A Governança da Internet em 2017: Hierarquias nacionalísticas versus redes multissetoriais?*

Wolfgang Kleinwächter, professor da Universidade de Aarhus. Ex-membro do Conselho da ICANN (2013-2015).

Data da publicação:

Abril de 2017

Dois eventos que ocuparam as manchetes do mundo digital em 2016 balizam a pauta da governança da Internet em 2017. No dia 1º de outubro de 2016 a supervisão das funções IANA passou a ser conduzida pela comunidade multissetorial representada na ICANN, com a expiração do contrato de supervisão entre esta entidade e o governo dos EUA.[2] Em 2 de novembro de 2016, o governo chinês anunciou a entrada em vigor de uma nova lei de segurança cibernética a partir do dia 1º de julho de 2017.

A Transição da IANA e a Lei Chinesa de Segurança Cibernética

A transição da IANA significa um processo no qual as políticas são formuladas a partir das bases. Por sua vez, a lei chinesa é uma abordagem governamental que se dá de cima para baixo. O novo estatuto da ICANN talvez não seja a versão mais avançada de um mecanismo multissetorial em prol de uma Internet livre, aberta e desfragmentada. A lei chinesa da segurança cibernética talvez seja a versão mais eloquente de como um país é capaz de controlar a Internet no interior de suas fronteiras territoriais. Aqui temos uma rede multissetorial global. Lá temos um governo nacional. E o governo chinês não é o único a aprovar uma legislação nacional forte para a Internet. Também o fazem Rússia, Turquia, Irã, Paquistão, Arábia Saudita, Hungria, Polônia, até mesmo o Reino Unido. Será que vamos ver surgir um novo tipo de conflito entre redes multissetoriais e políticas nacionais para a Internet? Será que a nova onda de nacionalismo vai alastrar-se pelo ciberespaço onde já não existem fronteiras? E com um novo nome agora ocupando o Salão Oval de Washington, será que a política do poder, pura e exclusivamente, vai atropelar a sabedoria coletiva? Será que as ficções vão ganhar dos fatos?

A resposta mais simples que se pode dar para essa pergunta retórica é: infelizmente “sim”. Sim, vamos continuar com os calafrios de uma “Ciberguerra Fria”. Sim, veremos que mais e mais governos, em nome da segurança, passarão a restringir direitos humanos individuais básicos tais como privacidade e liberdade de expressão. E sim, veremos que mais e mais governos querem renacionalizar o ciberespaço global e erguer fronteiras em torno do seu “segmento nacional da Internet” onde conseguem controlar indivíduos, empresas privadas, dados pessoais bem como o fluxo e o conteúdo da comunicação.

Entretanto, essa resposta curta só conta metade da verdade. A realidade é mais complexa. Qualquer tentativa de descrever o ciberconflito básico de nosso tempo como “democracias vs. ditaduras” seria simplória demais. Sim, existem conflitos entre estruturas políticas, sistemas de valores e ideologias. E sim, existem conflitos entre espaços demarcados (geridos por estados hierarquicamente organizados). Mas a verdade é que existem hierarquias nas redes e redes nas hierarquias. E não existe 100% de democracia de um lado e 100% de ditadura do outro.

Existem governos no mundo ocidental que preferem uma regulamentação forte para a Internet, argumentam que a segurança do ciberespaço é mais importante do que a proteção dos dados e reduzem qualquer compromisso que tenham com o modelo multissetorial a uma mera gestão técnica dos recursos da rede tais como nomes de domínio, endereços IP ou protocolos de Internet. Por outro lado, o governo chinês já reconheceu que o conceito de soberania no espaço cibernético, conforme insiste o presidente Xi, precisa levar em consideração também o papel dos atores não estatais. Observadores críticos reconheceram que, na 3a Conferência Mundial de Internet de Wuzhen, os conferencistas introduziram a terminologia da “governança quadripartite”, que é a versão chinesa do modelo multissetorial. A “governança quadripartite da Internet” convida a iniciativa privada, a comunidade técnica e inclusive a sociedade civil do país a participarem na formulação das políticas para a Internet. Até que ponto isso

vai traduzir-se na prática é o que se verá no futuro, mas trata-se de um passo interessante no bojo de uma linguagem de governança já ideologicamente sobrecarregada.

Em outras palavras, o que vimos em 2016 e o que já vemos em 2017 é uma mistura cada vez maior de posturas de amplo espectro, que vão desde um modelo multissetorial plenamente funcional como o da nova ICANN pós-transição da IANA até uma legislação nacional bastante rígida, simbolizada na nova lei chinesa de segurança do ciberespaço.

O Ecossistema de Governança da Internet como uma "floresta tropical"

No meu artigo sobre perspectivas da governança da Internet em 2014[3] comparei o ecossistema de governança da Internet a uma floresta tropical:

Na floresta tropical, um sem-número de plantas e animais diversos convivem no seio de um sistema muito complexo." Na "floresta tropical virtual", também temos uma diversidade cada vez maior de redes, serviços, aplicativos, regimes e outra propriedades que coexistem num mecanismo de interdependência de comunicação, coordenação e colaboração. Uma coisa que se pode aprender é que não há como gerir a floresta tropical. Ela não pode ser governada nem controlada, mas pode ser danificada e destruída. No ecossistema de governança da Internet, diversos atores com situações jurídicas muito distintas entre si atuam em diferentes camadas – nos níveis local, nacional e regional – movidos por inovação técnica, necessidades do usuário, oportunidades de mercado e interesses políticos.

Como resultado disso, vemos um processo muito dinâmico onde, a partir de uma ótica político-jurídica, surge uma ampla gama de regimes regulatórios, co-regulatórios ou auto-regulatórios, que coexistem, complementam-se ou entram em conflito uns com os outros. Como um todo, o sistema é descentralizado, diversificado e não tem autoridade central. Entretanto, no cerne dos vários subsistemas existe uma variedade incrivelmente grande de submecanismos distintos que vão desde estruturas hierárquicas controladas por um único governo ou sob controle intergovernamental até redes não hierárquicas baseadas em mecanismos auto-regulatórios de grupos não governamentais com uma ampla gama de acertos co-regulatórios no meio nos quais setores interessados – sejam eles do governo, da iniciativa privada, da sociedade civil ou da comunidade técnica – trabalham de mãos dadas.

Não existe uma solução única que atenda a todos os quesitos. A forma específica de cada subsistema precisa ser elaborada conforme necessidades muito específicas e de acordo com a natureza de cada questão. Havendo um mecanismo assim, a legislação tradicional de cada país e os acordos intergovernamentais continuarão desempenhando o seu papel, mas precisarão estar embutidos nos arcabouços já existentes e nos vários níveis das regulamentações. Assim, o princípio de "não causar dano" torna-se mais importante do que nunca. Significa que aquilo que os atores tanto governamentais quanto não governamentais fizerem na Internet precisará levar em conta as consequências diretas ou indiretas que tais atos terão sobre terceiros não envolvidos bem como o que os efeitos colaterais não intencionais acarretarão para o sistema como um todo.

Uma coexistência entre regimes e mecanismos de tal forma distintos e tão competitiva assim cria oportunidades, mas também riscos. Existem oportunidades incríveis para novos mecanismos, plataformas e serviços que possam trazer uma dinâmica maior para as estratégias políticas, as ações sociais e o desenvolvimento de mercados. Essa coexistência competitiva é capaz de estimular a inovação, promover a criação de empregos, aumentar todo tipo de atividade cultural e ampliar o uso das liberdades individuais pelo público em geral nos países tanto desenvolvidos quanto em desenvolvimento. Mas existe o risco de que as diferenças entre regimes e sistemas criem controvérsias e produzam conflitos pesados, dentre os quais a ameaça de impedir inovações, um abalo no desenvolvimento sustentável, uma redução das liberdades individuais e a poluição do ecossistema de governança da Internet de forma tal que algumas partes ficarão prejudicadas ou mesmo destruídas.

EUA vs. China: As chances de uma *détente* digital

Era o caso em 2014. E também é em 2017 e nos anos vindouros. O que precisa ser acrescentado hoje é que, entre os riscos que ora enfrentamos, também há o de uma "ciberguerra acirrada" com ciberarmas de verdade, uma guerra invisível de consequências incalculáveis e efeitos colaterais indesejados. O governo estadunidense já deixou claro que qualquer ciberataque sério contra a sua soberania ou infraestrutura crítica irá receber uma resposta forte. No dia 2 de dezembro de 2016, a Comissão sobre o Aprimoramento da Cibersegurança Nacional dos EUA, presidida por Thomas Donilon, apresentou o seu relatório ao Presidente Obama e este recomendou que o seu sucessor leve muito a sério as recomendações da comissão.[4]

Três semanas depois, em 29 de dezembro de 2016, a Administração do Ciberespaço da China (CAC)[5] apresentou a sua nova "Estratégia Nacional para a Segurança do Ciberespaço".[6] O documento diz que o uso da Internet "para traição, secessão, revolta, subversão, roubo ou vazamento de segredos de estado será castigado". Ele avisava também das punições por trabalhar com "forças estrangeiras" com vistas a "sabotagem, subversão ou secessão".

Acaso seria em preparação para uma luta iminente? Sim e não. Comparando os dois documentos, é possível se chegar a algumas conclusões interessantes. Existe de fato a grande probabilidade de uma corrida armamentista de hardware e de software, e também de sérios ciberconflitos sino-americanos em 2017. Mas também existem janelas abertas para o diálogo e a compreensão mútua. Ambos os artigos destacam a necessidade de se trabalhar em conjunto na luta contra os ciberterroristas e os cibercriminosos. E ambos querem promover a economia digital.

Em outras palavras, o confronto e a cooperação vão andar lado a lado. Existe muita desconfiança e há tanto interesses quanto valores conflitantes. Mas também existe uma disposição para o diálogo e para criar confiança no ciberespaço bem como para o respeito ao direito internacional na era digital. Para 2017, isso significa que as várias negociações e os vários diálogos multilaterais em torno da cibersegurança, tais como o trabalho do 5o Grupo de Especialistas Governamentais (GGE)[7] da ONU ora em andamento, estão agora mais importantes do que nunca. Contanto que haja canais de comunicação abertos, sempre haverá opções para se lidar com as polêmicas e para se chegar a algum acordo. E a nova "Comissão Global sobre a Estabilidade no Ciberespaço" (GCSC)[8], lançada em fevereiro de 2017 na Conferência de Segurança de Munique (MSC)[9], poderia tornar-se uma plataforma bastante útil para a construção de pontes, para combater as novas cibertensões e para abrir caminho para uma nova "*détente* digital".

Sequência infindável de negociações governamentais e não-governamentais

O cenário das grandes ciberpotências é uma realidade. Mas seria simplório outra vez reduzir a Agenda da Governança da Internet para 2017 à ciberrivalidade entre Estados Unidos e China. A cibersegurança, a economia digital e os direitos humanos são, entrementes, questões de alta prioridade para quase todos os países. E o assunto estará na pauta de vários encontros de cúpula política no ano de 2017.

Reuniões de Cúpula

Em 2016, a Cúpula do G7, rede das principais potências do mundo ocidental, adotou em Isa-Shima um documento especial para fortalecer a cibersegurança. Em 2017, a Itália detém a presidência do G7. A cúpula está prevista para o fim de maio de 2017, em Taormina. Em setembro do mesmo ano, haverá uma reunião especial dos Ministros do G7 para a Internet, em Torino, semelhante ao encontro que o Japão organizou em Takamatsu em abril de 2016. Em 2017, o G7 vai contar com novos líderes sentados à mesa de negociação. Resta saber quanto tempo e energia ainda detêm os países do G7 para ultrapassarem os acordos de Isa-Shima no que tange à governança da Internet. Em 2018, a presidência do G7 vai para o Canadá, um dos países que mais vêm apoiando o modelo multissetorial, há anos.

A cúpula dos BRICS, que reúne líderes da China, Rússia, Índia, Brasil e África do Sul, está marcada para setembro de 2017, na litorânea cidade chinesa de Xiamen. A reunião de cúpula dos BRICS de 2016 na cidade indiana de Goa prestou substancial apoio ao GGE da ONU destacando que "os estados têm o importantíssimo papel de assegurar a estabilidade e a segurança no uso das TICs". Mas também defenderam uma "Internet aberta, desfragmentada e segura, reafirmando que a Internet é um recurso global e que os Estados devem ter igual participação na sua evolução e funcionamento, levando em conta a necessidade de envolver setores relevantes na sua atuação e nas suas responsabilidades".[10] Pode-se questionar, porém, se a cúpula de Xiamen vai conseguir ir além dessa linguagem. Os BRICS, neste momento, passam por uma fase complicada. Brasil e África do Sul estão ocupados com problemas domésticos, Índia agora está apoiando o modelo multissetorial enquanto Rússia e China pensam diferente a respeito de transferir a "cibersoberania" para os canais da diplomacia internacional.

Também não está claro como a Organização de Cooperação de Xangai (SCO na sigla em inglês)[11] vai atender as questões cibernéticas. Os fundadores da SCO são a China, a Rússia e algumas das antigas repúblicas soviéticas. Agora, países como o Paquistão, o Irã e a Turquia estão parados na fila de espera. A cúpula da SCO está marcada para o mês de junho de 2017 em Astana, no Casaquistão.

A paz que resta entre ICANN e UIT?

O ano será novamente agitado para o pessoal da governança da Internet. Porém, após a transição da IANA e a renovação do mandato do IGF, não existe nada de significativo à espreita. O ano de 2017 provavelmente vai se tornar o "ano da transição", onde novos líderes políticos irão definir suas posições, novos mecanismos serão postos à prova do estresse e será elaborada uma nova pauta política, com vistas ao ano de 2020 em diante.

A ICANN fará três reuniões: em Copenhague (março), Joanesburgo (junho) e Abu Dhabi (outubro). Depois da transição da IANA, a ICANN tem agora a chance de voltar à sua atividade fim, que é a gestão do Sistema de Nomes de Domínio (DNS). Mais de mil novos gTLDs na raiz da Internet e mais de 25 milhões de novos nomes de domínio registrados dentro do novo programa gTLD não está mal. A concorrência funciona. Mas não é só o mercado que conta. A cada novo gTLD, a lista de problemas políticos relacionados e geralmente inesperados aumenta: .amazon, .africa, .gmbh, .vin são apenas alguns exemplos a nos dizer que, por trás de cada palavra, que agora aparece depois de um ponto, também existe um conflito político. Mas esse problema também é uma boa chance de demonstrar que o modelo multissetorial funciona, que aquilo que agora está no papel nos novos estatutos da ICANN passa na prova do estresse do cotidiano. E a ICANN deverá concluir este processo sob o chamado "Workstream 2": transparência das organizações de apoio e dos comitês consultivos, direitos humanos, jurisdição e outros.[12]

A Força-Tarefa de Engenharia da Internet (IETF)[13] também terá três reuniões: Chicago (março), Praga (julho) e Cingapura (outubro). Passo a passo, ela foi percebendo nos últimos anos que as questões técnicas com as quais lidam têm muitas implicações políticas, particularmente em relação à privacidade. Será interessante ver como em 2017 os programadores globais da IETF e outras organizações padronizadoras como a IEEE ou o W3C irão melhorar a cooperação com os legisladores de cada país. E isso continua sendo uma questão para cinco registros regionais da Internet (os RIRs)[14] que gerenciam o conjunto de bilhões de endereços IPv4 e IPv6, recurso que vem se tornando cada vez mais visado pelas normas internas de cada país.

Até agora, esses recursos se encontram em boas mãos da iniciativa privada e da comunidade técnica. O ano de 2016 já demonstrou que a UIT[15] e a ICANN poderão trabalhar juntas se respeitarem os seus domínios. Mas não se pode excluir que, nos anos vindouros, alguns governos na UIT tornem a tentar arrancar competências das mãos das organizações técnicas para colocá-las sob o regime de uma UIT intergovernamental. Alguns esforços durante a Assembleia de Padronização das Telecomunicações Mundiais da UIT (WTSA-16)[16] em outubro de 2016 na Tunísia emitiram incômodos sinais que têm o poder de perturbar o que alguns chamaram de "Paz de Busan". Em Busan, durante a Conferência Plenipotenciária da UIT de 2014, houve um acordo tácito que a UIT não vai mais tentar interferir nas atividades da ICANN, da IETF e dos RIRs. Mas essa paz é frágil, e algumas das antigas e falidas propostas podem ressurgir, agora recicladas.

Existem vários grupos de trabalho da UIT que lidam com políticas públicas relativas a questões da Internet. Esses grupos se abriram um pouco mais para o público, mas ainda estão longe de se tornarem mecanismos multissetoriais. Existe o Grupo de Estudo 20 da UIT-T, que lida com a Internet das Coisas. Esse órgão novo detém um mandato um tanto vago que também pode ser mal utilizado para uma reprogramação dos objetivos originais. E esse redirecionamento também é assunto para o Fórum da CMSI, organizado pela UIT. O mandato original para o Fórum da CMSI foi documentar o progresso nas Linhas de Ação da CMSI-16, adotado pelo Plano de Ação de Genebra de 2003. Mas, com o passar dos anos, o Fórum da CMSI foi além do seu bem demarcado território e adentrou o campo mais sensual da Governança da Internet. Conforme a Agenda da Tunísia, o Fórum da Governança da Internet (FGI/IGF)[17] é o principal local para se discutir assuntos relativos à Internet. A concorrência sempre é boa, mas com recursos limitados é melhor pensar duas vezes para ver se é necessário repetir o IGF através de um Fórum anual da CMSI, conforme combinado novamente para julho de 2017 em Genebra.

O Conselho da UIT fará sua reunião anual em maio de 2017. Pretende-se dar início aos preparativos para a Conferência Plenipotenciária da UIT 2018 em Dubai. Foi lá onde se realizou a fracassada Conferência Mundial de Telecomunicações Internacionais de 2012. Espera-se que não seja escrita na parede...

O que se faz necessário não é vinho antigo em garrafas novas; o que se faz necessário é uma melhor cooperação entre todos os setores envolvidos. O 2o Grupo de Trabalho sobre Cooperação Aprimorada (WGEC II) da Comissão de Ciência e Tecnologia para o Desenvolvimento (CSTD) da ONU poderia desempenhar um papel importante aqui, uma vez que precisa apresentar um relatório com recomendações para a 73a Assembleia Geral da ONU no segundo semestre de 2018, que ocorrerá justo antes da Conferência Plenipotenciária da UIT em

Dubai.[18] Uma primeira reunião foi realizada no final de janeiro de 2017, em Genebra. Será discutido um relatório interino durante a reunião regular da CSTD em maio de 2017. Com a transição da IANA, desaparece uma polêmica fundamental, que impedia todo e qualquer progresso do primeiro WGEC. O caminho agora deveria estar livre para se pensar e apresentar ideias inovadoras, e para aprimorar ainda mais a colaboração entre todos os setores, governamentais e não governamentais, dos países desenvolvidos e não desenvolvidos.

Existem muitos outros órgãos lidando com questões da governança da Internet, como a OMPI, a OMT ou a UNESCO, que realizarão em Paris a sua 39a Conferência Geral em novembro de 2017,[19] na qual irão discutir o progresso dos princípios ROAM (direitos, abertura, acesso e multissetorialidade) da UNESCO para a Governança da Internet desde a 38a Conferência em 2015.

A lista das importantes reuniões sobre a governança da Internet para 2017 é, mais uma vez, extensa. Começou em janeiro com o Fórum Econômico Mundial (FEM) em Davos, onde são discutidas questões como o crime cibernético, políticas digitais nacionais e a localização de dados. A Conferência de Segurança de Munique já mencionada analisou em profundidade a cibersegurança. Haverá reuniões da Freedom Online Coalition (FOC), que realizou sua 8a reunião em 2016 na Costa Rica, do projeto “Internet & Jurisdiction”, que teve uma ótima primeira reunião de alto nível em novembro de 2016 em Paris, e outra Conferência Mundial da Internet no segundo semestre de 2017 em Wuzhen, China. Haverá uma série interminável de simpósios acadêmicos, encontros de negócios e seminários técnicos nos níveis global, regional e nacional que irão produzir milhares de páginas de relatórios de pesquisa, propostas normativas e recomendações para ações futuras. E em 2017 deverão ser realizados cerca de 100 fóruns de governança da Internet nacionais e regionais. Encerrando o ano, em dezembro de 2017 o 12o FGI ocorrerá no Palais des Nations, em Genebra.

O Papel Fundamental do FGI

Olhando para o que já aconteceu, é possível dizer que o FGI amadureceu. Ele vem se tornando, cada vez mais, o que ninguém chegou a esperar em 2005 quando foi lançado: uma câmara de compensação para a normatização da Governança da Internet. Depois de onze anos, e com um mandato renovado até 2015, o FGI é agora o melhor lugar de fato para se iniciar uma discussão ou para se organizar a pressão em prol a formação de órgãos decisórios capazes de encontrar soluções para as questões que vão surgindo.
Durante o recente FGI em Guadalajara (dezembro de 2016), isso ficou demonstrado, dentre outras coisas, pelas sessões sobre a governança da Internet e pelas negociações do comércio. Ninguém discorda que o comércio, particularmente o e-comércio, seja um elemento fundamental para o futuro da economia digital. Fazem-se necessários acertos entre os países. Porém, até o momento, as negociações sobre a Internet e as negociações do comércio baseiam-se em duas culturas políticas bastante distintas. As discussões em torno da governança da Internet baseiam-se em processos abertos e transparentes onde todos os setores estão envolvidos a partir dos seus papéis respectivos e em suposto pé de igualdade. As negociações do comércio ocorrem entre governos, apenas a portas fechadas, com lobby muito forte dos grandes atores da iniciativa privada.

Para muitos dos palestrantes em Guadalajara, os fracassos da ACTA, da Parceria Transpacífica (TPP) ou da Parceria Transatlântica de Comércio e Investimento (TTIP) são resultado de um embate entre culturas. O bom de Guadalajara foi que todos os setores – negociadores governamentais para o comércio e seus oponentes das organizações de proteção ao consumidor, empresários e especialistas técnicos – tiveram uma chance de apresentar seus entendimentos, suas perspectivas e suas expectativas, e todos deram ouvidos a todos.

Tal nível de abertura e transparência é fundamental para identificar as áreas afins e para encontrar soluções que equilibrem interesses legítimos, porém conflitantes, com os quais, ao fim e ao cabo, todas as partes possam conviver. A discussão ajudou a ampliar a compreensão dessa nova complexidade.

Os processos multissetoriais decerto são mais difíceis, e provavelmente demoram mais. Porém, entre os participantes de Guadalajara pôde-se observar um reconhecimento cada vez maior do fato de que um processo inclusivo como esse há de aprimorar as oportunidades para que se encontrem soluções sustentáveis. E nas negociações de comércio da OMC, os governos não se mostraram capazes de atingir resultados mais rápidos entre si, atuando em um silo isolado. A Rodada de Negociações do Comércio de Doha permanece sem resultados concretos já há quase vinte anos.

Este exemplo é um bom indicativo das razões pelas quais o FGI é necessário, e também das razões pelas quais o Fórum não precisa de um mandato para fazer ele mesmo as negociações. É óbvio que se faz necessária uma nova rodada de negociações sobre o comércio global. E, no final das contas, serão os governos a tomar a decisão

final, de assinar e ratificar tratados. Mas as discussões multissetoriais abertas – como as que ocorrem no FGI – permitem que os especialistas dos governos sentados à mesa de negociações possam compreender melhor as várias perspectivas em conflito a fim de encontrar as concessões certas a serem feitas de parte a parte para que se alcance um desfecho sustentável. E permitem que os setores não governamentais ergam a voz, articulem interesses especiais e se tornem parte do processo.

Outro exemplo foi a discussão em torno da Internet das Coisas (IoT). Desde 2008, uma chamada Coalizão Dinâmica do FGI para a Internet das Coisas (DC-IoT) vem discutindo as questões da IoT, inclusive sua governança, privacidade e segurança. Em 2008, quando foi formada a Coalizão Dinâmica durante o 3o FGI em Hyderabad, Índia, a IoT meramente despontava no horizonte. Agora, em 2016, encontra-se no centro do debate sobre a Internet global. Em Guadalajara, a reunião do DC-IoT apresentou as perspectivas dos governos (Comissão Europeia, NTIA do Departamento de Comércio dos EUA, o Grupo de Estudo 20 da UIT-T), da comunidade técnica (IETF, ISOC), da iniciativa privada (ICC Basis, Oracle, Google) e grupos da sociedade civil que levantaram, entre outros temas, a necessidade de aprimorar também a compreensão que se tem das implicações éticas no desenvolvimento de novos serviços e dispositivos relativos à IoT.

O encontro não tirou um resultado concreto. Mas as questões levantadas na discussão foram alertas para que todos os presentes no salão abarrotado de gente de todas as partes e setores não fiquem só nos seus silos de interesse setorial onde se discutem questões da IoT junto a seus círculos mais fechados de especialistas, mas que sim saiam ao encontro de outros interessados e demais setores para falarem das suas práticas e aprenderem uns com os outros a aproveitar as novas oportunidades da IoT mantendo controle sobre os inerentes riscos de segurança e privacidade.

Um novo “grand design” para a agenda de governança da Internet

Em outras palavras, o FGI foi amadurecendo com o passar dos anos e acabou tornando-se uma plataforma de discussão que ajuda a formular pautas e a deitar bases para ação. Num mundo cibernético, onde a lista de questões novas e abertas cresce a cada semana, uma “estruturação do debate” desse porte, por si só, é um grande valor. Um tipo de estrutura capaz de permitir uma abordagem mais holística é dividir as dezenas de questões relativas à governança da Internet em quatro compartimentos diferentes. Isso ajuda a identificar áreas (“cestas”) onde se fazem necessários acordos formais e informais entre os vários setores (inclusive os tratados intergovernamentais) e quem deve discutir o que com quem, onde e como.

Cesta 1: Cibersegurança
Todas as novas ameaças à segurança nacional, os riscos de guerras cibernéticas, o surgimento das armas cibernéticas, a espionagem cibernética, a luta contra o ciberterrorismo e o cibercrime vão dominar a discussão em torno da Internet durante muitos anos daqui para frente. O FGI não será o lugar onde se negociarão as soluções. Mas, para que se compreendam todos os novos desafios da segurança cibernética, não bastará que especialistas governamentais se reúnam para tentar chegar a acordos relativos a novos tratados intergovernamentais. Será necessária a cooperação da comunidade técnica e da iniciativa privada, como bem demonstrou recentemente o caso entre o FBI e a Apple. E a sociedade civil também precisa tomar parte na discussão. Se os governos ignorarem os interesses de bilhões de usuários da Internet, todo e qualquer acordo intergovernamental em torno da segurança cibernética estará fadado ao fracasso, conforme já vimos com os acordos comerciais.

O órgão que surgiu nos últimos anos com a maior autoridade para as questões globais de segurança cibernética é sem dúvida o já citado GGE, que opera dentro do 1o Comitê da Assembleia Geral da ONU. Trata-se de um mecanismo puramente intergovernamental. Porém, seria sábio da sua parte ouvir com atenção o FGI e outras discussões multissetoriais e acatar as ideias e os argumentos razoáveis, que representam os legítimos interesses e perspectivas de setores não governamentais.

Cesta 2: Economia Digital
Não se deve esquecer que, por trás das estratégias políticas e valores culturais, existem os interesses econômicos. A economia digital é força motriz do crescimento econômico e da geração de empregos nos EUA, na China e no resto do mundo. Até 2020, mais dois bilhões de pessoas vão ingressar no mundo online. Quem vai atender esses novatos no mundo cibernético? Acaso serão as GAFAs norte-americanas (Google, Apple, Facebook, Amazon), ou as chinesas WeiBATs (Weibo, Baidu, Alibaba, Tencent), ou os novos grandes da Europa, Ásia, América Latina ou África?

Economicamente falando, não há como voltar à era pré-Internet. Conforme já mencionamos, um dos aspectos

fundamentais disso é o comércio. Mas o futuro da economia digital vai além do e-comércio. Nesse futuro estão incluídas – conforme propôs a recente Reunião Ministerial da OCDE em Cancun (junho de 2016) – as e-skills (capacitação cibernética) e os e-jobs (empregos cibernéticos), a indústria 4.0 e os vários outros aspectos. Na reunião de cúpula do G20 em Hangzhou em setembro de 2016, os líderes dos 20 maiores países adotaram a "Iniciativa de Desenvolvimento e Cooperação sobre Economia Digital".[20] Trata-se de uma iniciativa que ainda está mal definida, em seu estágio inicial. Porém, estando ligada às recomendações da conferência da OCDE de Cancun, tem grande potencial para ajudar os países a definirem as estratégias para a sua economia digital e a identificarem novas áreas para cooperação digital global.

Em 1º de dezembro de 2016, a Alemanha assumiu a presidência do G20 para 2017. A cúpula do G20 está marcada para julho de 2017 em Hamburgo. Em abril de 2017, será realizada uma reunião especial dos ministros responsáveis pela economia digital com uma conferência multissetorial especial marcada para a véspera.

Tal qual ocorre no campo da segurança cibernética, o FGI não deverá tornar-se o órgão de negociação para a economia digital global. A OMC, o G20, a OCDE e outros órgãos intergovernamentais têm legitimidade e autoridade para transformar discussões em decisões. Mas isso não exclui os setores não governamentais da normatização e do processo decisório da economia digital. Um bom exemplo é, novamente, a OCDE. Lá, os setores não governamentais encontram-se organizados em quatro comitês consultivos: negócios (BIAC), sindicatos (TUAC), comunidade técnica (TAG) e sociedade civil (CSISAC). Todos eles participaram da elaboração dos documentos finais de Cancun, e suas contribuições foram extremamente úteis na formulação de estratégias como e-skills e e-jobs.

Cesta 3: Direitos Humanos
A proteção aos direitos humanos na era digital está mais importante do que nunca. Nunca se viu na história da humanidade risco maior de perda da privacidade e do direito à livre expressão. Conquistas importantes foram consagradas nos últimos anos. O Conselho da ONU para os Direitos Humanos adotou uma resolução confirmando que os indivíduos têm os mesmos direitos dentro e fora da rede cibernética. Grande passo também foi a adoção da de uma declaração consensuada de princípios de governança da Internet no Encontro NETmundial em São Paulo, em abril de 2014,[21] que colocou os direitos humanos no topo dos seus oito princípios. Mas também testemunhamos uma quantidade cada vez maior de violações dos direitos humanos no ciberespaço. Recentemente, a IPS noticiou que, em 2016, dezenas de países aprovaram medidas internas de censura restritiva.[22] E a prática cotidiana do vigilantismo continua.

Não é preciso introduzir novos direitos humanos. Mas há necessidade, sim, de aprimorar a compreensão que temos de como implementar na era digital os direitos humanos já consagrados. A Coalizão Dinâmica do FGI sobre Direitos e Princípios produziu um bom documento que pode ser usado como diretriz para melhorar essa compreensão. Existem projetos como o Marco Civil brasileiro ou a Carta de Direitos da Internet italiana. Recentemente, foi apresentada ao Parlamento Europeu uma iniciativa alemã para uma Carta Europeia dos Direitos Digitais.

Contudo, mais esforços ainda se fazem necessários. Com seus relatores especiais para a liberdade de expressão na era digital, o Conselho da ONU para os Direitos Humanos é um forte mecanismo capaz de fazer muito no sentido de destacar ou de envergonhar governos e empresas caso venham a violar os direitos humanos no ciberespaço. Existem vários vigilantes nesse campo, como os Repórteres Sem Fronteiras, a Human Rights Watch e outros mais. O ano de 2019 marcará o quinto aniversário do importante encontro multissetorial NETmundial. Talvez seja uma boa ideia a comunidade multissetorial produzir um relatório abrangente sobre a implementação dos princípios de São Paulo. O NETmundial+5 poderia ser realizado em cooperação com o 14o FGI em 2019.

Cesta 4: Tecnologia
A Internet, por si só, é uma inovação técnica. Mas neste meio tempo, existem tantos produtos, dispositivos e serviços inovadores surgindo além da Internet e do seu DNS que o desenvolvimento tecnológico como tal já se tornou uma questão central. Hoje em dia, a Internet das Coisas, a Computação na Nuvem e a Inteligência Artificial já estão no centro da discussão. Ninguém sabe quais serão as invenções do amanhã, nem que aspecto terá a próxima geração de questões. É importante contar com um ambiente multissetorial para a condução das discussões acerca dessas novas questões. O FGI pode funcionar aqui como um sistema de alerta previdente, onde tanto as oportunidades para o surgimento de novas tecnologias quanto os seus inerentes riscos e ameaças possam ser discutidos.

Olho no futuro: tudo está ligado a tudo

O 11o FGI em Guadalajara ajudou a estruturar a agenda da governança da Internet para o ano de 2017 em diante. Mas também ajudou a abrir nossos olhos para compreender melhor que, no mundo da Internet, tudo está conectado a tudo. Isso significa que tanto as questões de cibersegurança quanto as questões relativas à economia digital ou aos direitos humanos já não podem mais ser discutidas em separado. Tomando apenas um exemplo: a Internet das Coisas, uma questão técnica, é fundamental para a economia digital. Mas se passarmos dos carros sem motoristas para tanques sem condutores, a mesma tecnologia se torna uma questão de cibersegurança. E o seu impacto sobre a nossa privacidade individual é imenso.

Noutras palavras, se pensarmos no futuro, será preciso montar discussões e negociações globais sobre a governança da Internet sobre um mecanismo capaz de refletir essas interconexões universais. Isso de fato requer uma normatização inovadora. A Internet é a rede das redes, conectada através de protocolos técnicos universais. O que precisamos no campo da normatização é uma rede de redes semelhante de políticas, onde vários órgãos, plataformas e regimes estejam interconectados através de algo como um “protocolo político” universal.

O ciberespaço ainda é território ainda sendo mapeado, aberto à criatividade e à inovação. Mas é um bem comum que pertence a toda a humanidade. Não existe alternativa à cooperação global entre todos os setores, tanto dos países desenvolvidos quanto dos países em desenvolvimento. Esforços nacionais solitários ou a tradicional política do poder não irão trazer soluções, mas têm o potencial de jogar o mundo numa turbulência muito séria. Será que aprendemos alguma coisa com a história?

Nos meus tempos de estudante, em dado momento assisti a uma aula de um velho professor que falava sobre “Os Sete Saltos na História da Humanidade”. Ao mudar do passado para o futuro, ele ilustrou o argumento contando-nos que a humanidade agora se encontra numa canoa que desce em direção a uma enorme cachoeira. E fez uma breve pausa antes de nos dar a sua recomendação: “Não briguem com a cachoeira; procurem estabilizar a canoa!”

--
* 1. Adaptado do texto original publicado em CircleID: http://www.circleid.com/posts/20160106_Internet_outlook_2017_nationalist.... Publicado com autorização do autor.

2. Para informações detalhadas sobre as funções IANA e a transição mencionada, ver D.R.Canabarro, E.T.Rodrigues, “A transição IANA chegou à outra margem do Rubicão”, poliTICs 23, https://politics.org.br/edicoes/transi%C3%A7%C3%A3o-iana-chegou-%C3%A0-o...

3. Wolfgang Kleinwächter, “Internet Governance Outlook 2014: Good News, Bad News, No News?”, CircleID, dezembro de 2013, http://www.circleid.com/posts/20131231_internet_governance_outlook_2014_...

4. O relatório pode ser obtido em https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecur...

5. Ver https://en.wikipedia.org/wiki/Cyberspace_Administration_of_China

6. O documento em inglês pode ser obtido em https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cybersp...

7. Ver https://digitalwatch.giplatform.org/processes/ungge

8. Ver https://cyberstability.org

9. Ver https://www.securityconference.de/en

10. Ver http://indianexpress.com/article/india/india-news-india/8th-brics-summit...

11. Ver http://www.sectsco.org

12. Ver https://community.icann.org/display/WEIA/WS2+-+Enhancing+ICANN+Accountab...

13. Ver http://ietf.org

14. Ver https://www.nro.net

15. Ver http://www.itu.int/en/Pages/default.aspx

16. Ver http://www.itu.int/en/ITU-T/wtsa16/Pages/default.aspx

17. Ver http://www.intgovforum.org/multilingual

18. Ver http://unctad.org/en/Pages/CSTD/WGEC-2016-to-2018.aspx

19. Ver https://en.unesco.org/events/general-conference-39th-session

20. Ver http://www.china.org.cn/world/2016-09/28/content_39392786.htm

21. Ver http://netmundial.br/pt

22. Ver http://www.ipsnews.net/2016/12/more-than-50-internet-shutdowns-in-2016

Categoria:

- poliTICs 25