras como "não envie e-mail não solicitado" e "respeite os copyrights do material que você reproduzir".

O problema com a netiqueta era a inexistência de um mecanismo para sua implementação. Pessoas responsáveis respeitavam as regras, mas a conduta irresponsável continuava impune. A pior coisa que poderia acontecer com quem quebrasse as regras era ter sua reputação manchada diante da comunidade. Mas quando criminosos, pessoas que praticam crimes motivados pelo ódio, pedófilos, vândalos e terroristas começaram a povoar a internet no fim dos anos noventa, a 'netiqueta' chegou ao seu limite.

:: O SETOR PRIVADO VS. A LIDERANÇA GOVERNAMENTAL

Assim, dava para entender porque alguns governos começaram, já em meados dos anos noventa, a pensar sobre algum tipo de estrutura de regulação para a internet apoiada pelo governo.

O Comissário Europeu Martin Bangemann utilizou a Conferência da União Internacional das Telecomunicações (UIT) de setembro de 1997, em Genebra, para propor uma 'Declaração para a

6. Ver em <https://secure.wikimedia.org/wikipedia/en/wiki/Telnet> 7. Ver em <https://secure.wikimedia.org/wikipedia/en/wiki/Usenet> 8. Protocolo Gopher: ver em https://secure.wikimedia.org/wikipedia/en/wiki/Gopher_%28protocol%29 9. Sigla de Wide Area Information Servers. Ver em https://secure.wikimedia.org/wikipedia/en/wiki/Wide_area_information_server 10. Sigla de File Transfer Protocol: ver em <https://secure.wikimedia.org/wikipedia/en/wiki/FTP>

Sociedade da Informação'. A ideia não conseguiu angariar o apoio necessário.

Os novos empresários da crescente economia da internet temiam que tal declaração não fosse promover, mas sim restringir o desenvolvimento da internet, introduzindo uma regulação pesada que poderia eventualmente bloquear o conceito criativo de 'inovação sem permissão'. E o governo dos EUA temia que uma Declaração com o apoio da ONU pudesse reabrir o debate contraproducente da UNESCO sobre uma 'Nova Ordem Mundial de Informação e Comunicação' (NWICO, sigla em inglês), nos anos oitenta.

Como resultado, as novas grandes empresas da internet estabeleceram proativamente o 'Diálogo de Negócios Global em e-Comércio' (GBDe, sigla em inglês) no qual propuseram desenvolver uma estrutura autorreguladora. E o governo dos EUA lançou uma iniciativa privada chamada 'Corporação da Internet para Atribuição de Nomes e Números', a ICANN, na qual governos têm apenas papel consultivo.

Nem todos ficaram felizes com a ICANN e com o princípio de liderança do setor privado. Quando a ONU lançou a Cúpula Mundial sobre a Sociedade da Informação (CMSI) em 2002, a China argumentou que a liderança do setor privado era provavelmente positiva numa internet de um milhão de usuários. Mas com um bilhão de usuários, a liderança dos governos seria necessária para manter a internet sob controle.

A Governança da Internet se tornou subitamente o foco do conflito pelo poder político. O resultado foi EUA vs. China, ICANN vs. UIT, a liderança do setor privado vs. liderança dos governos.

Foram necessários três anos de negociações e intensos esforços de um Grupo de Trabalho da ONU sobre Governança na Internet (GTGI), organizado pelo ex-Secretário Geral da ONU Kofi Annan, até que fosse possível chegar a um acordo.

O GTGI rejeitou a ideia de uma 'liderança única' e propôs um modelo multissetorial no qual todas as partes - governos, setor privado e a sociedade civil - deveriam trabalhar juntas 'através de seus respectivos papéis', 'compartilhando princípios, normas, regras, procedimentos para a tomada de decisões, e programas que moldam a evolução e o uso da Internet'.

A recomendação do GTGI alcançou a Agenda de Túnis, que foi adotada pelos chefes de estado de mais de 150 governos do mundo na Segunda fase da CMSI, em novembro de 2005.

A agenda de Túnis não introduziu uma regulação específica para a internet, no entanto, esta incluía, em uma linguagem vaga, um conjunto de princípios gerais que poderiam ser interpretados como o ponto de partida para uma estrutura de regulação para a governança da internet, baseada em um modelo multissetorial.

O Fórum de Governança na Internet (IGF, sigla em inglês), outro resultado da CMSI, tornou-se

um espaço para a continuação do debate. Durante a segunda reunião anual do Fórum, no Rio de Janeiro (em novembro de 2007) a chamada Coalizão Dinâmica sobre Direitos e Princípios na internet, foi formada – e produziu um relatório razoável em três anos.

O Fórum não tem capacidade de tomada de decisão e os resultados das Coalizões Dinâmicas não são mais (mas também não menos) do que sugestões para reflexão.

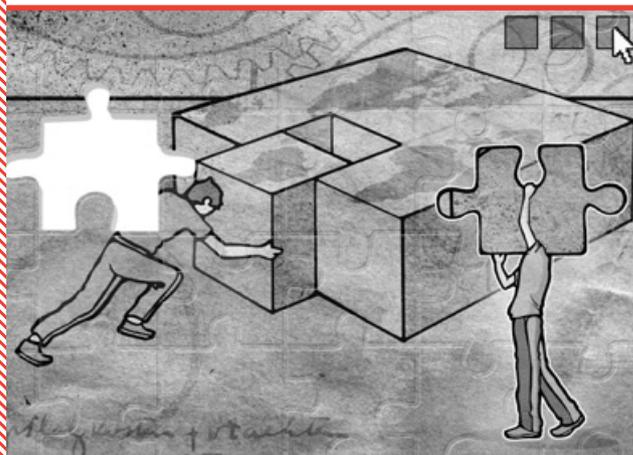
:: REPENSANDO A FORMULAÇÃO DE POLÍTICAS DE INTERNET

E, claro, o IGF fez com que fosse repensada a necessidade de se ter algo como uma estrutura de regulação global para a internet. Enquanto emergiu rapidamente o “consenso aproximado” de que a ideia sobre ter ‘algo no papel’ não seria tão ruim, havia uma divisão marcante. De um lado, havia grupos que desejavam ver uma convenção de valor jurídico; de outro, havia grupos a favor de uma solução mais suave, uma declaração política de princípios gerais não-vinculativos que ajudaria a identificar o que seriam condutas positivas ou negativas na internet.

Na ONU, os países do G-77 argumentaram que faltaria um elo no ecossistema de Governança da Internet e eles propuseram um novo mecanismo intergovernamental, que poderia chegar a um tratado da Internet.

Em 2010, o governo dos EUA propôs à OCDE começar a esboçar princípios para formulação de políticas na Internet. E quando a França chegou à

■ Enquanto todos parecem concordar a respeito do multisetorialismo, existem incertezas e diferenças profundas em relação ao que se entende a respeito deste princípio vagamente definido.



presidência do G-8 em 2011, o Presidente Sarkozy anunciou, em janeiro deste ano, que a Internet seria a prioridade de sua presidência.

Esta febre em torno dos princípios da internet não é uma surpresa. Com mais de dois bilhões de usuários, a internet não é mais um lugar para *nerds*, mas reflete um mundo em sua totalidade e com suas deficiências.

Em 2011, a internet pousou no centro da economia e política mundiais. 'O mundo deve reconhecer em conjunto os desafios apresentados pela entrada de atores malévolos no ciberespaço e atualizar e fortalecer nossas políticas nacionais e internacionais adequadamente', argumentou o Presidente norte-americano, Barack Obama, em sua 'Estratégia Internacional para o Ciberespaço' em maio de 2011. 'Atividades que ocorrem no ciberespaço têm consequências para nossas vidas no espaço físico e nós temos de trabalhar em direção à construção de regras e leis, para prevenir que os riscos de conectar-se não superem os benefícios'.

O Presidente disse ainda: 'O futuro de um ciberespaço aberto, interoperacional, seguro e confiável depende de que as nações reconheçam e protejam aquilo que deve durar, enquanto confrontam aquilo que pode desestabilizar ou minar nosso mundo cada vez mais conectado'.

O que podemos ver aqui é uma mudança de política importante: de uma constelação 'sem leis vs. com leis vinculativas' para uma abordagem mais suave, uma 'netiqueta' que busca não apenas alcançar a comunidade da internet mas também todos os governos, setor privado e sociedade civil.

Tal abordagem de direito indicativo poderia sim garantir a continuação da flexibilidade da internet – necessária para sua evolução – e um grau de estabilidade mais alto, necessário para conseguir a confiança dos próximos bilhões de usuários e da nova geração de empresários.

Uma abordagem de direito indicativo também permite que se vá além dos mecanismos tradicionais intergovernamentais para formular leis internacionais e para melhorar parcerias e cooperação no desenho de estruturas políticas e de regulação para a governança na internet.

Após o Conselho da Europa (em junho de 2011) e a OCDE (em julho de 2011) terem adotado documentos e os EUA, UE e o G-8 terem publicado declarações, faz sentido fazer uma análise mais detalhada sobre estas atividades.

Uma comparação breve entre estes novos documentos leva-nos a quatro conclusões interessantes:

1. Todas as partes apóiam o modelo multissetorial como princípio básico de governança;
2. Todas as partes apóiam os princípios de arquitetura historicamente concebidos de uma internet aberta (e2e);
3. Todas as partes identificam três áreas principais onde políticas são necessárias: Direitos Humanos, Segurança e Economia;
4. Todavia, as partes têm diferentes prioridades quando se trata de questões políticas.

Tabela 1: Comparação de Princípios de Governança na Internet da Declaração do Conselho da Europa (junho de 2011), do Comunicado da OCDE (julho de 2011), da Estratégia Internacional para o Ciberespaço dos EUA (maio de 2011), a Proposta da União Europeia (julho de 2011) e a Declaração do G-8 (maio de 2011). Princípios específicos estão identificados por '[x]'..

Assunto	Conselho da Europa	OCDE	EUA	UE	G-8
Direitos Humanos	[1] Direitos Humanos, Democracia e leis	[1] Livre Fluxo de Informação Global	[1] Suporte às Liberdades Fundamentais	[4] Pró-Democracia	[1] Liberdade
	[10] Diversidade Linguística e Cultural	[9] Proteção da Privacidade	[3] Valorização da privacidade		[2] Proteção da Privacidade
Segurança	[3] Responsabilidade dos Estados	[5] Base de Dados confiável para formulação de políticas	[4] Proteção contra Crimes	[1] Responsabilidade Cívica	[5] Cibersegurança
	[6] Integridade da Internet	[6] Transparência, Processo Justo e Prestação de Contas	[5] Direito de Auto-Defesa		[6] Proteção contra Crime
		[13] Cooperação para Segurança na Internet	Cibersegurança e investigação rigorosa		
Governança	[3] Governança Multissetorial	[5] Processos multissetoriais de desenvolvimento de políticas	[9] Governança multissetorial	[3] Governança multissetorial	[4] Governança multissetorial
	[4] Empoderamento dos usuários	[6] Códigos de Comportamento Voluntariamente Desenvolvidos		[7] Governança Transparente	
	[7] Gerência Descentralizada	[10] Empoderamento e responsabilidade do indivíduo			
		[14] Aplicação e execução das normas			
Tecnologia/Arquitetura	[5] Universalidade da Internet	[2] Internet aberta, distribuída e interconectada	[6] Interoperabilidade Global	[2] Uma Internet	
	[8] Arquitetura Aberta		[7] Estabilidade da Rede	[5] Arquitetura Aberta	
	[9] Rede Aberta		[8] Acesso Confiável		

Tabela 1: Comparação de Princípios de Governança na Internet da Declaração do Conselho da Europa (junho de 2011), do Comunicado da OCDE (julho de 2011), da Estratégia Internacional para o Ciberespaço dos EUA (maio de 2011), a Proposta da União Europeia (julho de 2011) e a Declaração do G-8 (maio de 2011). Princípios específicos estão identificados por '[x]'.

Assunto	Conselho da Europa	OCDE	EUA	UE	G-8
Economia		[3] Investimento e Competição na área de Banda Larga de Alta Velocidade [4] Entrega de serviços transfronteiras [11] Criatividade e Inovação [12] Limites para as responsabilidades e obrigações de Intermediários	[2] Respeito à propriedade	[6] Confiança para o Usuário	[3] Proteção à Propriedade Intelectual

Na teoria, princípios são bons. Eles fornecem a orientação e critérios através dos quais pode-se avaliar condutas individuais e coletivas. É bem mais fácil chegar a um consenso sobre princípios não-vinculativos do que sobre normas juridicamente vinculativas. Quando o mundo queria fazer algo após a Segunda Guerra Mundial para promover os direitos humanos, Eleanor Roosevelt, que presidiu a comissão de redação nas Nações Unidas, preferiu a abordagem baseada em direito indicativo como o passo inicial. A Declaração Universal dos Direitos Humanos (1948) é um conjunto de princípios não-vinculativos juridicamente.

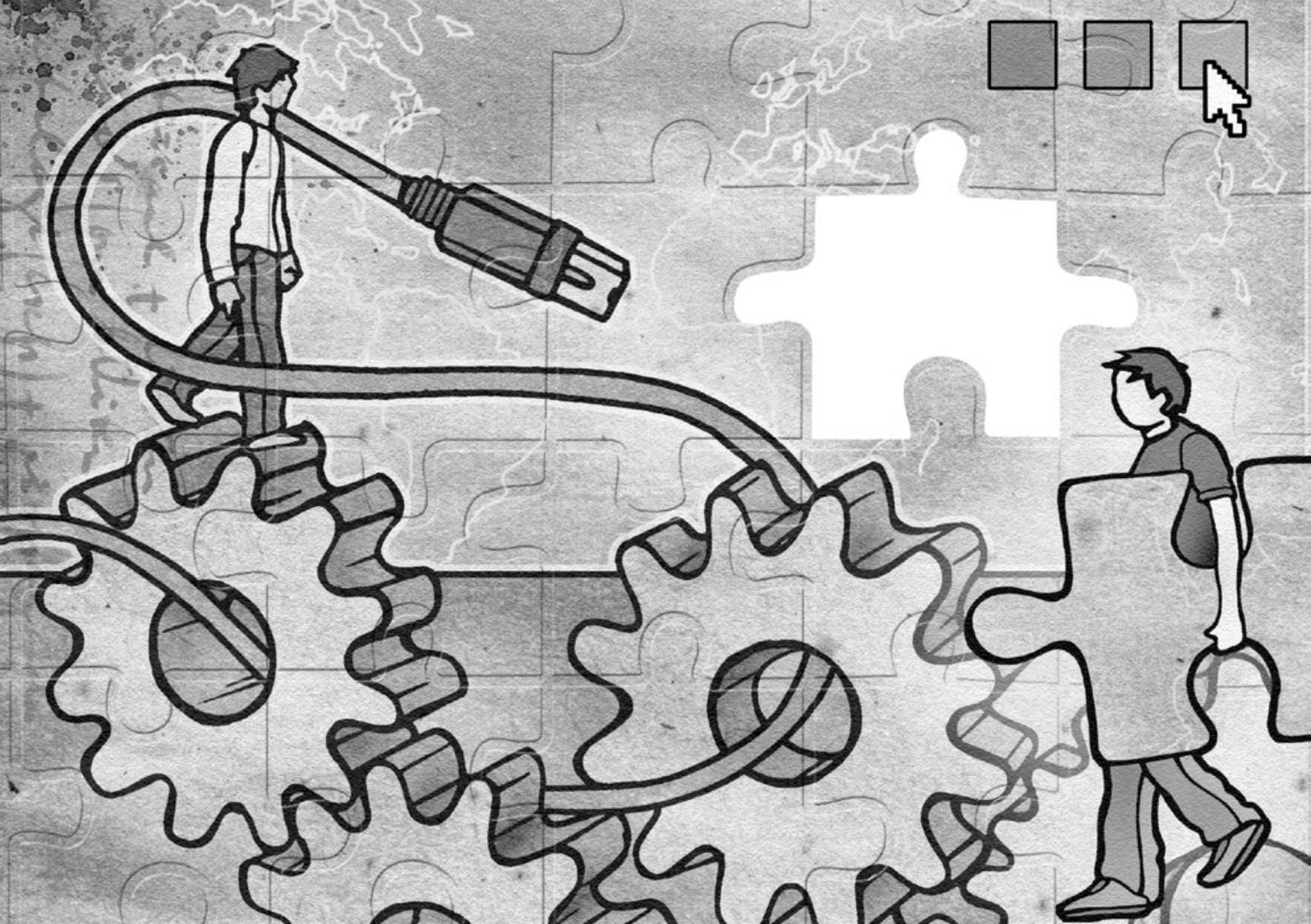
Demorou mais dezoito anos para ser finalizada uma convenção juridicamente vinculativa (1966) e mais vinte anos até a grande maioria da ONU ratificar o tratado.

Como mostra a experiência, o poder político dos princípios da Declaração dos Direitos Humanos não pode ser subestimado. Mas princípios não são 'executáveis' - assim como a 'netiqueta' - a única coisa que se pode fazer é acusar e envergonhar.

:: O NOVO TRIÂNGULO

No entanto, mesmo a abordagem de direito indicativo é cheia de armadilhas - e diferentes governos, investidores e organizações têm ideias diferentes sobre as prioridades em relação aos campos de política não-técnica.

Para o Conselho da Europa, sede do Tribunal Europeu de Direitos Humanos e da Convenção Europeia de Direitos Humanos, Direitos Humanos e Liberdades dos indivíduos que utilizam a internet são prioridade máxima.



Para a OCDE, o mais importante é a inovação, o crescimento econômico e a proteção da propriedade intelectual.

Para o governo dos EUA, assim como para a OTAN (que ainda não adotou um documento formal mas está trabalhando em uma versão provisória de Princípios da Internet), a cibersegurança é a preocupação número um.

Estas formas de priorizar não significam que o Conselho Europeu ignora a segurança e a economia da OCDE e que o governo dos EUA ignora os Direitos Humanos. O problema é que em caso de um conflito, onde interesses e valores legítimos têm que ser equilibrados entre si, diferentes organizações oferecem diferentes soluções. Se para uma organização a dimensão de direitos humanos de um caso especial é vista

como mais importante do que as implicações em relação à segurança, outra organização pode chegar a uma outra conclusão e argumentar que a cibersegurança também precisa de limites em relação a direitos humanos individuais.

Em outras palavras, o que veremos no futuro não é apenas uma batalha entre governos e entre investidores governamentais ou não-governamentais, mas também uma batalha entre segurança, economia e ativistas de direitos humanos dentro dos governos, setor privado e sociedade civil.

O desafio de como criar um triângulo mágico que equilibre aspectos de segurança, economia e direitos humanos se tornará uma questão crucial para o desenvolvimento de políticas da internet nos próximos dez anos.

As negociações dos princípios da OCDE foram um bom exemplo, que serviu para abrir os olhos de todos. A OCDE, uma organização intergovernamental, abriu-se para o modelo multissetorial após sua conferência Ministerial em Seul, em 2007. Esta convidou o setor privado, a comunidade técnica e a sociedade civil a formar comitês para participar nos processos de formulação de políticas da OCDE.

Durante a fase final das negociações da OCDE, o conselho consultivo da sociedade civil – o CSISAC – discordou de dois princípios. Aos olhos do CSISAC, os princípios da OCDE dariam preferência aos interesses empresariais e ignorariam os direitos humanos, particularmente em relação aos direitos de propriedade intelectual e responsabilidade de intermediários.

Os governos da OCDE, incluindo o governo dos EUA, realizaram esforços para incluir as posições do CSISAC. Mas o conflito não pôde ser amenizado e o CSISAC decidiu não apoiar o documento final.

O Conselho da Europa não tem ainda um mecanismo multissetorial, mas organizou uma conferência multissetorial antes de redigir a versão final de sua declaração em Estrasburgo, em abril de 2011.

Durante esta conferência ficou claro que as partes não-governamentais apoiam várias ideias na declaração provisória mas rejeitaram a ideia de assinar um documento que seria incorporado apenas por governos. Estas organizações desejavam ficar em posição de igualdade em um processo de desenvolvimento de políticas de caráter

transparente e que se desse de baixo para cima. O Conselho da Europa, que apoia o modelo multissetorial, está considerando agora continuar esta discussão e melhorar a 'Declaração de Princípios de Governança na Internet' intergovernamental, em um 'Marco de Compromissos' multissetorial (FoC, sigla em inglês).

:: SEGUINDO ADIANTE EM TERRITÓRIO NÃO EXPLORADO

Estes casos nos levam a outro problema: enquanto todos parecem concordar a respeito do multissetorialismo, existem incertezas e diferenças profundas em relação ao que se entende a respeito deste princípio vagamente definido.

Alguns governos perceberam que têm de ir além de seus procedimentos tradicionais de formulação de políticas, mas outros apenas apóiam da boca para fora o slogan bonito e continuam operando como de costume.

Isto não funcionará. Voltando à definição do GTGI, o princípio sugere que normas, princípios, regras e até a tomada de decisões deveriam ser 'compartilhados' entre as partes.

O modelo multissetorial não expressa uma relação senhor-escravo, no qual governos ditam o que tem que ser adotado em última instância; é um diálogo, uma nova parceria, na qual todas as partes, incluindo governos, participam de forma igualitária em seus respectivos papéis.

As ferramentas da diplomacia do século XX não são mais adequadas. É necessária uma nova

Diplomacia da Internet do século XXI. E para tanto são necessárias novas formas de interação entre as partes, dentro e fora do governo.

Sem dúvida, isto é difícil. Para os governos é certamente uma novidade ter que incluir uma organização da sociedade civil como o CSISAC (como no caso da OCDE) ou aceitar decisões que não lhes agradam (como no novo caso gTLD da ICANN).

Mas um modelo que volte ao processo de tomada de decisão organizado hierarquicamente, de cima para baixo, é o atalho errado. Não há uma outra forma de ir adiante neste novo campo de formulação de políticas. A inovação e a criatividade são necessárias não apenas no desenvolvimento de novos aplicativos e serviços da internet mas também na formulação de políticas da internet.

É verdade que o princípio do multissetorialismo ainda não está bem definido. E os procedimentos, o modo como as partes devem interagir em relação ao desenvolvimento de políticas e tomada de decisões, não estão escritos. A governança multissetorial é um passo em um território ainda não mapeado.

Quando os governos, o setor privado, a sociedade civil e a comunidade técnica entram nesta *terra incógnita*, todos os lados têm que respeitar uns aos outros – em seus respectivos papéis – e aí aprender a colaborar entre si, a se comunicar e coordenar de uma nova forma, encontrando soluções sustentáveis para um pacto público global.

Isso se torna ainda mais complicado porque existem muitos governos neste mundo que não são membros do G-8, nem da OCDE ou do Conselho da Europa e que têm suas próprias ideias sobre a Governança da Internet e o multissetorialismo – como a China, o Brasil, a Índia, a África do Sul, a Arábia Saudita, entre outros.

Não é preciso ser profeta para ver que o futuro da Governança na Internet será um campo de batalha importante nas próximas décadas.

Já na segunda metade do ano de 2011 veremos três eventos importantes nos quais esta questão irá surgir: em setembro de 2011, a sexta reunião anual do IGF ocorrerá em Nairóbi; em outubro de 2011, o Segundo Comitê da 66^a Assembléia Geral das Nações Unidas iniciará sua discussão sobre a Internet em Nova Iorque; e os líderes do G-20, incluindo China, Brasil, Índia, África do Sul e outros membros do G-77 se reunirão em Cannes.

* Nota dos editores: Este texto, ao ser distribuído em algumas listas de discussão na internet, gerou comentários interessantes sobre a necessidade de um olhar menos “eurocêntrico” sobre os temas que o texto aborda. No site da poliTICs alguns destes comentários estão reproduzidos, e o espaço está aberto para mais opiniões e possíveis debates. Convidamos nossas leitoras e leitores a acompanhar e participar em www.politics.org.br. ●

Os Guerreiros dos Dados Abertos estão lutando a favor de Robin Hood ou do xerife?

Reflexões sobre a OKCon 2011 e a emergente exclusão informacional



> **Michael Gurstein** Diretor executivo do Centre for Community Informatics Research, Development and Training e editor-chefe do Journal of Community Informatics.

Passei os últimos dias em um fascinante (e tenebroso) evento em Berlim – a OKCon¹ – uma conferência para meganerds (neste caso, em sua maioria europeus) que estão em processo de recriar governos e potencialmente a própria governança na Europa Ocidental (e além).

O ideal que estes revolucionários estão buscando não é, como fizeram as gerações anteriores, – a justiça, a liberdade, a democracia – é a ‘abertura’: Dados Abertos, Informação Aberta, Governo Aberto. Exatamente o que ‘abertura’ significa nunca é precisamente definido (ao menos não no contexto desta conferência), de forma que um leigo possa compreender o conceito, e talvez criticá-lo. Mas a intenção era boa, animadora e convincente – um cálice sagrado a ser procurado pelos guerreiros do ‘World of Warcraft’ em uma missão contra os dragões do governo. Suas armas neste caso são habilidades técnicas e zelo suficientes para aniquilar quaisquer racionalizações e resistências à ‘abertura’ por parte de burocratas ou políticos – por exemplo, ao não quererem transformar seus baús cheios de tesouros de informações em nodos universalmente acessíveis, no fluxo contínuo do universo global de dados.

Se pareço um pouco cínico/cético não é porque eu não acredito neste objetivo da ‘abertura’ (quem poderia ser obtuso o suficiente para apoiar

coisas ‘fechadas’, sistemas fechados, portas fechadas, mentes fechadas...você entende). Acontece que eu vejo uma grande desconexão entre o idealismo destes revolucionários, com sua crença passional na verdade da sua causa, e a profunda ausência de qualquer ideia clara do que precisamente é esta causa e onde esta poderá levá-los (e a nós) no futuro breve.

Começando do começo... o movimento ‘dados abertos/governo aberto’ surgiu a partir de uma perspectiva profundamente política que afirma que o governo é, de maneira geral, ineficiente e ineficaz (e possivelmente corrupto) e que ele esconde esta ineficiência e ineficácia (e possivelmente a corrupção) do escrutínio público através da falta de transparência em suas operações – particularmente, negando ao público o acesso a informações sobre suas operações. Este acesso, uma vez disponível, daria aos cidadãos meios para responsabilizar burocratas e políticos por suas ações. Isto também daria a estes mesmos cidadãos uma plataforma sobre a qual trabalhar(ou ao menos colaborar) com os burocratas em certas atividades importantes – planejamento, análise, orçamento, este tipo de coisa. Além disso, através da implementação dos processos de *crowdsourcing*² os burocratas poderiam usufruir do enorme benefício de ter acesso ao conhecimento e à sabedoria do público em geral.

1. The Open Knowledge Conference. Ver sobre o evento em <http://www.okcon.org/> 2. Ver em <https://en.wikipedia.org/wiki/Crowdsourcing>

■ O que está se constituindo são as estruturas para o ambiente de dados do futuro, da qual fazem parte algumas hipóteses e pressupostos sobre quem é e quem será o usuário final – e se irá ou não emergir uma nova ‘exclusão informacional’.

Em outras palavras – mas com essencialmente o mesmo significado –, o dinheiro público é do contribuinte e este tem o direito de participar na supervisão de como o dinheiro é gasto. Ter acesso ‘aberto’ aos dados e informações do governo dá aos cidadãos as ferramentas para exercitar este direito.

Além disso (conforme alguns argumentam), há soluções disponíveis para colocar nas mãos destes cidadãos e cidadãs os meios/ferramentas técnicas para selecionar, organizar e fazer análises críticas de atividades do governo – se apenas pudéssemos virar uma chave e ‘abrir’ a porta para acessar os dados governamentais.

Através de processos (parcialmente técnicos, parcialmente políticos) de persuasão, pressão política e eventualmente criação de políticas e mecanismos de intervenção, governos de toda parte estão em processo de desenvolvimento de

sistemas técnicos internos para tornar ao menos parte da informação governamental disponível – abrindo a porta para pessoas (tais como estas, que participaram do OKCon) trabalharem e desenvolverem maneiras de tornar esta informação útil e acessível. Na conferência ouvimos jovens entusiasmados que estão fazendo acontecer estas mudanças em várias partes da Europa, Estados Unidos, Brasil, etc.

Grande parte da conferência foi composta de oficinas especializadas nas quais foram estudados detalhes técnicos de como fazer os links entre vários conjuntos destes dados recém-acessíveis a outros conjuntos de dados; como estruturar estes dados para que sirvam a vários objetivos, e, talvez ainda mais importante, como fazer o design da arquitetura e da ontologia (em última análise, políticas e processos de gerenciamento)

dos dados dentro do governo, para que estes já “nasçam abertos” em vez de serem liberados somente após a ocorrência dos fatos que os geraram. Este processo tornaria muito maior a utilidade dos dados, no mundo de dados universalmente acessíveis e abertos.

Bem, até agora, tudo certo. Mas no primeiro dia da conferência, quando chegou a hora da minha apresentação, eu subitamente percebi que havia um cão na sala, um cão grande e importante que não estava latindo... Durante o primeiro dia do evento – e com uma ou duas exceções, também no segundo dia –, o que eu não escutei nem ao menos indiretamente foi uma discussão a respeito de quem seriam os usuários destes dados (aqueles que se beneficiariam da ‘abertura’) e qual seria realmente a utilidade destes dados.

Alguns podem se perguntar por que eu acho que este “cão que não late” tem tanta importância... por que importa quem será o usuário? O importante é que eles/nós tenhamos acesso aos dados e a melhor abordagem para isso é desenvolver um design que ‘qualquer um’ possa usar – um usuário universal – de forma que o que estiver sendo construído não seja um veículo, mas sim uma plataforma, e que não importe quem são os motoristas, se todos puderem usar a estrada.

Por isso, na ausência de qualquer expressão articulada de quem o (suposto) usuário ou usuária é, vamos especular um pouco sobre quem esta figura fantasma pode (ou não) ser – dado que em

situações como esta tende-se, na ausência de outras influências, a voltar ao que é conhecido e familiar. Então aqui uma pessoa pode certamente imaginar que espera-se que o usuário seja mais ou menos como as pessoas que estavam na sala – jovens, inteligentes, falando bem inglês, muito bem educados, em sua maioria do sexo masculino, pouca ou nenhuma minoria de raça ou cor representada, a maioria de classe média, com muitas habilidades técnicas e com um conjunto de valores e conceitos que combinam com as características anteriores: por exemplo, altamente individualistas, competitivos e não-tolerantes.

Minha hipótese é que o suposto usuário destes dados e dos tipos de medidas (políticas, procedimentos, programas), pelas quais existem batalhas e que estão sendo incluídas em políticas e práticas governamentais parecem muito com estas pessoas nesta conferência – o que me dá bastante medo. Sinto medo especialmente quando associo esta ideia às as evidências **bastante** fragmentadas que estão surgindo sobre quem estaria realmente utilizando estes dados abertos (o que corresponde bem à minha hipótese) e quais são os benefícios de seu uso.

Talvez o exemplo mais significativo até hoje de uma política de ‘abertura’ nacional seja a do governo indiano, a lei do Direito à Informação³ – que, comparada a qualquer padrão, é uma das legislações a favor do governo ‘aberto’ mais fortes

3. Ver em <http://righttoinformation.gov.in>

do mundo. Acontece que houve falhas (que me parecem erros fatais) na legislação/programa que só agora estão ficando evidentes. As falhas mais significativas são a falta de mecanismos de controle de aplicação das leis, e, talvez ainda mais importante, a falta de uma estratégia para a ampla implementação desta política nas bases da sociedade, com foco no usuário final.

O que aconteceu na Índia é que, ao construir a (falsa) hipótese de que usuários finais, como cidadãos, teriam os meios para usar esta lei para exercitar seu direito à informação sem auxílio adicional ou algum tipo de intervenção, a Índia criou uma situação na qual os indivíduos precisam participar por si mesmos de uma luta desequilibrada pelo acesso e uso da informação, e o resultado tem sido uma onda de assassinatos – na qual as vítimas são aqueles que tentam utilizar a informação para expor casos de corrupção, nepotismo e uso indevido do dinheiro público.

A legislação não fornece mecanismos para garantir a aplicação da lei – e assim indivíduos e grupos tiveram que assumir por sua própria conta a tentativa de obter acesso às informações desejadas através de ações individuais. Portanto, ao invés de ter uma legislação focada no usuário final em potencial – aquele que conforma as suas multidões –, a Índia

simplesmente promoveu um ‘acesso’ conceitual e deixou o restante com os cidadãos e indivíduos, gerando resultados nefastos⁴.

Mas por que estes jovens entusiasmados, que estão a cinco mil milhas de distância da Índia, deveriam se importar? Bem, se olharmos para um dos poucos estudos detalhados sobre o usuário final⁵ (Escher) de um projeto de dados abertos⁶ da ferramenta para a democracia cidadã online TheyWorkForYou.com, começamos a perceber um padrão:

“Em geral, a demografia destes usuários vai além dos preconceitos tradicionais na participação política: na TheyWorkForYou.org o público com mais de 54 anos tende a estar super-representado, enquanto as pessoas com menos de 45 anos estão sub-representadas em comparação à população da internet. Em termos demográficos existe um viés forte para o sexo masculino e uma forte super-representação de pessoas com ensino superior, o que traduz uma forte participação de grupos de renda alta... Um em cada cinco usuários (21%) do site não esteve politicamente ativo no último ano”.

Se eu entendi bem, isso significa que 79% dos usuários deste website (e da informação relacionada a ele) mostraram-se politicamente ativos no último ano!

4. Ver: Primeiro Assassinato por conta do Direito à Informação - <http://www.foiadvocates.net/es/noticias/43-news/237-first-right-to-information-murder>. Outro Ativista pelo Direito à Informação Assassinado na Índia - <http://www.imaxi.org/content/another-right-information-activist-murdered-india>. Três Ativistas pelo Direito à Informação foram assassinados neste país em três meses - http://www.tehelka.com/story_main47.asp?filename=Ne091010Dead_Right.asp
5. Em http://www.mysociety.org/wp/wp-content/uploads/2011/06/TheyWorkForYou_research_report-2011-Tobias-Escheri.pdf 6. Este projeto tem sido reproduzido em algumas jurisdições nacionais.

Então esta tentativa para melhorar a participação democrática acabou oferecendo uma oportunidade adicional para aqueles que, devido à sua renda, educação – e outras características típicas daqueles que têm um status mais alto – já possuem os meios de se comunicar e de influenciar políticos. Esta informação e este canal de comunicação adicionais, portanto, têm o efeito de reforçar padrões de oportunidade que já existem, ao invés de ampliar a base de participação e influência.

Em um post anterior⁷ analisei um caso similar: os resultados de um programa para digitalizar registros de terras em Bangalore que teve o efeito imprevisto e perverso de fornecer um meio para que os ricos proprietários de terra ampliassem suas propriedades e riqueza às custas dos pobres, porque eles tinham o conhecimento sobre como utilizar a nova informação posta à disposição, bem como os recursos para empregar profissionais para ajudá-los a interpretar a informação da maneira mais útil para eles.

Por isso importa muito quem é o (suposto) usuário, já que o que está se constituindo são as estruturas para o ambiente de dados do futuro, da qual fazem parte algumas hipóteses e pressupostos sobre quem é e quem será o usuário final – e se irá ou não emergir uma nova ‘exclusão informacional’ mais profundamente embrenhada no tecido da Sociedade da Informação do que a anterior ‘exclusão digital’.

Em cada uma destas instâncias, pelo fato de **não** se prestar atenção em quem serão os usuários finais em potencial dos ‘dados e informações abertos’ (e portanto não havendo intervenções para se redefinir isso), o efeito tem sido o de reforçar ou até mesmo estender as estruturas de poder e de influência existentes, ao invés desta abertura ser uma base para uma participação democrática mais inclusiva. Na ausência de modelos explícitos de um usuário final – e conseqüentemente de um design de processos apropriado para abrir a informação e torná-la acessível para a maior (e menos implicitamente discriminatória) gama de pessoas possível, o resultado será o que temos visto: o usuário é aquele que já está em condições de utilizar a informação por conta de suas habilidades, conhecimento, poder ou status.

Para que estes processos não gerem este tipo de resultados, o designer de dados deve basear seu trabalho em um modelo implícito de usuário que não tenha renda alta, que não tenha características de cor, gênero ou classe que automaticamente representem influência e poder.

Já lidei com a questão de como garantir oportunidades para uma base mais ampla de uso efetivo (e de usuários efetivos) de tecnologias de informação e comunicação em outra ocasião⁸ – mas neste contexto, como uma recomendação para aqueles que apoiam e para aqueles que estão

7. Em <http://gurstein.wordpress.com/2010/09/02/open-data-empowering-the-empowered-or-effective-data-use-for-everyone/> 8. Ver em <http://gurstein.wordpress.com/2010/09/09/open-data-2-effective-data-use/>

desenvolvendo projetos de Dados Abertos, gostaria de sugerir que haja um comprometimento formal de dedicar 10% dos recursos dos projetos e programas, o que inclui tempo e dinheiro, para garantir que os Dados Abertos sejam utilizados por grupos e indivíduos que não têm habilidades técnicas, que não são de classe média/alta, que não se encontram ativos nos processos políticos mas que possam fazer o melhor uso dos recursos que estão se tornando acessíveis⁹.

:: 'ABERTO' – NECESSÁRIO, MAS NÃO SUFICIENTE

Meus comentários e reflexões sobre a recente conferência da OKCon, o evento anual da Open Knowledge Foundation¹⁰ (OKF) parecem ter causado um pouco de polêmica entre certos membros sêniores da OKF. O resultado foi uma série de comentários no meu post original e agora uma resposta num post em um blog¹¹ criado por Peter Murray-Rust, um membro do conselho da OKF, com sérias reações ao meu texto.

Em relação a esta repercussão eu afirmei, em uma discussão paralela que se desenrolou online, que eu acredito que uma medida do sucesso de uma postagem em um blog é quando esta suscita comentários que a superam em termos de paixão,

conhecimento e inteligência – e é isso que está acontecendo, neste caso.

Então, onde estamos? Primeiro, quero esclarecer o máximo possível minha própria posição, só para ter certeza que fique evidente que eu sou fortemente a favor da 'abertura', tanto no sentido mais trivial de 'abertura para tudo' (quando não ser 'aberto' significa apoiar o 'lado sombrio'), e no sentido mais construtivo dado ao termo, que é utilizado pela OKF no seu website: **'Um conteúdo ou dado que é aberto para qualquer um e é grátis para utilizar, re-utilizar, e redistribuir – sujeito somente, ao requisito de se atribuir e partilhar este dado da mesma forma'**.

Uma breve biografia pode ser relevante neste momento. Passei a maior parte dos últimos quinze anos trabalhando no que agora é chamado de Community Informatics (CI)¹² – que diz respeito ao uso das Tecnologias da Informação e Comunicação (TICs) para empoderar e capacitar as comunidades. Há milhares de pessoas no mundo todo que se consideram profissionalmente dentro desta estratégia/disciplina/abordagem. A CI inclui uma publicação de acesso e arquivo abertos (da qual sou editor), revisada pelo público, um wiki¹³, várias e-listas¹⁴, conferências¹⁵, blogs, até cursos

9. Para as pessoas que tiverem interesse em minhas reflexões sobre o "Como fazer" recomendo uma postagem anterior do blog no qual há uma versão editada de artigo publicado numa edição recente de First Monday: em <http://gurstein.wordpress.com/2010/09/09/open-data-2-effective-data-use/> 10. Ver em <http://www.okfn.org/> 11. Ver em <http://blogs.ch.cam.ac.uk/pmr/2011/07/06/why-openness-matters-to-me-and-to-you-the-architecture-of-access-to-scientific-knowledge/> 12. Para saber mais: http://en.wikipedia.org/wiki/Community_informatics 13. Em <http://cirn.wikispaces.com/> 14. Ver em <http://vancouvercommunity.net/lists/info/ciresearchers> 15. Ver em <http://cirn.wikispaces.com/prato2010> 16. A definição do conceito pelo autor está em artigo na First Monday: <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1107/1027>

universitários, etc. Estou falando sobre isso porque a Community Informatics até certo ponto foi gerada no amplo contexto do ativismo local, técnico, político, baseado em respostas à exclusão digital – entendida em termos amplos como a divisão entre aqueles que têm e aqueles que não têm acesso às TICs.

A CI trouxe um componente chave a este contexto, que foi a noção de que embora o ‘acesso’ às TICs fosse uma condição necessária para superar a exclusão digital, somente o

acesso era ‘insuficiente’ para tornar disponível (e operacional) a gama de oportunidades para a promoção de avanços sociais e econômicos que as TICs tornam possíveis, e que tem transformado tão intensamente (e fortalecido, enriquecido e empoderado) negócios e governos. Por isso, a necessidade de darmos passos adicionais, promover intervenções e dar apoio para transformar ‘acesso’ em oportunidades – o que eu chamo de ‘uso efetivo’¹⁶.



Vejo um paralelo direto entre as questões que meus colegas e eu (e muitas outras pessoas) temos trabalhado nestes últimos quinze anos no contexto da exclusão digital e o que vejo agora em relação a Dados Abertos e movimentos relacionados.

Certamente não sou contra Dados Abertos e Governo Aberto da mesma forma que não sou contra a distribuição mais ampla possível do acesso à internet e a outras ferramentas de TICs (e isto tem sido o foco do meu trabalho nos últimos quinze anos). No entanto, da forma como vem sendo delineado o movimento de Dados Abertos em termos do objetivo geral do movimento, os Dados Abertos em si são insuficientes para realizar as mudanças positivas no governo, na ciência e na democracia.

De alguma forma o argumento aqui é mais claro do que foi em relação aos esforços para superar a exclusão digital. Comentando a resposta de Peter Murray-Rusk ao meu primeiro post sobre o assunto, Egon Willighagen diz:

*Dados Abertos não diz respeito a apresentar dados (governamentais) de maneira legível para a compreensão do público em geral, para que este possa tirar proveito dos dados (embora eu entenda por que ele tenha tido esta ideia), mas Dados Abertos diz respeito a tornar isto politicamente e tecnicamente *possível*. Ele não entendeu isso, infelizmente.*

Respondendo a Egon (e a Peter), eu entendi muito bem a questão sobre Dados Abertos; é precisamente sobre isto que estou sendo crítico.

Estou argumentando que Dados Abertos, apresentados desta forma, são suficientes apenas para fornecer recursos adicionais para ao Xerife de Nottingham e não para o Robin Hood.

'Dados Abertos', conforme articulado acima por Willighagen, é como um clube privado – tecnicamente (e legalmente) aberto para associação, mas os sócios precisam ter educação, recursos, habilidades técnicas – de forma que o clube se mantém ao alcance de um grupo bem seletivo.

Allison Powell, com seus comentários atenciosos nas minhas discussões do blog (no contexto de 'Hardware Livre') fala sobre aqueles que estão numa posição, através de pré-condições de riqueza, conhecimento técnico e poder, de se apropriar dos resultados da 'Abertura' (no caso, de hardware) para seus próprios objetivos corporativos.

Parminder Jeet Singh em seus comentários contrasta a ideia de Dados Abertos com a de Dados Públicos – uma terminologia e mudança conceitual com a qual estou começando a concordar – onde Dados Públicos são dados não somente 'abertos' mas também estruturados para serem utilizados pelo 'público' em geral (a população).

No contexto original da exclusão digital articulei noções sobre o que chamei de uso 'efetivo', ou seja, os fatores que precisam existir para que 'acesso' possa ser transformado em 'uso' pela população. Em uma postagem anterior¹⁷ eu transferi estes conceitos e os atualizei em um contexto de

17. Em <http://gurstein.wordpress.com/2010/09/09/open-data-2-effective-data-use/>

'Dados Abertos/Conhecimento Aberto e gostaria de sugerir que através da implementação da estratégia de incorporar o uso 'efetivo' de dados, o valor real deste projeto pode ser atingido e os perigos análogos de uma exclusão informacional podem ser evitados.

:: EXCLUSÃO INFORMACIONAL? OS QUE 'TÊM' E OS QUE 'NÃO TÊM' INFORMAÇÃO E OS DADOS ABERTOS GOVERNAMENTAIS

O conceito e substância da exclusão digital¹⁸ têm sido intensamente discutidos e pesquisados. A definição mais básica é: a divisão entre aqueles que têm acesso às Tecnologias da Informação e Comunicação, particularmente a internet, e aqueles que não têm este acesso.

Minha intenção aqui é me concentrar na discussão sobre a exclusão informacional – particularmente pensando em Dados Abertos Governamentais - neste momento, quando as coisas estão de alguma forma em fluxo, e existe uma possibilidade real daqueles mais diretamente envolvidos, designers de dados e funcionários públicos, prestarem atenção e intervirem de forma positiva.

Pesquisadores têm explorado¹⁹ extensivamente a gama de barreiras sociais, econômicas e geográficas que fundamentam e até certo ponto explicam (causam) a exclusão digital. Minha contribuição²⁰ tem sido argumentar que “o acesso não é suficiente”, o que faz diferença são oportunidades

e pré-condições para o “uso efetivo” da tecnologia, especialmente para as camadas mais populares.

Passou a me ocorrer a ideia de uma possível exclusão paralela – o hiato informacional²¹ entre aquelas pessoas que têm acesso aos dados e oportunidade de fazer uso efetivo deles (particularmente dos dados abertos) e as que não têm. Eu estava participando de vários eventos de planejamento/contratação para o movimento de Dados Abertos aqui em Vancouver e a demografia social e parte dos princípios políticos pareciam destoar da posição que advogava “dados para todos”.

Portanto, os “dados abertos²²” que estavam sendo defendidos provavelmente não seriam acessíveis e utilizáveis para grupos e indivíduos com os quais a Community Informatics tem se preocupado – as comunidades, os pobres e marginalizados, os indígenas, a população rural e moradores de favelas em países menos desenvolvidos. Foi – e ainda é – difícil ver, de acordo com as explicações dadas até o presente, como estas pessoas poderiam utilizar estes dados de maneira efetiva para ajudá-las a responder às oportunidades para o avanço e melhorias sociais que os ativistas de dados abertos vêm apontando como o resultado de seus esforços.

À medida em que eu mostrava esta inquietude em fóruns públicos e através do meu blog²³, tornou-se mais claro que muitos envolvidos no movimento de 'dados abertos' viam seus interesses e atividades

18. Ver em http://en.wikipedia.org/wiki/Digital_divide 19. Uma lista destes pesquisadores está em http://scholar.google.com/scholar?hl=en&rlz=1C1ACAW_ENZZ323&=&q= 20. Ver em <http://ojphi.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/1107> 21. Ver artigo na revista First Monday: <http://first-monday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3316/2764> 22. Ver em http://en.wikipedia.org/wiki/Open_data 23. Ver em <http://wp.me/pjQl5-7h>

limitados a tornar a informação 'legalmente' e 'tecnicamente' acessível – e o que aconteceria após isso seria responsabilidade de outros. Com isso concordo em parte. Assegurar a mais ampla oportunidade para o uso de, por exemplo, Dados Abertos Governamentais é uma grande responsabilidade pública obviamente partilhada entre autoridades públicas e desenvolvedores técnicos; na minha opinião os técnicos ficariam com a responsabilidade de certificarem-se de que, do seu lado, nenhuma barreira seja introduzida e que barreiras técnicas existentes sejam removidas para permitir o mais amplo uso dos dados.

Conforme fui pensando mais claramente nestas questões eu percebi que enquanto existiam paralelos marcantes entre a exclusão digital e o que eu vinha rapidamente associando como uma exclusão informacional, também existiam diferenças significativas – por exemplo, enquanto a exclusão digital lida com questões de infraestrutura em sua maior parte, a exclusão informacional se concentra em questões de conteúdo.

Além disso, enquanto a exclusão digital pode existir como resultado de considerações geográficas e políticas - e por isso ter efeitos uniformes sobre todos aqueles no lado desfavorecido da linha de exclusão, seja qual for sua situação sociodemográfica -, a exclusão informacional (e particularmente um dos componentes mais

importantes do movimento de dados abertos, que trata dos dados abertos governamentais), teria efeitos especialmente negativos e resultaria em significativas oportunidades perdidas para grupos e indivíduos mais vulneráveis na sociedade e no mundo.

A exclusão informacional seria então a diferença entre aqueles que têm acesso e têm a capacidade de utilizar Dados Abertos Governamentais e aqueles que não têm nem acesso, nem capacidade. Sugeri em outro momento²⁴ que existem vários componentes e camadas através dos quais a exclusão informacional (com base em uma análise similar da exclusão digital) pode ser compreendida:

1. infraestrutura— estar em situação de exclusão digital e portanto não ter acesso à infraestrutura básica que sustenta a disponibilidade de dados abertos governamentais;
2. ferramentas – dados que não são acessíveis universalmente e cujo acesso depende de ferramentas específicas (por exemplo, que só funcionam em um iPhone);
3. software – dados 'acessíveis' que requerem software e/ou treinamento específico para serem 'utilizáveis';
4. conteúdo – dados não desenvolvidos para serem utilizados por pessoas com deficiências, que não falam inglês ou com níveis baixos de escolaridade;

24. No blog: <http://gurstein.wordpress.com/2010/09/09/open-data-2-effective-data-use/>

5. interpretação/sentido — dados que só são acessíveis para o uso através de um intermediário técnico ou somente podem ser utilizados se ‘interpretados’ por um intermediário profissional;
6. ativismo— se os dados abertos governamentais estão em um formato e contexto que apoia seu uso em atividades de advocacy e ativismo social em nome de indivíduos e grupos marginalizados;
7. governança— se os processos relacionados a dados abertos governamentais incluem representação do público em geral em sua política de desenvolvimento e governança (não somente advogados, técnicos e funcionários públicos).

Intervir neste estágio relativamente inicial, através de designers de dados abertos ou programas e políticas do governo (ou de outros atores) – pode ajudar a evitar a exclusão e prevenir muitos dos efeitos negativos (e eventualmente os altos custos para sua correção) e oportunidades perdidas associadas à exclusão.

Minha sugestão – e esperança – seria que um mínimo de 10% das despesas com dados abertos do governo fossem direcionados para assegurar que não sejam criadas estruturas que determinem novas formas de exclusão como resultado de projetos de dados abertos governamentais. Contribuições para

a formação de capacidades para o uso dos dados, para a educação digital, para a criação de interfaces de design para usuários com deficiências, para apoiar atividades de advocacy com base em dados abertos, para assegurar que o projeto de dados abertos não seja dependente de ferramentas específicas, para ajudar na ampliação da participação dos cidadãos e cidadãs na governança dos dados abertos, entre outras medidas, seriam muito importantes para alcançar o objetivo de uma verdadeira inclusão informacional. ●

■ A exclusão informacional seria então a diferença entre aqueles que têm acesso e têm a capacidade de utilizar Dados Abertos Governamentais e aqueles que não têm nem acesso, nem capacidade.