Editorial PoliTICs 27

Esta edição da PoliTICs expõe alguns dos principais desafios para o cultivo da Internet democrática e voltada ao exercício de direitos e justiça social. Da regulação de serviços “over-the-top” aos riscos de terrorismo facilitados pelo avanço das tecnologias da informação e da comunicação, além de uma extensa análise sobre as possíveis abordagens para a governança da Internet, articulando aspectos técnicos e políticos.

Nesta edição, publicamos dois ensaios e um prêambulo sobre serviços “over-the-top” (OTTs): o último busca contextualizar as atuais disputas em torno do conceito e como elas podem impactar em sua regulação. Você pode não ter ouvido falar em OTTs como esse conjunto de letrinhas, mas elas constituem algumas das mais famosas aplicações que utilizamos cotidianamente nas redes. Nosso preâmbulo procura elucidar sobre o que são e como a União Internacional de Telecomunicações (UIT) os definiu recentemente, buscando trazer, para seu colo, a responsabilidade de regulá-las – ao menos em parte. O texto institucional do Observatorio Latinoamericano de Regulación, Medios y Convergencia, um *think tank* latinoamericano que integra a iniciativa da Fundación Libertis, propõe um conjunto de 10 diretrizes para a regulação desses serviços, de forma a garantir o exercício de direitos humanos, diante da crescente importância e do impacto desses provedores de serviços na sociedade. A advogada da PROTESTE Flávia Lefèvre, por sua vez, defende que precisamos mais de aplicação das leis atuais do que da aprovação de novas regulações – uma vez que já dispomos de uma série de instrumentos regulatórios que não têm sido observados.

Wolfgang Kleinwächter, Professor Emérito da Universidade de Aarhus, ex-membro do Conselho da ICANN, analisa o reequilíbrio entre o papel das organizações políticas e as técnicas no ecossistema global de governança da Internet, em um contexto de crescente importância das primeiras na definição de políticas públicas. Apresenta as abordagens multissetoriais que envolvem setores governamentais e não-governamentais, bem como iniciativas inovadoras que promovem uma “colaboração mais estreita entre criadores de código e criadores de leis”. Kleinwächter nos apresenta uma valioso mapa de áreas temáticas da governança da Internet e em que organizações – tanto técnicas como políticas e/ou governamentais – elas são debatidas.

Zach Aysan, cientista especialista em cibersségurança dedicado à defesa de melhor qualidade de vida nas cidades e membro da iniciativa comunitária CityAction em Toronto, nos apresenta novos problemas de cibersségurança causados pela transformação de carros em computadores. “Se hackear um jipe é tão simples quanto hackear um servidor, e os servidores são rotineiramente violados, então onde estão todos os carros hackeados?” Os veículos autônomos abrem brechas extremamente sensíveis para a segurança das pessoas. Aysan chama então a atenção das autoridades para o risco premente de carros, que são hoje computadores, serem hackeados e tornarem-se armas. À primeira vista, sua hipótese pode parecer exagerada, ou mesmo um roteiro de ficção científica, mas Aysan apresenta elementos muito concretos para sustentar sua preocupação e a necessidade de os governos tomarem medidas para prevenir ataques cibernéticos por meio do uso de máquinas como carros.

Boa leitura!

Terroristas poderiam usar Teslas para matar-nos[1]

Uma guerra no campo da ciberssegurança dos carros autônomos está chegando. O que pode ser feito para ganhá-la.

Zach Aysan – cientista especialista em ciberssegurança dedicado à defesa de melhor qualidade de vida nas cidades; membro da iniciativa comunitária CityAction em Toronto, Canadá.

Em uma calma manhã de sábado em agosto do ano que vem, subitamente, em todo o país, 12.000 sedãs Tesla Modelo S ligam ao mesmo tempo. Com o piloto automático ativado, saem para a estrada. Alguns deles chegam aos postos de gasolina locais. Outros dirigem-se a subestações elétricas. Chegam a seus objetivos em velocidade máxima. As baterias do Modelo S explodem espetacularmente com as colisões, incendiando tudo na área. A rede elétrica de Los Angeles é derrubada quase imediatamente. Surgem centenas de incêndios. A América está sob ataque.

Isso parece ficção científica. Mas não é.

Com a segurança cibernética, a primeira coisa a entender é que a Internet é ingovernável porque a localização é irrelevante e a identidade é ocultável. Isso ocorre por padrão – é a Internet, onde supostamente todos podemos conversar com todos, e não foi projetada no nível do protocolo para exigir pagamento ou identificação.

Os cibercriminosos cometem erros e são presos ocasionalmente, mas os ataques podem se vir de nações que não cooperam com instituições internacionais ou de governos estrangeiros. E fora do mundo desenvolvido, há sempre uma distinção ainda menor entre indivíduos privados e atores estatais: um especialista em segurança de software pode trabalhar para enriquecer uma empresa criminosa ou a si mesmo e também trabalhar para o serviço de inteligência de seu governo. Isso torna a cooperação internacional ainda mais difícil.

A segunda coisa a reconhecer sobre segurança cibernética é que o ataque é muito mais fácil que a defesa. Os invasores podem sondar vários pontos, como computadores ou servidores previamente invadidos, alugados com informações de cartão de crédito roubadas. Eles podem pacientemente tentar estratégias diferentes até conseguirem. Invasores talentosos podem primeiro inventar um novo método de ataque e então escrever software para sondar servidores ou o tráfego de Internet, para criar uma lista priorizada de organizações potencialmente vulneráveis e só então começar a violá-las sistematicamente.

Um defensor, por outro lado, é um alvo à espera. Seu aplicativo é voltado para o público, com URLs,[2] domínios e centros de dados que qualquer pessoa pode investigar. Ele possui um conjunto consistente e detectável de sistemas operacionais, linguagens de software e bibliotecas que são tão bem compreendidas pelos potenciais adversários quanto pela equipe interna responsável por administrá-las.

E um defensor só tem que cometer um erro: um único ponto de entrada incorretamente protegido permitirá o acesso aos atacantes. Defender todos os pontos de entrada e mantê-los perpetuamente defendidos, apesar das mudanças nos requisitos organizacionais, de pessoal e de um fluxo interminável de atualizações de vulnerabilidades para bibliotecas de software, é praticamente impossível. E mesmo as organizações que têm a competência técnica e os recursos para se defender contra ataques persistentes, como a NSA, por exemplo, correm o risco de uma violação ou vazamento crítico por alguém de dentro. A superfície de ataque é enorme e a ameaça é persistente. Se você não puder prender os invasores e os invasores tiverem o tempo que precisarem para encontrar vulnerabilidades, a pergunta não é se o sistema pode ser violado – é quando o sistema será penetrado. E o que os invasores farão quando o penetrarem.

Quando um sistema é penetrado, um invasor suficientemente preparado pode usar software pronto para atingir objetivos prioritários. Por exemplo, um *malware* que ataca uma plataforma de varejo pode inicialmente extrair listas de senhas e chaves criptográficas primeiro e só depois coletar informações, como o histórico de compras. Quando um invasor começa a suspeitar que suas atividades foram percebidas, ele pode criptografar os discos rígidos do servidor comprometido antes de devolvê-los a seus proprietários. Bem-vindo ao futuro cyberpunk: é mais estranho e menos sombrio do que se poderia esperar, mas os

---

[1]Publicado originalmente em *http://www.weeklystandard.com/terrorists-could-use-teslas-to-kill-us/article/2011171*. Reproduzido com permissão. Notas de rodapé são da editoria da **poliTICs**.

[2]Sigla de "Uniform Resource Locator" – designa endereços mnemônicos de serviços Web na Internet.

hackers têm organizações reféns em pânico lutando para pagar resgates em criptomoedas. Eu sei. Sou um dos que ajudam essas organizações durante as crises.

Nos anos 90, como um jovem irresponsável, eu hackeei computadores ilegalmente por diversão, antes de começar a escrever softwares comerciais críticos para a segurança de empresas de telefonia. Minha experiência inicial com criptomoedas e o trabalho como *whitehat*[3] atraiu empresas vítimas de *ransomware*.[4] Eu os ajudo a entender suas opções e os passos que eles precisam dar para colocar seus sistemas em funcionamento, com estratégias de mitigação para a próxima vez. (Se você está lendo isso e precisa de ajuda, desculpe, eu só presto serviços através de contatos pessoais para evitar ser alvo de cibercriminosos. Também não tenho mais criptomoedas pelas mesmas razões.)

Mesmo os defensores mais dedicados têm algumas vulnerabilidades. Os tipos mais perigosos são conhecidos como "vulnerabilidades de dia-zero" porque são fragilidades básicas no software que ninguém – nem mesmo os programadores originais – sabia que existiam. O dia-zero mais famoso é provavelmente o Heartbleed, uma falha de segurança em uma biblioteca amplamente usada chamada OpenSSL, que depois de descoberta causou pânico em várias organizações enquanto os administradores de sistemas procuravam corrigir a falha.[5] Como exemplo da gravidade desse risco, hackers utilizando as brechas do Heartbleed roubaram as chaves de segurança de um grande sistema hospitalar dos EUA, colocando em risco a privacidade de 4,5 milhões de registros de pacientes.

A terceira coisa a ser entendida sobre segurança cibernética é que certas classes de ataques cibernéticos, incluindo a maioria das vulnerabilidades de dia zero, podem quebrar todas as instâncias do mesmo sistema ao mesmo tempo. Por exemplo, enquanto seriam necessários dois mísseis separados para destruir dois drones predadores separados, uma vulnerabilidade de software pode ser explorada por um vírus que desative ambos os mísseis simultaneamente. Foi assim que o vírus do tipo *ransomware* WannaCry conseguiu infectar centenas de milhares de computadores, incluindo máquinas críticas usadas em hospitais no Reino Unido.[6]

E uma vez que os atacantes controlam um sistema, pode ser muito difícil recuperá-lo. Os dados viajam muito rapidamente. Um servidor em Austin, Texas, leva cerca de 140 milissegundos para enviar dados para um servidor em Tóquio. O que isto significa é que, se você confiar no julgamento humano durante um ataque para proteger um sistema desconectando-o, talvez seja tarde demais porque os dispositivos comprometidos podem desvincular-se do controle remoto. Um telefone hackeado, por exemplo, pode ter seu programa de controle de rede modificado para passar todas as informações por meio de uma VPN[7] controlada por um atacante. E sem contramedidas previamente configuradas pelo fabricante do telefone, as instruções para atualizar o software vulnerável do telefone podem ser automaticamente bloqueadas, resultando em um dispositivo permanentemente comprometido.

Para reiterar, aqui estão nossos três preceitos:

1) A Internet é anárquica. É difícil atribuir ataques e, mesmo quando possível, a divulgação pública desses ataques revela fontes e métodos.

2) A defesa cibernética é extremamente difícil, especialmente com o tempo, à medida que as organizações mudam.

3) Algumas classes de ataques cibernéticos permitem o controle de todas as instâncias de um dispositivo e, com o planejamento correto, podem impedir o acesso ao proprietário do dispositivo comprometido.

O que nos leva à interseção entre os computadores e o mundo real.

Em 2010, uma equipe de pesquisadores descobriu o Stuxnet, um vírus escrito em uma colaboração conjunta entre Israel e os Estados Unidos para interromper o programa de armas nucleares iranianas.[8] Embora os iranianos tenham tomado medidas para garantir que seu equipamento de processamento de material nuclear não estivesse conectado à Internet, o vírus foi levado à instalação em um pendrive. Uma vez que o Stuxnet assumiu o controle, alterou sutilmente a operação das centrífugas da instalação para que

---

[3]Expressão que denota um hacker bem-intencionado.

[4]Ataque a computadores ou redes que bloqueia os serviços ou sistemas até que um resgate seja pago ao atacante.

[5]Ver, por exemplo, *https://en.wikipedia.org/wiki/Heartbleed*

[6]Ver *https://en.wikipedia.org/wiki/WannaCry_ransomware_attack*

[7]Sigla de "Virtual Private Network", conexão ponto-a-ponto criptografada entre dispositivos de rede.

[8]Ver *https://pt.wikipedia.org/wiki/Stuxnet*

elas se destruíssem lentamente, de forma aparentemente inexplicável, sem revelar a presença do *malware*.

O Stuxnet ensinou ao mundo da segurança cibernética duas coisas: primeiro, os vírus não são apenas ferramentas de inteligência – são ferramentas de guerra. Segundo, se um computador está ou não conectado à Internet é mais um fator do que algo decisivo. O programa de armas iraniano pode ser bem secreto, mas é vulnerável a um pendrive; um perfil no Twitter pode ser muito ativo, mas ainda assim pode ficar offline ocasionalmente. E os dados podem ser extraidos através de uma infinidade de métodos.

Com os avanços no aprendizado por máquina, os dados podem ser analisados e filtrados localmente, de modo que uma conexão com baixa velocidade ou alta latência deixe de ser uma barreira. Por exemplo, um atacante pode usar técnicas de conversão de voz para texto nos vídeos internos de uma empresa e apenas extrair as frases que mencionem palavras-chaves críticas para sua pesquisa.

E para mostrar como é complicada é essa "floresta de espelhos", considere que o Kaspersky Lab, o grupo de pesquisa que descobriu o Stuxnet, foi recentemente classificado pelo Departamento de Segurança Interna dos Estados Unidos como tendo ligações com o FSB russo, o substituto pós-soviético da KGB. Então, talvez a descoberta do Stuxnet pelo Kaspersky não tenha sido apenas um presente acidental para os iranianos, afinal.

Nos últimos 20 anos, uma infinidade de dispositivos de nosso dia-a-dia tornaram-se computadores. As geladeiras são agora computadores. Os relógios são agora computadores. Até mesmo coisas como sensores de uso único empregados para garantir o endurecimento correto do concreto são agora computadores.

Carros também são agora computadores.

E eles são tão seguros quanto computadores em qualquer outro lugar. Em 2015, o jipe foi hackeado e a montadora teve que enviar milhões de pendrives para reparar o software automotivo.[9] Mas por que apenas o jipe? Se hackear um jipe é tão simples quanto hackear um servidor, e os servidores são rotineiramente violados, então onde estão todos os carros hackeados? É algo um pouco parecido com o Paradoxo de Fermi.[10]

A explicação é provavelmente uma mistura de fatores. Pode ser que os pesquisadores de segurança não estejam prestando atenção suficiente aos carros. Pode ser que os *blackhats* não estejam motivados para atacar veículos porque o retorno do investimento não valha a pena. Pode ser que hackers tenham problemas para adaptar técnicas que funcionam em servidores e computadores pessoais para carros, porque a área de ataque é menor. Ou a resposta poderia ser mais sinistra. O Uber escondeu uma violação de dados de 57 milhões de usuários, pagando os hackers.[11] Talvez as empresas automotivas tenham feito o mesmo em silêncio.

Os engenheiros estruturais definem o limite de flexão[12] que uma viga ou ponte pode sofrer durante a carga esperada, não porque os próprios desvios sejam necessariamente inseguros, mas porque esperam que as pessoas relatem de forma confiável quando as coisas parecem erradas – e se flexões grandes, mas seguras, são rotineiras; flexões grandes, mas inseguras, podem não ser reportadas. Os engenheiros estruturais também fazem cálculos estruturais mais conservadores quando os sistemas podem não exibir fraqueza potencial antes da falha.

Você deve pensar nos computadores da mesma maneira.

Computadores atingidos por *malwares* sofisticados não mostram sinais de infecção. Mesmo que um ataque requeira vários estágios ou computadores intermediários, como o Stuxnet, os vírus bem programados são invisíveis. Todo software, incluindo um vírus, é apenas código, código significa dados, e dados não mudam a forma como percebemos o computador em que ele reside, a menos que o software no computador esteja preparado para perceber a mudança.

E agora vamos às coisas assustadoras. Lembre-se do nosso terceiro preceito: que algumas classes de ataques cibernéticos comprometem todas as instâncias de um dispositivo.

Pensamos em Teslas como carros, assim como pensamos em um iPhone como telefone, mas uma explicação mais precisa da realidade é que eles são apenas computadores. Um leva você pelos caminhos enquanto o outro fica no seu bolso, mas isso é basicamente a soma da diferença. Não importa o quão estranho possa

---

[9]Ver *https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway*

[10]Ver *https://en.wikipedia.org/wiki/Fermi_paradox*

[11]Ver *https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach*

[12]Ver *https://en.wikipedia.org/wiki/Deflection_(engineering)*

parecer para um leigo, para um desenvolvedor de software a semelhança entre os dois é tão óbvia que nem vale a pena mencionar: eles são apenas sistemas operacionais em uma peça de hardware.

O que significa que algo como o WannaCry é tão possível para o Teslas quanto para os hospitais. Ambos são hackeáveis, e em escala.

Há outra diferença, é claro: o seu iPhone não pode mover-se por si mesmo. Mas um veículo autônomo, como um Tesla, que bate em uma fábrica de produtos químicos, em um subsistema elétrico, um duto de petróleo ou posto de gasolina correndo a 200 km/h pode causar muitos danos.

Agora vamos combinar esses dois pensamentos. O que aconteceria se alguém hackeasse milhares de carros autônomos de uma só vez e os transformasse em armas?

Nada de bom mesmo.

Um dos problemas que tive no último ano e meio é como comunicar essa ideia sem soar como um maluco ou péssimo ator.

Quando percebi isso pela primeira vez há um ano e meio, informei o Ministério de Segurança Pública do Canadá. Um ano depois, encontrei-me com o parlamentar federal de meu distrito[13] para descobrir que esforços estávamos propondo para mitigar a ameaça em potencial. Descobri que não havia apenas regulamentações sobre veículos autônomos, mas também não havia planos de criar regulamentos.[14]

Depois de conversar com a maioria dos principais fabricantes de carros autônomos, incluindo Tesla, BMW, GM e Toyota, percebi que os tomadores de decisão em grandes empresas automotivas, tal como os desenvolvedores de *start-up*s de software, não têm uma solução mágica.

Eles sabem que precisam de tecnologia de condução autônoma para competir no mercado. Eles também sabem que estão expostos. No momento, sua principal defesa é a obscuridade de sua plataforma, o que significa que, quanto mais bem-sucedidos eles se tornam, mais vulneráveis eles estarão. Não é uma posição confortável.

Ademais, a maioria dos desenvolvedores de software realmente não pensou simultaneamente em dirigir carros e na segurança cibernética, e ele pouco sabem sobre as interfaces vulneráveis dos sistemas elétricos automotivos.

O que isto significa é que temos tempo. Essas explorações não são difíceis para organizações como a NSA, mas não são algo que o ISIS ou a Coreia do Norte sejam capazes de dominar facilmente. Estamos expostos, sim, mas o céu não está caindo. Temos tempo para criar os regulamentos e acordos internacionais corretos – se pudermos incentivar a vontade política e agir.

Existem várias maneiras de abordar a segurança de veículos autônomos, mas vamos começar com uma avaliação franca do que não funcionará:

1) Confiar em software antivírus do mercado. O único antivírus que deve ser confiável é aquele que vem com o sistema operacional.

2) Utilizar dispositivos autônomos. Vírus Bluetooth que viajam através de lâmpadas inteligentes, dispositivos de depuração em sua oficina automotiva local, ou simplesmente erros antigos (como as vulnerabilidades em rádios definidos por software), são lacunas via rádio que não podem ser garantidas. As instalações nucleares iranianas estavam isoladas e isso não impediu o Stuxnet e a CIA, então não vamos achar que estamos protegido contra ataques da RPDC.

3) Revisão de código. Quando os governos ocidentais constroem seus sistemas de segurança, eles geralmente dependem de peças de hardware construídas na China. A "segurança" desses componentes é certificada pela inspeção estatística do código embarcado em um punhado de amostras.

Mas enquanto o governo britânico pode revisar o código de equipamentos de rede chineses em Banbury, Oxfordshire, se houver uma guerra total com os chineses eles provavelmente terão que substituir tudo isso por material americano. Porque a menos que você inspecione cada componente individual que você recebe de um fornecedor, e ele tenha um código fisicamente inalterável, você não tem ideia de qual código está realmente sendo executado em seu sistema.

O principal impedimento contra um fornecedor chinês, como o fato de a Huawei inserir *malware* em seus

---

[13]No regime parlamentarista do Canadá o voto é distrital.

[14]Ver *http://www.cbc.ca/news/business/autonomous-vehicles-self-driving-cars-uber-google-general-motors-1.4287591*

produtos, é a perda de prestígio comercial - considerações de mercado que são discutíveis quando se trata de estabelecer prioridades estratégicas na guerra.

4) Confiar nas empresas automotivas. Equifax e Ashley Madison estavam em segurança. Até que deixaram de estar. A segurança nacional não é algo a ser confiado a corporações e certamente não a corporações de países com histórico ruim de segurança cibernética, como a China. O capitalismo recompensa invenção e risco, não mitigação de risco de longo prazo.

5) Certificação de componentes individuais ou veículos. A regulamentação detalhada e prescritiva e a certificação individual são muito lentas em relação ao ritmo acelerado do desenvolvimento moderno de software. Nossas corporações mais seguras atualizam seu código várias vezes por dia. Este não é apenas um artifício correlativo de empresas de tecnologia bem administradas – é causal. O primeiro agente a encontrar uma vulnerabilidade geralmente é a organização responsável pelo serviço ou dispositivo e ele trata de corrigir o problema o mais rapidamente possível.

Em vez disso, os regulamentos devem ser funcionais. Por exemplo, uma máxima como "dados nunca devem ser lidos por um dispositivo intermediário de rede" ou "nenhuma ação executada no computador de acesso deve alterar o estado do computador de controle" de modo que multas e recompensas de segurança não sejam arbitrárias, mas empresas automotivas possam ainda competir na velocidade de seu avanço tecnológico.

6) Permitir que o mercado leve em conta ataques cibernéticos em larga escala como parte do cálculo do seguro automotivo existente. Com todo o respeito, as seguradoras não têm nem os dados nem a experiência para efetivamente estimar esses riscos. A distribuição de Poisson[15] é maravilhosa, mas os vírus de computador invalidam todas as classes do mesmo sistema ao mesmo tempo – portanto, essa técnica estatística não deveria ser usada como base para avaliar ou prever ataques. Sem independência estatística, as vulnerabilidades dessa escala não podem ser precificadas com precisão porque é impossível obter probabilidades precisas da ocorrência de um evento-surpresa. Engenheiros civis projetam para uma tempestade destrutiva em 100 anos. Como seria um ataque cibernético destrutivo em 100 anos? Ninguém sabe.

7) Esperar que veículos autônomos sejam usados em ataques de pequena escala antes de elaborar a legislação. Se esperarmos por tal ocorrência, a legislação resultante provavelmente será direcionada para ataques de pequena escala e não focada no risco maior. Nossa primeira preocupação deve ser sobretudo a segurança nacional (hacks em larga escala de frotas inteiras), não apenas alvos específicos (hacks de carros individuais).

Então, o que funcionaria? Políticas eficazes devem começar com o reconhecimento de que os governos não conseguirão regular de maneira inteligente o problema. Um esforço bem financiado e de código aberto com recomendações claras será a maneira mais eficaz de proteger o veículo sem motorista.

1) Os profissionais de software devem educar e encorajar os engenheiros elétricos e mecânicos a apresentar propostas que ajudem as empresas de veículos autônomos e os governos a proteger o público.

2) As comunidades de inteligência e de controle de armas devem ajudar na elaboração de acordos internacionais para tornar ilegal o ataque cibernético de sistemas civis durante a guerra sob leis internacionais - e precisamos de especialistas jurídicos para elaborar regulamentos de referência que países menos avançados tecnicamente possam usar como base.

3) Nossos acordos comerciais devem refletir a natureza mutável de nossa interdependência. A China anunciou recentemente que empresas automotivas estrangeiras, como a Waymo, do Google, não podem fotografar cada centímetro quadrado de suas estradas devido a preocupações com a segurança nacional. Mas os veículos autônomos exigem câmeras e uma conexão à Internet para operar, portanto este regulamento terá o efeito de manter veículos autônomos de origem estrangeira fora das estradas chinesas.

Os chineses entendem a ameaça que os veículos autônomos representam e querem limitar sua exposição – ou estão usando as preocupações de segurança nacional para mascarar uma tentativa de incubar sua própria indústria de veículos autônomos.

De qualquer forma, os chineses entendem claramente algo que já não é percebido por muitos ocidentais: o comércio liberalizado é muito bom, mas a segurança nacional é mais importante. Sem a cooperação internacional sobre a regulamentação de veículos autônomos e acordos comerciais simétricos com disposições severas contra violação, não devemos permitir o acesso de estados não-amigáveis a nossos

[15]Ver *https://en.wikipedia.org/wiki/Poisson_distribution*

mercados de veículos autônomos. (Também não devemos permitir componentes desses países.) Os chineses entendem isso. Nós deveríamos também.

4) Qualquer dispositivo permanente, não militar, que possa voar, dirigir, andar, disparar ou nadar autonomamente deve conter um módulo de segurança padronizado. O poder do mecanismo de propulsão, assim como os computadores e sensores que comandam o dispositivo autônomo, devem conectar-se através deste módulo de segurança. E se isso não for possível devido à natureza do sistema de propulsão (por exemplo, dispositivos com foguetes químicos), um sistema de desativação de emergência deverá estar presente.

O dispositivo não deve ser acionável ou operável a menos que o módulo de segurança esteja presente e o dispositivo não consiga acessar seu próprio módulo de segurança de forma alguma. (Dispositivos militares não devem estar sujeitos a estes regulamentos.)

Os países devem ser capazes de especificar quais módulos de segurança são aceitáveis em seus domínios, e você esperaria que a maioria dos países desenvolvessem seu próprio módulo ou confiassem apenas em dispositivos com módulos de segurança de seus aliados mais próximos. Mas os dispositivos podem ser projetados para aceitar vários módulos, e qualquer um deles pode iniciar os procedimentos de segurança. Dessa forma, o movimento autônomo não precisa cessar ao cruzar uma fronteira.

(Embora seja necessário ter cuidado para garantir que os dispositivos sejam realmente independentes. Qualquer módulo de segurança deve ser capaz de desligar o dispositivo ou colocá-lo offline, mesmo se outros módulos tiverem comandos para agir de maneira mal-intencionada. A segurança deve ser aditiva, não multiplicativa.)

Os módulos de segurança devem poder comunicar-se através de múltiplos canais; incluindo satélite, rádio, LTE e até luz pulsante via câmera embarcada. Dessa forma, utilizando chaves e certificados criptográficos, os governos poderiam ordenar comandos de emergência de dispositivos autônomos (através do módulo de segurança), como “desligamento em 5 segundos” ou “cessar atualizações de software até instruções adicionais”. O módulo de segurança deve ser capaz de desligar a energia e o computador de controle em situações de emergência.

E, finalmente, para garantir a integridade do próprio módulo, independentemente do código presente no computador do dispositivo autônomo, o dispositivo não deve interferir no módulo de segurança ou no módulo de segurança de outros dispositivos autônomos.

(A maneira mais direta de proteger o módulo de segurança seria empregar a arquitetura tradicional do computador com uma conexão unidirecional para o computador principal e um retorno a um chip ASIC imutável com seu próprio par de chaves criptográficas e uma conexão direta com a fonte de energia.)

5) Sistemas redundantes padronizados são outra salvaguarda. Se a energia for removida do computador principal de um dispositivo autônomo, o veículo ainda poderá pousar ou estacionar com segurança. Desligamentos totais devem estar sempre disponíveis, mas não devem ser o primeiro recurso durante um ataque cibernético.

6) Para que um veículo autônomo vá mais rápido que um limite de velocidade predefinido, ele deve solicitar permissão para isso ao módulo. Dessa forma, você poderia chegar ao hospital rapidamente durante uma emergência, mas os governos poderiam limitar quantos veículos velozes são permitidos de uma só vez. Por que isso é importante? Porque um carro que anda com metade da velocidade tem um quarto da energia cinética – reduzindo a possibilidade de uma explosão de bateria em uma colisão.

7) Isolar o computador de controle. A maioria das unidades de controle eletrônico automotivo se comunica usando a rede local do controlador (barramento CAN) - um barramento central não criptografado e não autenticado. Em todo o mundo, os desenvolvedores de software cospem seu café ao ler a sentença anterior. Não permita que computadores de controle leiam dados diretamente do barramento CAN. E não conecte o computador de acesso do veículo ao computador de controle.

Se precisamos obter o estado do barramento CAN, ele deve ser feito através de um módulo intermediário que converte os sinais em um de uma série finita de estados enumerados. (E enquanto estamos nisso, devemos criar um acordo internacional para abolir o barramento CAN e substituí-lo por algo mais seguro.)

8) Tome nota da Apple e use um Enclave Seguro dedicado a tarefas críticas de segurança, como a atualização do software do computador de controle. Assim como no módulo de segurança, o enclave seguro deve ter métodos de comunicação de reserva para desativar o carro com segurança durante uma vulnerabilidade crítica. Idealmente, o enclave seguro deve ser projetado com vários conjuntos de chips de diferentes fabricantes, a fim de mitigar a espionagem industrial ou vulnerabilidades como o *Meltdown* da

Intel.[16]

9) Não confie na rede. Não confie em cadeias de DNS ou certificados. Empregue pinagem de IP e fixação de certificado com estratégias de reserva. Não confie apenas em HTTPS. Protocolos e cifras não são perfeitos e ataques de degradação de protocolo são muito fáceis. Use criptografia do lado do cliente, além de HTTPS, e use chaves realmente grandes.

Envie cada carro com sua própria chave One Time Pad (OTP).[17] E crie a OTP com várias fontes aleatórias seguras em computadores nunca conectados à Internet em local seguro e protegido usado para assinatura de código. Não deve ser fisicamente possível ler o mesmo bit duas vezes a partir da OTP. A revisão final do código deve estar em computadores nunca conectados à Internet. E nunca, nunca, permita o acesso SSH a qualquer veículo autônomo – mesmo aqueles em desenvolvimento.

10) Empregue criptografia e assinatura de código e dados em tudo que é possível, incluindo dados em memória volátil. Todas as atualizações no computador de controle devem ser criptografadas, assinadas e duplamente verificadas. (O *checksum* deve ser compartilhado com os governos e transmitido para o módulo de segurança.) Se o computador de controle não puder verificar a assinatura ou a soma de verificação da atualização de software com o módulo de segurança, o computador de controle deve desligar o veículo com segurança.

Há outras maneiras de os governos colaborarem para mitigar parte do problema: os governos devem se unir para criar um sistema de recompensas, a fim de incentivar os pesquisadores de segurança. (Recompensas pelo controle remoto real poderiam variar entre US$100 e US$10.000 por dispositivo, dependendo de fatores como a velocidade máxima atingível.) Os governos também devem concordar em impor multas severas e sentenças de prisão por fabricação, venda ou fornecimento de produtos eletrônicos automotivos falsificados.

E nos países avançados deve-se aumentar dramaticamente o financiamento para as unidades de guerra cibernética e encontrar uma maneira de expandir as reservas cibernéticas para envolver especialistas em computação no setor privado. Para aqueles que não puderam obter uma autorização de segurança, encaminhá-los para iniciativas de código aberto e *think-tanks*.

Finalmente, devem aumentar o financiamento para pesquisas em chips especializados em segurança, não em desempenho (para que vulnerabilidades como *Meltdown* e *Spectre* sejam menos prováveis) e criar regulamentos que incentivem linguagens de programação mais seguras, como Rust, em detrimento das inseguras ou de comportamento indefinido.

Há uma linha de esperança em todo o trabalho que temos que fazer: a natureza da ameaça do veículo autônomo pode finalmente trazer a vontade política, os incentivos econômicos e as ideias de que precisamos para proteger nossos sistemas de computadores do mundo real. E com um pouco de sorte, poderíamos acordar décadas a partir de agora e falar com espanto sobre os eventos cibernéticos do início dos anos 2000, como fazemos com os incêndios químicos nos rios em meados do século XX.

[16]Ver *https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)*

[17]Ver *https://pt.wikipedia.org/wiki/One-time_pad*

OTTs: conceitos em disputa podem ter consequências para sua regulação

Oona Castro é coordenadora de conteúdo do Instituto Nupef e editora da revista poliTICs.

Serviços *Over-the-Top*, conhecidos como OTTs, são aqueles que operam na camada de aplicações da Internet[1], ou seja, onde os usuários da Internet produzem, acessam e trocam informações. Usualmente, são essas as plataformas que conhecemos, embora para navegarmos seja necessária a utilização das camadas de infraestrutura e de protocolos sobre as quais a de aplicações funciona.

OTTs são, assim, os serviços baseados em aplicativos através dos quais publicamos, acessamos e trocamos conteúdo. Entre os mais conhecidos estão os de vídeo sob demanda (VoD), como YouTube, Hulu, Netflix, Apple TV, o serviço de *streaming* de vídeos da Amazon, os de transmissão de mensagem e voz sobre IP, como WhatsApp, Telegram, Facetime, Skype, Viber, Messenger, iMessage, ou mesmo Xbox 360 e World of Warcraft no mundo dos jogos. Até mesmo Facebook, Twitter, Google e todos os sites podem ser compreendidos como OTTs quando os compreendemos tecnicamente como tudo o que está “over the top”, ou seja, na camada de aplicações da Internet.

No entanto, recentemente a União Internacional de Telecomunicações (UIT), agência da ONU dedicada a temas relacionados às Tecnologias da Informação e Comunicação (TICs), adotou a recomendação do grupo de trabalho SG3 (que lida com aspectos econômicos, financeiros e regulatórios), que definiu OTTs como “aplicações acessadas ou entregues na rede pública que podem substituir de forma direta ou funcional os serviços de telecomunicações tradicionais”. Ou seja, na prática, com essa definição, a UIT circunscreve a definição de OTT às aplicações que competem com os serviços de telecomunicações, especialmente os serviços de vídeo, voz e mensagens sobre IP. Em outras palavras, considera que esses serviços específicos deveriam de algum modo ser da alçada regulatória da UIT.

O texto do Observatorio Latinoamericano de Regulación, Medios y Convergencia (Observacom), iniciativa da Fundación Libertis, um *think tank* regional sem fins lucrativos que reúne especialistas do campo da comunicação, antecede a adoção da definição pela UIT e não se restringe a ela. É no contexto mais abrangente – compreendendo como OTTs as diversas plataformas e aplicações que operam na camada de conteúdo – que se inserem as recomendações de regulação do Observacom que ora publicamos.

Já o o texto da Flávia Lefèvre é posterior e traz questionamentos importantes em relação à decisão da UIT. A recomendação adotada pela organização foi levada pelo Brasil, por meio da participação da Anatel (Agência Nacional de Telecomunicações) no grupo de trabalho sobre impacto econômico.

---

[1] Além da chamada "camada física" (cabos e transceptores de rádio terrestres ou via satélite que constituem a infraestrutura de telecomunicações), a Internet é funcionalmente organizada em quatro camadas ou níveis: a camada de rede (também chamada de "enlace de dados") que transporta os datagramas; a camada de internet, que fornece endereçamento e roteamento dos datagramas; a camada de transporte, que garante a consistência do tráfego de dados ponta-a-ponta; e a camada de aplicações (os serviços de conteúo de todo tipo: voz, vídeo, email, páginas Web etc).A camada de aplicações é tudo aquilo que vemos na Internet – e a que nos referimos geralmente quando falamos “vi na Internet” - são os sites, plataformas, aplicações, tudo aquilo que visitamos e publicamos. O conjunto dessas quatro camadas caracteriza o Serviço de Valor Adicionado (SVA) definido na Norma 4, de 1995, do então Ministério das Comunicações, separando-o da regulação de telecomunicações.

Em reunião do Conselho de Comunicação Social do Senado em 4 de junho de 2018, Jefferson Fued Nacif, da Anatel, declarou que, “para a UIT, OTTs são todas aplicações que competem com os serviços tradicionais de telecomunicações”. Disse, ainda, que “a UIT não trabalhará sobre o que é Uber, que não é uma aplicação de discussão para a UIT, mas o Facebook Messenger, o WhatsApp e o Skype são aplicações para serem discutidas na UIT. E por quê? Porque fazem frente aos serviços tradicionais de telecomunicações”.

A editoria da revista poliTICs ouviu especialistas no setor para compreender se essa definição da UIT vai impactar na definição conceitual e política do que é OTT em todo o mundo ou se ela diz somente respeito àquelas OTTs que a UIT vai se permitir discutir. Ou seja, com essa definição, ela pretende apenas delimitar e justificar o que pretende discutir (os serviços e aplicações que competem com aqueles prestados por operadoras de telefonia), ou pretende reconceituar o que é OTT, de acordo com seus interesses (de trazer para o seu guarda-chuva esse debate), impactando não apenas a agenda política dos estados membros como também o campo epistemológico. Os países que tiverem uma compreensão mais abrangente do conceito de OTTs precisarão adotar a definição da UIT e tratar de aplicar outro termo para se referir a todas as aplicações não inclusas nesse recorte?

Para essas especialistas – a jornalista Cristina de Luca, que acompanha o tema há décadas, e Flávia Lefèvre, advogada da PROTESTE e representante da sociedade civil no Comitê Gestor da Internet no Brasil – a questão está em aberto. Ainda não se pode afirmar precisamente quais serão os resultados dessa iniciativa. Até o fim de 2018 haverá novas discussões e decisões nos fóruns da UIT e novas articulações dos estados membros. O conceito de OTT pode permanecer abrangente, e a UIT apenas restringir sobre quais OTTs ela pretende incidir e regular. Ou pode ser que os países membros adotem essa definição e precisemos adotar outros termos para referir-nos a todas as outras aplicações não contempladas pela restrita conceitualização do órgão das Nações Unidas.

O que se pode dizer, com convicção, é que a UIT deu um passo que há muito pretendia dar, que é o de trazer para dentro do seu fórum a possibilidade de regular alguns serviços e aplicações da Internet, hoje orientada por diretrizes de diversas instâncias multissetoriais, debatidas em fóruns nacionais, regionais e no Fórum de Governança da Internet (IGF), com forte participação da academia, da sociedade civil, de empresas e de governos. A UIT é uma das organizações mais antigas da ONU, mas tradicionalmente dita regras apenas para o setor de telecomunicações – responsável pela infraestrutura das redes – e é bastante permeável às preocupações e pressões do mercado. Trazer para o seu colo aspectos chave da Internet como aplicações da camada de conteúdo pode ter significativas consequências para a regulação da Internet no mundo.

A pressão é para definir condições econômicas semelhantes para as OTTs e para as empresas de telecomunicações. No Brasil, a Internet é considerada um serviço de valor adicionado (SVA) e, portanto, as empresas de OTTs não estão sujeitas às obrigações das empresas de telefonia – cobrança de impostos como o ICMS, obrigações de investimentos em infraestrutura e regulação da Anatel.

Com essa definição em curso sendo adotada pelo país, a Anatel poderá incidir sobre a regulação da camada de conteúdo da Internet, abrindo precedente para regulação de outros aspectos relacionados. O Brasil divulgou com orgulho a adoção da recomendação, como resultado de um processo que já vinha acontecendo há dois anos, sem consenso, visto que nem todos os países membros tinham a

mesma visão sobre OTT. De acordo com Jefferson Fued Nacif, “alguns países, principalmente África e Oriente Médio (SIC), têm uma visão de OTTs que dificilmente se compatibiliza com a visão dos Estados Unidos e da Europa sobre o que devem ser as discussões sobre OTT na UIT. O subgrupo de trabalho número três, do bureau de padronização, é presidido pelo brasileiro superintendente de competição da Anatel, Abraão Balbino, que conseguiu chegar a um documento de consenso entre essas distintas visões. Levou-se dois anos para se chegar a essa definição”. Mas não revelou a extensão do resultado desse trabalho: “se haverá regulação, propostas de resolução, acordos, tratados, ninguém sabe dizer por enquanto. Pelo menos se abre uma janela de oportunidade para discutir o tema. É melhor ter um foro internacional que discuta isso de forma tranquila, consciente, racional, do que cada país sair regulamentando o seu mercado de forma aleatória. Isso é muito prejudicial para o mercado”. Na opinião do representante da Anatel, “nós queremos um mercado que promova a inovação, a competição e bons serviços, e esses serviços OTTs estão aí para isso, no entanto não é fácil tratar desses temas, que são complexos, porque existe uma questão principal que é a extraterritorialidade – que são serviços que não estão baseados no Brasil mas são prestados no Brasil e não há outra forma de tratar esses temas senão no plano internacional. É impossível o Brasil ou qualquer outro país regulamentar isso sozinho”.

Já no fim da apresentação do representante da Anatel, na mesma reunião do Conselho de Comunicação Social ocorrida em 4 de junho, pergunta e resposta reveladoras: o representante das empresas de televisão e vice-presidente de programação da Associação Brasileira de TV por Assinatura, José Francisco de Araújo Lima, questionou Nacif se a Anatel estava acompanhando o andamento dos projetos de lei que tratam de vídeo sob demanda no Brasil, com os quais demonstrou estar visivelmente incomodado. Embora o representante da Anatel tenha confirmado que a agência acompanha todos os projetos de lei relacionados às telecomunicações, ele não sabia dizer uma só palavra sobre os projetos de lei ou sobre como a Anatel vê a questão.

Se restava alguma dúvida de que o foco de atenção da Anatel não está voltado para OTTs como Netflix e outras empresas de VoD, mas para os serviços de voz e mensagem sobre IP, o episódio foi didático ao esclarecer que, se existe uma inquietação central da agência sobre o tema, esta preocupação está relacionada aos serviços que competem com as operadoras de telefonia fixa e móvel, e não com as operadoras de TV por assinatura.

Regulação dos serviços OTT

Pontos de uma regulação democrática dos serviços de Internet ("over-the-top") para garantir uma Internet livre e aberta, e o pleno exercício dos direitos digitais e da liberdade de expressão

OBSERVACOM – Observatório Latinoamericano de Regulação, Meios e Convergência[1]

Introdução

É inegável a importância crescente sobre serviços "over-the-top" (OTT)[2] na economia mundial e seu papel fundamental no exercício de direitos humanos como a liberdade de expressão e o direito à informação. Também é inegável que sua irrupção desencadeou uma dura disputa econômica entre atores privados da economia digital que se traduz em debates regulatórios. É inevitável advertir, além disso, que este conflito econômico impacta a vida das pessoas e seus direitos.

Os temas centrais deste debate têm estado relacionados com a concorrência, os investimentos ou a tributação. Trata-se de aspectos sem dúvida importantes, mas um enfoque economicista limita a abordagem de um assunto tão complexo quanto vital para a humanidade e os direitos da pessoa humana.

Grande parte do debate sobre a neutralidade de rede e as assimetrias regulatórias provém de, ou está influenciado por, disputas entre importantes empresas de capital transnacional. Ademais, o atual desenvolvimento da Internet e o papel cada vez mais importante dos provedores de serviços OTT também põem em tensão o papel do Estado e a questão da soberania nacional, assim como os caminhos democráticas que se devem adotar para proteger o direito das pessoas no novo cenário convergente, enquanto se constroi um ambiente que garanta o desenvolvimento de uma Internet livre e aberta.

Tudo isso representa um forte desafio para que as organizações da sociedade civil adotem posições a partir de uma perspectiva independente,[3] ainda que não tenhamos ainda todas as respostas e soluções. Para isto, deveríamos contar com mais pesquisas e dados revelados também de forma independente, e não - somente - a partir dos insumos oferecidos por empresas, especialistas ou *think tanks* das partes em disputa.

Ainda que efetivamente existam assimetrias regulatórias entre empresas que disputam similares mercados ou oferecem serviços comparáveis, os serviços OTT apresentam desafios regulatórios que, por si só, precisamos abordar. Em nossa opinião, essa tarefa deveria ser enfocada com uma perspectiva de direitos humanos, colocando as pessoas como o centro das preocupações, e não as empresas e seus (legítimos) interesses comerciais.

Grande parte das discussões se canalizam por organismos multilaterais que não consideram

[1]OBSERVACOM é um think-tank regional sem fins de lucro, profissional e independente, integrado por especialistas e pesquisadores da comunicação comprometidos com a proteção e a promoção da democracia, diversidade cultural, direitos humanos e a liberdade de expressão. Para mais informações: *contacto@observacom.org*

[2]Apenas por razões práticas, neste documento vamos usar o termo amplo "over-the-top", uma definição também de debate.

[3]Embora em alguns casos essas posições possam coincidir com os interesses de uma das partes. O caso do debate sobre a neutralidade da rede é um exemplo sobre a confluência de posições, não sempre com base nas mesmas razões e interesses.

esse enfoque de direitos, como a Organização Mundial do Comércio (OMC), ou a União Internacional de Telecomunicações (UIT)[4] e que, portanto, não são os espaços mais adequados para tratar desses assuntos regulatórios. Por sorte, a Unesco e as relatorias para a Liberdade de Expressão das Nações Unidas ou da Comissão Interamericana de Direitos Humanos (CIDH) incluíram esses assuntos em suas pautas, convertendo-se em instâncias internacionais mais adequadas.

Desde a primeira metade do século XX, consolidou-se na maioria das democracias avançadas a perspectiva de que a regulação no setor de comunicações é fundamental como garantia da democracia. Isso se deve à centralidade que uma esfera pública plural e diversa tem para o seu bom funcionamento. A qualidade da democracia e um vigoroso debate cívico dependem amplamente da variedade de informações e visões que competem em um espaço público e que estão disponíveis para o cidadão. Em um cenário centralizado pelos meios de comunicação tradicionais, estava claro que o mercado não garantia – por si só – a diversidade, o pluralismo nem a liberdade de expressão fundamentais para a democracia. Com o surgimento da Internet, parecia que parte dos argumentos que davam sentido e fundamento à regulação democrática poderiam ter se perdido. De fato, alguns importantes atores do ecossistema digital afirmam que a regulação no âmbito da Internet não só é perigosa, como não deveria existir porque já nem sequer é necessária ou possível.

Entretanto, passada a fase inicial de funcionamento mais descentralizado e aberto da rede, novos gargalos se formam e a Internet passa por uma crescente centralização de alguns poucos agentes do ecossistema digital que afeta seu potencial de servir a toda a humanidade, como aponta o criador da Web, Tim Berners-Lee. A tendência à concentração e as ameaças à liberdade de expressão na rede mostram que a diversidade e a pluralidade – inclusive a noção de uma Internet aberta e livre – necessitam de garantias regulatórias para que possam ser mantidas como valores e paradigmas das comunicações digitais modernas.

Com esses conceitos e fundamentos, o OBSERVACOM elaborou este documento com propostas a respeito dos aspectos chaves que deveriam ser considerados para se estabelecer um ambiente regulatório democrático sobre os serviços de Internet denominados OTT, a partir da perspectiva dos direitos humanos e com o objetivo de garantir os direitos digitais e a liberdade de expressão, e uma Internet livre e aberta.

1. Uma única regulação para todos os serviços OTT não é adequada

Há aspectos da regulação que deveriam ser comuns a qualquer serviço com usuários e consumidores (obrigações de transparência ou proteção de direitos do consumidor, por exemplo) e que não devem ser ignorados. Mas as tentativas de aprovar uma legislação única para todos os provedores de serviços OTT é um erro, já que este setor inclui uma ampla diversidade de serviços.

As regulações, tomando como referência os princípios de interesse público que estão por trás da regulação de serviços similares deveriam levar em consideração, de maneira diferenciada e específica, o tipo de serviço e os direitos a proteger. Não se deveria regular de forma igual as atividades que oferecem serviços financeiros, locações de casas, entrega de pizzas ou que oferecem alternativas a transportes locais considerados como serviços públicos.

A proteção dos direitos humanos e da liberdade de expressão valem também para a Internet, mas precisam atender suas características específicas com relação a outros suportes

[4]Este documento é motivado pela consulta pública sobre a regulação dos serviços OTT, realizada pela UIT e encerrada em 29 de agosto de 2017.

tecnológicos, considerando ferramentas e medidas adequadas no ambiente digital. Por exemplo, precisa manter o serviço de proteção da infância em qualquer platafoma, mas o horário de proteção diário reconhecido internacionalmente como medida adequada para a TV aberta não é aplicável para determinados serviços na Internet.

As particularidades deveriam ser atendidas especialmente no caso dos provedores OTT que oferecem serviços audiovisuais – tanto lineares como não lineares.[5] Estes bens e serviços culturais não são simples mercadorias sujeitas a regras de comércio, como afirma a Convenção sobre Diversidade Cultural da Unesco, de modo que a adoção de medidas de proteção e promoção das indústrias audiovisuais nacional e a diversidade cultural não só são um direito dos Estados como também uma obrigação. Os esforços da União Europeia para a regulação do vídeo sob demanda mostram a importância – bem como os limites – da busca da aplicação desses princípios.

2. Pagar impostos sem impedir inovação nem asfixiar empresas pequenas ou sem fins lucrativos

Existem assimetrias regulatórias em matéria tributária que geram concorrência desleal com empresas que oferecem serviços sobre outros suportes, em alguns casos com empresas de capital nacional que realizam investimentos e geram empregos diretos e indiretos no país onde operam. Por sua vez, essa situação implica uma grande extração de dinheiro para o exterior, que prejudica especialmente os países em desenvolvimento, que sofrem perdas econômicas e uma erosão constante de sua base tributária.

Para conseguir fazer isso, as principais empresas do setor nem sempre se estabelecem nos países onde oferecem seus serviços, seja por razões operativas como também como estratégia para maximizar seus lucros. O modelo tributário conhecido por “double Irish” implica a escolha de países que são paraísos fiscais ou com menores cargas tributárias para registrar formalmente suas operações comerciais.[6] Os provedores de serviços OTT deveriam pagar impostos se desenvolvem atividades comerciais, como qualquer outra empresa de caráter lucrativo, em especial se oferecem serviços que são concorrentes ou substitutos de serviços existentes em determinado país. O princípio da cobrança nos lugares de consumo e realização do serviço deveria se sobrepor ao princípio de cobrança no país de onde o serviço é prestado.

Não obstante, as medidas tributárias e outras relacionadas também deveriam atender as diferenças entre pequenas e grandes empresas, entre *start-ups* e empresas de serviços OTT consolidados de alcance global, entre provedores de serviços OTT comerciais ou iniciativas sem fins de lucro ou educativas; entre outras razões, como forma de promover a concorrência, estimular a inovação e permitir o surgimento e desenvolvimento de pequenos e médios empreendimentos nacionais.

3. Provedores de serviços OTT não deveriam estar acima das leis nacionais

Os desafios de regulação colocados pelos serviços OTT incluem a dificuldade de aplicação de

[5]A OBSERVACOM publicará em breve um documento com propostas de regulamentação de serviços de comunicação audiovisuais na Internet. Os autores seguem o modelo europeu que classifica esses serviços em "lineares" y "não lineares". Os primeiros são serviços como a TV aberta ou paga, cujas características são prefixadas pelo operador e o usuário não pode modificar. Os segundos são serviços como Netflix e similares, onde são oferecidos conteúdos audiovisuais que o usuário pode baixar ou visualizar no momento que deseje.

[6]Sobre o modelo “double Irish”, ver *https://pt.wikipedia.org/wiki/Arranjo_duplo_irland%C3%AAs*

medidas regulatórias – e o questionamento do próprio papel dos Estados nacionais – por terem suas operações em um ou mais países, manterem sua operação global fora do lugar onde são prestados ou consumidos os serviços, e por trabalharem com transações internacionais. Estas dificuldades não podem justificar que os provedores de serviços OTT funcionem fora do marco legal, nacional ou supranacional, que cada Estado decide adotar.

A questão da jurisdição nacional é chave para garantir soberania em um ambiente global. Não há forma de avançar no debate de tributação ou de estabelecer mecanismos efetivos dos direitos das pessoas sem resolver adequadamente este assunto, que implica o respeito às normas locais sobre esses assuntos, começando pelo registro formal da empresa no país onde oferece seus serviços.[7]

Outras questões demandam, entretanto, soluções globais. Assim, será necessário combinar distintas estratégias e âmbitos de aplicação das medidas, de forma a combinar autorregulação, corregulação, regulação dos Estados nacionais, foros multissetoriais (com participação de empresas e organizações da sociedade civil), assim como acordos e compromissos internacionais.

Assuntos relacionados à governança global da Internet deveriam manter-se em espaços multissetoriais, de acordo com o princípio de participação ativa e democrática de representantes dos distintos interesses como caminho para garantir a globalidade da Internet e mitigar as possíveis violações e abusos, em sintonia com as recomendações da Relatoria Especial para a Liberdade de Expressão da Comissão Interamericana de Direitos Humanos (CIDH) e da Unesco.

Torna-se necessário, de maneira complementar, o estabelecimento de estratégias e mecanismos de atuação conjunta entre os países da região, de forma a conseguir a capacidade de negociação e de implementação frente a corporações privadas globais. A América Latina vive atualmente processos de análises e debates de iniciativas em busca de acordos regionais para uma atuação conjunta na economia digital.

4. *Gatekeepers*: los Estados deveriam garantir a neutralidade de rede como um princípio básico da Internet

Regular é, fundamentalmente, um ato necessário para garantir direitos. Neste caso, das empresas provedoras de serviços OTT, ante possíveis abusos estatais como de outros atores do ecossistema digital e para fortalecer seu papel como intermediários chaves no exercício de direitos por parte da população que utiliza seus serviços ou plataformas.

Em sintonia com as recomendações da Relatoria para a Liberdade de Expressão da CIDH, deveria incluir-se expressamente o princípio da neutralidade da rede nos marcos legais nacionais, com o alcance e as exceções que ela mesma reconhece. Este princípio foi reconhecido pela Relatoria Especial como uma "condição necessária para exercer a liberdade de expressão na Internet" que tem como objetivo garantir "a liberdade de acesso e escolha dos usuários de utilizar, enviar, receber e oferecer qualquer conteúdo, aplicação ou serviço legal por meio da Internet sem que seja condicionada, direcionada ou restringida, por meio de bloqueio, filtro ou interferência".

Este princípio vale, em particular, para aqueles operadores de redes físicas que são provedores de acesso à Internet (ISP), de forma que não dêem um tratamento preferencial e

[7] O registo não implica a obrigação de obter uma licença através de um procedimento concorrencial prévio, e suas demandas devem contemplar as condições propostas no ponto 3 deste documento em relação a start-ups, iniciativas sem fins lucrativos, entre outras.

discriminatório aos provedores de serviços OTT por acordos comerciais e outras razões.

Este princípio deveria ser aplicável também aos planos de "tarifa zero", ou zero-rating, assim como as estratégias comerciais de alguns provedores de serviços OTT – como acontece em iniciativas de acesso parcial à Internet como Free Basics – quando afetam o princípio de acesso a uma Internet aberta e livre.

De forma alguma os princípios baseados no interesse público, como a neutralidade da rede, deveriam ser flexibilizados com a intenção de gerar algum tipo de equilíbrio ou compensação para superar as assimetrias regulatórias existentes.

5. Os Estados deveriam garantir a liberdade de expressão: sem responsabilização legal por conteúdos de terceiros

Os provedores de serviços OTT são atores privados que se converteram em ferramentas imprescindíveis para o exercício do direito à informação e à liberdade de expressão na Internet – como no caso das redes sociais, motores de busca e outras plataformas – de tal forma que é necessário preservar e potencializar esse papel. Este mesmo papel de intermediários, no entanto, os colocou sob pressões para "aproveitar a posição que ocupam como pontos de controle de acesso e uso da Internet", afirma a Relatoria da CIDH.

Seja porque esse lugar torna mais fácil "identificar e coagir estes pequenos atores do que os responsáveis diretos da expressão que se busca inibir ou controlar" ou pelo impacto que uma pressão sobre uma só empresa tem sobre o total de usuários afetados, o regime de responsabilidade legal sobre os conteúdos de terceiros se converteu em um aspecto crucial para a garantia da liberdade de expressão. Por esta razão, os Estados deveriam promover e proteger o exercício da liberdade de expressão, adotando leis, políticas e práticas administrativas que favoreçam um ambiente regulatório adequado para que os prestadores de serviços OTT possam fazer frente a ameaças e pressões ilegítimas de remoção, filtro ou bloqueio de conteúdos por parte de autoridades estatais e outros atores privados.

Por essa razão, concordamos com a Relatoria que a responsabilidade objetiva ou "estrita", que responsabiliza o intermediário por qualquer conteúdo considerado ilícito em sua plataforma é incompatível com a Convenção Americana Sobre Direitos Humanos,[8] e promove o monitoramento e a censura pelos intermediários, levando-os a ocupar uma função de autoridade legal que não lhes cabe.

A regulação deveria incorporar a noção de que "nenhuma pessoa que ofereça unicamente serviços técnicos de Internet como acesso, buscas ou conservação de informações em memória cachê deverá ser responsável por conteúdos gerados por terceiros e que se difundam por meio desses serviços, sempre que não intervir especificamente em tais conteúdos nem se negar a cumprir uma ordem judicial que exija a sua eliminação quando estiver em condições de fazê-lo ("princípio de mera transmissão")", como afirmou a Declaração Conjunta sobre Liberdade de Expressão e Internet de 2011.[9]

Essa questão não supõe afirmar que os intermediários não tenham "nenhuma responsabilidade" sobre a troca de conteúdo através de suas plataformas, já que não são meros serviços técnicos[10] e intervêm – muitas vezes por suas próprias decisões editoriais ou comerciais, sem necessidade de pressões estatais – priorizando ou amplificando certos

[8]Ver *https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm*

[9]Ver *http://www.oas.org/pt/cidh/expressao/showarticle.asp?artID=849&lID=4*

[10]Ver o ponto 9 deste documento.

conteúdos de terceiros, por exemplo.

6. Os Estados e empresas OTT deveriam garantir direito à privacidade e à proteção de dados pessoais

O direito à privacidade é um direito humano e sua proteção está em risco porque as tecnologias digitais permitem, tecnicamente, uma crescente capacidade para reunir, armazenar e trocar informações pessoais em termos do que agora se denomina *big data*. Ele implica que uma enorme quantidade de informação sobre as pessoas pode ser interceptada e analisada sem conhecimento desta situação e sem consentimento expresso e prévio.

Diante desses desafios, os Estados deveriam respeitar e proteger o direito à privacidade na Internet e adaptar sua legislação e suas ações protegendo todas as pessoas sob sua jurisdição, o que inclui dar garantias à confidencialidade dos dados pessoais online e fazer frente à crescente e indiscriminada vigilância e interceptação de comunicações na Internet. Isso porque, quando essa vigilância se dá de maneira maciça, segundo o Comitê de Direitos Humanos das Nações Unidas, resulta em efeitos negativos no gozo e exercício dos direitos humanos.

Dever-se-ia garantir proteção aos provedores de serviços OTT com relação à prática de alguns governos, polícias e outras autoridades estatais que os pressionam para registrar ou compartilhar dados pessoais, quando não se cumprem as condições que outorgam legitimidade à solicitação, por exemplo quando se realiza através de um pedido concreto e expresso de uma instância judicial.

A regulação deveria proteger as pessoas também "frente a possíveis ingerências arbitrárias ou abusivas também de terceiros", como recomenda a Relatoria para a Liberdade de Expressão da CIDH, na medida que "o modelo de negócios das empresas mais exitosas incide diretamente sobre o direito à privacidade".

É imprescindível exigir maior transparência dos Estados – sobre suas políticas e protocolos de vigilância, por exemplo – bem como das corporações privadas que oferecem serviços OTT, tanto sobre as solicitações que recebem por parte dos Estados, e ações e razões para suas respostas, como sobre suas próprias políticas de uso dos dados pessoais e mecanismos de "vigilância privada" com fins comerciais das comunicações pessoais de seus usuários, incluindo conhecer como os algoritmos processam tais dados.

7. Novos *gatekeepers*: as empresas de serviços OTT deveriam garantir o acesso a uma Internet aberta e livre

Sem os intermediários seria humanamente impossível desfrutar do enorme potencial disponível na rede das redes. As empresas provedoras de plataformas e aplicações na Internet têm um papel chave para o acesso a uma Internet aberta e livre pelo papel que ocupam como intermediários entre os usuários e os conteúdos disponíveis na rede. Mas este novo e vital papel – paradoxalmente – as converte em um potencial risco para a liberdade de expressão e o livre fluxo de informação na Internet.

Esses intermediários já não são somente suportes técnicos e "estradas de passagem", mas muitas vezes afetam os conteúdos que por ela circulam. Não só são capazes de monitorar todos os conteúdos produzidos por terceiros, mas também podem intervir neles, ordenando ou priorizando seu acesso e, portanto, determinando quais conteúdos e fontes de informação um usuário visualiza ou deixa de visualizar. Também bloqueiam, eliminam ou desindexam

conteúdos – que podem ser discursos protegidos pelo direito à liberdade de expressão –, assim como contas ou perfis de usuários. Essa ações muitas vezes são obrigadas por pressões externas de autoridades governamentais ou outros atores privados, mas também por decisões próprias.

Os algoritmos são responsáveis por decisões fundamentais sobre os conteúdos que podemos acessar efetivamente, facilitando ou dificultando o acesso aos conteúdos disponíveis na Internet. Uma arquitetura de algoritmos e o uso de formas de inteligência artificial que selecionem os conteúdos que podemos visualizar em função das predileções das pessoas e que tenha como objetivo deixá-lo "satisfeito" e "confortável" poderá ter boas intenções e ser uma exitosa estratégia comercial para atrair usuários, mas não é necessariamente compatível com a diversidade e o pluralismo, um requisito fundamental para o bom funcionamento de uma sociedade democrática.[11]

Esse acesso condicionado aos conteúdos, assim como a remoção daqueles entendidos como "inapropriados" ou "ofensivos" - por avaliação das próprias empresas e seus "moderadores" - se realizam com falta de transparência e de um devido processo para a tomada de decisões ou para se recorrer delas. As principais empresas do setor sequer informam publicamente quantas remoções por decisão própria realizam. Tudo isso as distancia dos padrões internacionais sobre restrições legítimas à liberdade de expressão, inclusive dos Princípios de Manila Sobre Responsabilidade dos Intermediários.[12]

Os organismos internacionais de proteção da liberdade de expressão começaram a advertir sobre este problema. David Kaye, Relator da ONU, disse que "é comum as empresas privadas censurarem, vigiarem ou realizarem outras restrições à liberdade de expressão, geralmente pressionados pelos governos, mas algumas vezes, por sua própria iniciativa". Para Edison Lanza, relator da CIDH, "a falta de transparência no processo de adoção de decisões por parte dos intermediários frequentemente encobre práticas discriminatórias ou pressões políticas que determinam as decisões das empresas". Em uma declaração conjunta sobre *fake news*, entretanto, as Relatorias para a Liberdade de Expressão, por sua vez, mostraram-se "consternadas por algumas medidas tomadas por intermediários para limitar a consulta ou a difusão de conteúdos digitais", tais como "sistemas de eliminação de conteúdos baseados em algoritmos ou no reconhecimento digital". Estes mecanismos, segundos os relatores, "não são transparentes, não cumprem os padrões mínimos de devido processo e/ou limitam de maneira indevida o acesso a conteúdos ou sua difusão".

8. A neutralidade das plataformas também deveria ser um princípio básico da Internet

Os padrões interamericanos incluem o princípio da neutralidade da rede como uma condição indispensável para a liberdade de expressão na Internet. O objetivo é, como se mencionou anteriormente, evitar que "a liberdade de acesso e escolha dos usuários de utilizar, enviar, receber ou oferecer qualquer conteúdo, aplicação ou serviço legal por meio da Internet não seja condicionada, direcionada ou restringida, por meio de bloqueio, filtragem ou interferência".

O mesmo princípio deveria alcançar outros intermediários – quer dizer, não apenas os provedores de serviços Internet (ISPs) – com o mesmo objetivo de garantir a diversidade, o

[11] O impacto na campanha eleitoral nos Estados Unidos, os resultados da busca de informação e opiniões sobre judeus e o holocausto, ou a remoção das fotos de Kim Phuc, a "menina de napalm", e de indígenas brasileiros ou australianos seminus, são alguns dos exemplos mais conhecidos.

[12] Ver *https://www.eff.org/files/2015/07/02/manila_principles_1.0_pt.pdf*

pluralismo e o acesso a uma Internet livre e aberta. Isso é importante, pois muitas dessas plataformas – e os algoritmos que utilizam – são crescentemente responsáveis por decisões fundamentais sobre o conteúdo que as pessoas acessam.

O nível de interferência potencial ou efetiva sobre os conteúdos na Internet coloca uma enorme responsabilidade nos intermediários que, na prática – e se existe algum tipo de regulação democrática –, se transforma em uma forma de regulação privada nunca antes vista. Uma situação agravada pela debilidade dos Estados democráticos para regular fenômenos que transcendem suas fronteiras administrativas. O conceito de "neutralidade" também é válido para este ator do ecossistema digital porque as corporações provedoras de serviços OTT têm o potencial de afetar a liberdade de expressão "condicionando, direcionando ou restringindo" conteúdos "por meio de bloqueio, filtro ou interferência" se não atuam de maneira neutra sobre as informações e opiniões que circulam por suas plataformas e aplicações.

Essa capacidade de ser um *gatekeeper* que reside no controle de uma camada física ou virtual de acesso não deveria afetar o princípio que deu origem à noção de neutralidade da rede e que o colocou como um tema chave da agenda de liberdade de expressão na Internet. De fato, não foi necessária uma evidência sistemática e ampla de uma violação da liberdade de expressão motivada por razões políticas ou ideológicas por parte dos ISPs para identificar um grave problema para este direito fundamental, e concluir que se tratava de um princípio básico da Internet que deveria ser regulado mediante a aprovação de leis nacionais.

9. Na Internet também há concentração, é crescente e impacta negativamente na liberdade de expressão

A existência de monopólios e oligopólios dos meios de comunicação tradicionais é uma realidade na região latinoamericana, constatada por inúmeras pesquisas acadêmicas e registrada por organizações internacionais como Unesco, entre outras.

A chegada da Internet supôs a eliminação de obstáculos para produzir, difundir e encontrar uma tão ampla gama de informações e opiniões que pareceria anacrônico e impertinente sequer mencionar a ideia de "concentração". No entanto, os processos de concentração e de constituição de posições dominantes também se encontram no novo ecossistema digital. Isso acontece tanto no âmbito dos ISPs e empresas de telecomunicações como também dos provedores de serviços OTT ou intermediários, em áreas chaves relacionadas com a liberdade de expressão e o direito à informação.

As evidências mostram uma tendência a uma maior concentração nas mãos de umas poucas corporações transnacionais como resultado da própria dinâmica do atual modelo de negócios de Internet. Essa acumulação de poder não só é resultado do êxito dos serviços e bens prestados entre os usuários, mas pelas próprias características de uma "economia de rede": escala global do negócio, capacidade de obter capitais para os investimentos necessários, dusão ou compra de outras empresas competidoras ou complementárias, entre outras razões. A disputa pelo espectro radioelétrico e a Internet das coisas (IoT) e, em especial, a capacidade de monetizar o *big data* resultante, parecem indicar processos de aprofundação da concentração atual.

A preocupação com relação à concentração na camada de serviços OTT se justifica, além dos aspectos de concorrência econômica, porque várias das corporações empresariais que têm um poder de mercado significativo e uma posição dominante na Internet são proprietárias de plataformas que habilitam o livre fluxo de informação e outros conteúdos relevantes, tais como redes sociais, motores de busca, aplicações de comunicação e plataformas de intercâmbio de vídeos. Neste ambiente concentrado, os riscos potenciais para o acesso, a

diversidade e a pluralidade de ideias e informações já mencionados se agravam de forma notável.

10. Nem desregular para resolver assimetrias, nem a autorregulação como única solução

Ainda quando há dificuldades para encontrar uma forma de regulação adequada para os serviços OTT e existem riscos de intervenções estatais abusivas, não é aceitável fragilizar a busca de regras de jogo democráticas para o funcionamento de nossas sociedades, inclusive no ambiente digital.

A autorregulação é parte da resposta a estes desafios, desde que se realize respeitando o março internacional de direitos humanos e seja compatível com padrões como os "Princípios Orientadores Sobre Empresas e Direitos Humanos" do Conselho de Direitos Humanos das Nações Unidas.[13] Seus termos de uso e código de ética, por exemplo, não deveriam estabelecer regras próprias que sejam contrárias à liberdade de expressão.

Quanto mais autorregulação e melhores práticas empresariais existirem, menos será a necessidade de intervenção estatal, o que é desejável. Mas não pode ser a única solução. Não se deveria privatizar o estabelecimento das regras de jogo democráticas de nossas sociedades. O mercado, por si só, não pode garantir a liberdade de expressão de todas as pessoas nem a existência de democracias inclusivas.

Por outro lado, tratar de resolver as assimetrias entre serviços comparáveis eliminando toda a regulação dos setores já regulados seria um grave retrocesso em uma sociedade democrática e na conquista de direitos humanos fundamentais, assim como a renúncia à obrigação de proteção desses direitos que têm os Estados. Por exemplo, se isso supõe remover todas as obrigações e contraprestações dessas empresas, e acabar com as garantias para uma efetiva proteção dos direitos das pessoas diante delas.

Eventualmente, poderia ser simplificado ou revisado o alcance de algumas das regulações econômicas ou administrativas, sempre que seja estritamente necessário e não signifiquem uma diminuição na proteção dos direitos humanos.

Diante do temor de intervenções estatais abusivas e toda forma de censura, o melhor antídoto é o mesmo que organismos do Sistema Interamericano de Direitos Humanos e das Nações Unidas elaboraram para orientar a proteção dos direitos: as regulações devem cumprir os padrões internacionais de liberdade de expressão para serem legítimas. Não deveria ser diferente para abordar os debates regulatórios sobre Internet e os serviços OTT.

[13]Ver *http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_SP.pdf*

Regulação ou Enforcement para as Empresas na Internet?

Está em pauta intensa discussão sobre qual tratamento regulatório devem receber as empresas conhecidas como Over the Top (OTTs) por oferecem aplicações e conteúdos sobre as camadas de infraestrutura de telecomunicações e protocolos de Internet. O debate tem como premissa a alegação de que essas plataformas, apesar de muito poderosas, estariam sub-reguladas.

É certo que o acelerado e enorme crescimento e importância dessas grandes plataformas de aplicações trouxeram não só alternativas a serviços de voz e mensagens, típicos das telecomunicações, facilidade de acesso a conteúdos dos mais diversos – de lazer a cultura e educação; mas trouxeram também perplexidades decorrentes do caráter transfronteiriço da Internet e das consequentes dificuldades de se aplicar conceitos como jurisdição e soberania, bem como do fato de que são vias poderosas para vigilância arbitrária e coleta massiva de dados pessoais – ativo mais valioso hoje no mundo dos negócios.

Tensiona ainda mais as discussões a respeito de como tratar essas plataformas a abrangência planetária da atuação de poucas e poderosas empresas que concentram de forma que nunca se poderia imaginar os mercados de diversos países. O mercado de tecnologia está fortemente concentrado entre cinco empresas: Apple, Google, Microsoft, Amazon e Facebook.

O Facebook, por exemplo, tem mais de 2,2 bilhões de usuários em todo o mundo – quase o dobro da população do continente africano. Recente pesquisa, divulgada pela Parse.ly de 2017, indica que 70% das notícias lidas na Internet são acessadas pelo Google e Facebook.

Aqui no Brasil, o Facebook, que conta com mais de 100 milhões de usuários, tem contrato com as três empresas que concentram o mercado do serviço de conexão a Internet – Claro, Vivo e OI com mais de 75% de *market share*, para garantir que, ao final do volume de dados contratados nos planos pré-pagos de acesso a Internet, o acesso a sua plataforma e ao WhatsApp, que integra seu grupo econômico, seja mantido, conferindo-lhes uma condição especial para coleta de dados e uma posição absolutamente superior a outras

empresas no que diz respeito às atividades de exploração de distribuição de conteúdos e veiculação de publicidade e propaganda, com um poder perigoso de influenciar comportamentos, formação de opinião e impactar os processos políticos e democráticos.

Além disso, discute-se muito sobre o quanto essas empresas pagam de tributo, principalmente considerando os efeitos disruptivos e negativos da exploração de seus negócios, como se revelou mais recentemente com o caso da transferência ilegal de dados de usuários do Facebook para a Cambridge Analytica, com influências determinantes na eleição de Donald Trump nos EUA e na decisão no Reino Unido sobre o Brexit.

Neste último mês de abril a União Internacional de Telecomunicações (UIT) -– organismo das Nações Unidas com atribuição para definir padrões e regular infraestruturas de telecomunicações no âmbito internacional, aprovou recomendação que adotou a definição das OTTs como “aplicações acessadas ou entregues na rede pública que podem substituir de forma direta ou funcional os serviços de telecomunicações tradicionais”. A justificativa é criar “estrutura colaborativa para promover a concorrência, proteção do consumidor, benefícios para os consumidores, inovação dinâmica, investimento, desenvolvimento de infraestrutura, acesso e acessibilidade em relação ao crescimento global de Aplicações Over the Top (OTT)”.

A UIT e seus estados membros, entre eles o Brasil, está em fase preparatória para a reunião plenipotenciária, que ocorrerá em outubro e dezembro deste ano em Dubai. Discutem-se nesse momento temas envolvendo as OTTs, tais como privacidade, proteção de dados, segurança, comércio eletrônico, com o objetivo de inclui-los no âmbito de regulação de telecomunicações. Esta discussão é muito conveniente para as empresas de telecomunicações, que sentem o peso da atuação das empresas de aplicações em serviços que substituem a telefonia e mensageria e que, além disso, possuem condições privilegiadas para a coleta de dados pessoais. E também para países que não convivem bem com liberdades democráticas e liberdade de expressão.

Não é a toa que a proposta em pauta para este tema é da Rússia, país com atuação questionável no que diz respeito a conquistas como a neutralidade da rede e o desincentivo à vigilância.

No Brasil estão envolvidos no processo de preparação para a discussão na UIT, além de representantes da sociedade civil e empresas de telecomunicações e aplicações, a Agência Nacional de Telecomunicações, (ANATEL), o Ministério das Relações Exteriores e o Comitê Gestor da Internet no Brasil (CGI.br) e é fundamental que acompanhemos o processo de construção da posição brasileira que será levada à reunião da UIT pelo Brasil.
Ou seja, essas iniciativas devem nos preocupar na medida em que tendem a levar as questões relacionadas a Internet para o campo regulatório tradicional, cujos dirigentes costumam ser indicados por governos, sem representação da sociedade civil, marcado por viés técnico e econômico, com peso reduzido para garantias dos direitos fundamentais e geralmente muito comprometido com interesses dos agentes privados regulados. O ideal, quando falamos de Internet, é a governança multissetorial, como tem sido reconhecido internacionalmente, nos debates que acontecem há doze anos no Fórum de Governança da Internet, promovido pelas Nações Unidas, e ficou consignado na Declaração de São Paulo, assinada por mais de cento e dez países em abril de 2014, no Encontro Net Mundial.
A Internet é um espaço público e não pode ser confundido com os ambientes criados por grandes grupos econômicos transnacionais privados que atuam em escala monopolista em todo o planeta.
Criar ainda mais regras e imposições além das que já existem pode nos levar a resultados adversos no sentido de encarecer o acesso e torná-lo ainda mais desigual e de reduzir conquistas de grande relevância como neutralidade da rede e proteções à privacidade e liberdade de expressão.
Ou seja, mais importante do que criar novas regras, correndo o risco de engessar os mercados e gerar dificuldades para que pequenas e médias empresas possam ingressar, é dar efetividade aos direitos já estabelecidos.
Aqui no Brasil temos o Código de Defesa do Consumidor, o Sistema Brasileiro de Concorrência e o Marco Civil da Internet, entre tantas outras normas, que regulam de forma extensa e profunda a atuação das plataformas; e mais recentemente, estamos em vias de aprovar uma Lei de Proteção de Dados Pessoais.
Todavia, nossos órgãos de controle pouco atuam na direção de dar concretude a todo esse sistema legal.

O Conselho Administrativo de Defesa Econômica recentemente concluiu que o acordo do Facebook e WhatsApp com as operadoras do serviço de conexão a Internet, reconhecidas pela ANATEL com Poder de Mercado Significativo (PMS), não traz prejuízos à concorrência, demonstrando que conta com uma estrutura de análise não adequada para o cenário atual que nos impõe o desenvolvimento tecnológico e a atuação em escala monopolista, como tem sido reconhecido pela Comunidade Europeia e por autoridades americanas, que já estudam medidas para quebrar a preponderância lesiva dessas empresas para as economias dos diversos países, assim como para o exercício de direitos de informação livre, privacidade, proteção de dados pessoais e segurança.

Ou seja, precisamos de *enforcement* e não de mais regras que poderão restringir o acesso a Internet, tão importante para o desenvolvimento econômico, cultural, educacional e social, assim como para a redução da enorme desigualdade entre ricos e pobres que marca os nossos tempos.

Uma abordagem holística para a construção de políticas públicas relacionadas à Internet

Pode o processo de Helsinque dos anos 70 ser uma fonte de inspiração para melhorar a estabilidade do ciberespaço?

Wolfgang Kleinwächter -- Professor Emérito da Universidade de Aarhus, ex-membro do Conselho da ICANN.

Há 20 anos, a governança da Internet[1] era uma questão técnica com algumas implicações políticas. Hoje, a governança da Internet é uma questão política chave com alguns componentes técnicos. Essa mudança está desafiando o equilíbrio institucional no ecossistema global de governança da Internet e seus mecanismos de negociação envolvendo instâncias governamentais e não-governamentais. Estruturas colaborativas intergovernamentais como o G20, G7 e BRICS, ou organizações como a OTAN, a OMC, a OIT e a OSCE, que no passado pouco ou nada tinham a ver com a governança da Internet, agora aparecem como atores fundamentais. Isso não significa que organizações técnicas como ICANN, IETF, ISOC, RIRs, W3C, IEEE, 3GPP etc, que dominaram as discussões sobre governança da Internet nas últimas duas décadas, estão perdendo relevância.[2] O que vemos é uma nova "complexidade de governança da Internet". O reequilíbrio do poder no interior do ecossistema de governança da Internet leva a abordagens inovadoras para a construção de políticas públicas relacionadas à Internet global e a uma cooperação aprimorada entre setores governamentais e não-governamentais, bem como a uma colaboração mais estreita entre criadores de código e criadores de leis, tanto nacional como globalmente.

A formulação de políticas para o ciberespaço é realizada por atores estatais e não estatais. A definição funcional de governança da Internet, adotada pela Cúpula Mundial da ONU sobre a Sociedade da Informação (CMSI/WSIS) no encontro de Túnis em 2005, destacou "governos, setor privado e sociedade civil" como as principais partes interessadas. Hoje a comunidade técnica-acadêmica é vista como uma quarta parte interessada. Todos esses setores, de acordo com a definição de Túnis, operam em seus "respectivos papéis" -- significa que são diferentes, não podem substituir um ao outro, mas têm que trabalhar lado a lado. Eles têm que "compartilhar princípios, regras, normas, procedimentos e programas de tomada de decisão". Nenhuma parte interessada pode gerenciar o ciberespaço sozinha. Todas são necessárias para garantir um ciberespaço aberto, livre, não fragmentado e estável.

O "ecossistema de governança da Internet" é um mecanismo em camadas. A definição da CMSI diferencia o "desenvolvimento" e o "uso" da Internet.

- O "desenvolvimento" da Internet refere-se à camada inferior ou técnica (governança da Internet), o "uso" da Internet refere-se à camada superior ou política (governança na Internet). Essa camada superior pode ser subdividida em três subcamadas interconectadas: segurança, economia e direitos humanos.
- Embora seja impossível separar a camada técnica da camada política, há também um entendimento comum de que todas as camadas / subcamadas devem ser tratadas diferentemente, de acordo com

[1]O termo "governança da Internet" foi cunhado pelo Harvard Information Infrastructure Project (HIIP) em meados da década de 1990. isso foi usado para esclarecer que a Internet não é gerenciada pelos governos. A Cúpula Mundial da ONU na Sociedade da Informação (WSIS) reconheceu o papel dos actores não governamentais e adoptou em Tunis (2005) uma definição de trabalho: "A governança da Internet é o e aplicação pelos governos, setor privado e sociedade civil, em seus respectivos papéis, de princípios, normas, regras, procedimentos de tomada de decisão e programas que moldam a evolução e uso da Internet. "A Agenda de Túnis também reafirmou "Que a autoridade política para questões de políticas públicas relacionadas à Internet é o direito soberano dos Estados." Quando a Internet se tornou mais relevante para a segurança internacional e a economia global, foi introduzida uma nova linguagem como "cyber" (usada principalmente por ministérios de negócios, defesa e interior) ou "digital" (usado principalmente pelos ministérios da economia, tecnologia e desenvolvimento). Alguns países usar "tecnologias de TIC" em vez de "Internet". O setor de negócios usa "e-commerce". Não há definição da "Internet das Coisas" (IoT) A Coalizão Dinâmica sobre IoT do IGF considera a IoT como uma "aplicação no topo do Sistema de Nomes de Domínio (DNS)".

[2]Ver glossário de siglas ao final do texto.

a natureza específica dos assuntos em questão. Não existe “tamanho único”. É geralmente aceito que atores não-estatais desempenham um papel de liderança na camada técnica, enquanto os governos lideram a camada política. No entanto, essa diferenciação não exclui envolvimento governamental na camada técnica, nem o envolvimento de atores não-estatais na camada política.

Não há uma definição consensual de "multissetorialismo" (em inglês, “multistakeholderism”). A definição de 2005 da CMSI introduziu o conceito dos “respectivos papéis” e a filosofia de “compartilhar”. A Declaração do Encontro NetMundial (2014) definiu elementos centrais como participação de baixo para cima ("bottom-up"), abertura, transparência, inclusão e foco em direitos humanos. Em outras palavras, temos algumas diretrizes gerais para uma *abordagem multissetorial*, mas não temos um *modelo multissetorial* único predefinido. Até agora, dois modelos diferentes de participação multissetorial surgiram: o *modelo consultivo* e o *modelo colaborativo*.

- No modelo consultivo, os governos “consultam” com partes interessadas não-governamentais, mas a decisão final continua em suas mãos. O processo da CMSI+10 de 2015 é um bom exemplo de que tal abordagem pode produzir resultados significativos. Outro exemplo é a OCDE, onde a Reunião Ministerial recebe contribuições de quatro Comitês Consultivos. Contudo, a realidade é que os governos simplesmente fingem ouvir os vários setores quando eles convidam atores não-estatais para consultas, mas ignoram seus conselhos ao tomar decisões. Assim, até agora não há mecanismo estabelecido sobre como o aconselhamento não governamental é tratado em processos intergovernamentais-- nem no G7 nem no G20, onde as chamadas “conferências multissetoriais” foram organizadas em paralelo às reuniões ministeriais sobre a economia digital.
- O modelo colaborativo vai além. Neste modelo, atores estatais e não estatais trabalham em pé de igualdade. O desenvolvimento de políticas é feito em processos de baixo para cima, abertos e transparentes. As decisões são tomadas por consenso aproximado. O modelo é baseado em confiança mútua, o princípio “não prejudicar”, a filosofia de “compartilhar” e a compreensão de que, em um mundo interdependente e interconectado, cada jogador sabe o que deve fazer. O Fórum de Governança da Internet (IGF), a Declaração de Princípios do Econtro NetMundial (2014) e a transição da IANA da ICANN (2016) são três exemplos bem-sucedidos. Este modelo é complexo e não é fácil de explicar para quem não acompanha o assunto, mas o resultado é mais sustentável do que decisões tomadas por um único setor.

Nos anos 90, havia uma clara distinção entre a camada técnica e a camada política. Com menos de 100 milhões de usuários da Internet em todo o mundo (para uma população total em torno de seis bilhões no final da década), os problemas da Internet eram vistos como “problemas setoriais” e não tiveram papel relevante na discussão de temas políticos globais, como segurança internacional, desenvolvimento econômico, comércio, meio ambiente, direitos humanos etc. Isso mudou. Hoje temos cerca de quatro bilhões de usuários da Internet e quase todas as questões “tradicionais” de políticas públicas trazem um componente relacionado à Internet. Especialistas da Internet estão agora incluídos na elaboração de políticas públicas e os governos prestam mais atenção à discussão sobre questões técnicas. Isso levou a estruturas de negociação paralelas e parcialmente competitivas, bem como a um choque de culturas.

1. Estruturas institucionais paralelas:

- O sistema intergovernamental das Nações Unidas que surgiu ao final da Segunda Guerra Mundial baseia-se em tratados intergovernamentais que dão às organizações um mandato especial limitado para uma área claramente definida. As questões são negociadas apenas pelos governos e resultam em tratados juridicamente vinculativos. Há muito pouca ou nenhuma coordenação ou cooperação interinstitucional entre os vários setores.
- Nas últimas três décadas surgiu um sistema complementar de grupos não governamentais onde atores não estatais do setor privado, da sociedade civil e da comunidade técnica construiram instituições que desenvolvem políticas específicas. Os resultados são código técnico, auto-regulação da indústria ou compromissos juridicamente não vinculativos. Estas plataformas são altamente interconectadas.
- Como resultado, questões como segurança cibernética, e-comércio, privacidade, protocolos ou o sistema de nomes de domínio (DNS) da Internet são negociados por diferentes grupos estatais e não estatais, o que pode levar a regulações confusas e contraditórias.

2. Choque de culturas:

- Negociações entre grupos organizados são processos iterativos que incluem consulta pública. Eles são abertos, transparentes, de baixo para cima, inclusivos e baseados na filosofia de "consenso

aproximado e código de execução".[3]

- Negociações entre governos são principalmente a portas fechadas, não são inclusivas ou transparentes e baseiam-se no voto majoritário ou no consenso total.

Negociações intergovernamentais globais sobre desarmamento, meio ambiente, comércio ou desenvolvimento não são interligadas. Elas são administradas por diferentes ministérios dentro dos governos nacionais. Há pouca ou nenhuma coordenação entre os vários negociadores. Na Internet, tudo está conectado a tudo. Este novo protocolo técnico pode ter grandes implicações para a ciber-segurança, afetar os modelos de negócios e fortalecer ou enfraquecer os direitos humanos. O mesmo vale para decisões políticas. O novo Regulamento Geral sobre Proteção de Dados (GDPR) da Europa, que pretende fortalecer o direito individual à privacidade, afeta o modelo de negócios de muitas empresas da Internet, comércio digital, bem como o policiamento do ciberespaço e o trabalho de agentes da lei.

Quase não há mais nenhuma questão de política pública que não esteja relacionada à Internet. Em 2015 um grupo de correspondência criado pelo Grupo de Trabalho de Cooperação Aprimorada da CSTD da ONU (conhecido como WGEC) tentou identificar e categorizar assuntos de políticas públicas e terminou com uma lista de mais de 600 assuntos, que podem ser organizados em quatro grupos temáticos: ciber-segurança; economia digital; direitos humanos; tecnologia.

Para a maioria dessas questões, existem plataformas onde governos ou atores não estatais estão negociando normas e regulamentos. Isto levou a um quadro muito diversificado e desconexo de negociações e discussões relacionadas à Internet em que diferentes grupos organizados ficam restritos a seus silos -- muitas vezes ignorando o que está acontecendo em outros silos.[4] Há apenas um número limitado de plataformas, como o IGF, que permitem e estimulam a interssetorialidade e discussões pluralistas, bem como uma abordagem mais holística.

A segurança cibernética é discutida em muitas instâncias intergovernamentais: Nações Unidas, principalmente no Primeiro Comitê da Assembléia Geral e no Conselho de Segurança da ONU, na UIT, no Conselho da Europa, na União Europeia, na União Africana, na Interpol/Europol, no Arranjo de Wassenaar[5], na Comissão Global sobre a Estabilidade do Ciberespaço (GCSC), na Conferência Global sobre Ciberespaço (GCCS), na Conferência de Segurança de Munique (MSC), no Fórum Global de Perícia Cibernética (GFCE), na OTAN, na CMSI/WSIS, no IGF, na OSCE, nos encontros do G7, BRICS e outros. Para questões específicas, há negociações especiais e plataformas de discussão:

- Normas de comportamento de atores estatais e não estatais no ciberespaço: UNGGE, OSCE, G7, BRICS, GCSC, GCCS, WEF;
- Medidas de construção de confiança no ciberespaço: UNGGE, OSCE, ASEAN, G7, BRICS, GCSC, GCCS;
- Proteção do núcleo público da Internet e infraestrutura crítica como eletricidade, transações financeiras, serviços de transporte e sistemas eleitorais: ONU, G7, ICANN/PTI, GCSC, GCCS, MSC, OTAN;
- Moratória para o desenvolvimento de sistemas de armas autônomas letais (LAWS) e outras armas cibernéticas ofensivas baseadas na Internet: GCCS;
- Tecnologias de dupla utilização: Arranjo de Wassenaar, GCSC, GCCS;
- Luta contra o cibercrime: Conselho da Europa, Interpol/Europol, GFCE, GCSC, GCCS, WEF, UE, UA;
- Luta contra o uso terrorista das TICs: Comitê Contra o Terrorismo do Conselho de Segurança da ONU, Interpol/Europol, GCCS, GCSC, WEF.

A economia digital é discutida pelo G20, G7, OMC, UNCTAD, PNUD, OMPI, UNCITRAL, OCDE, WEF, UNCSTD,

---

[3]Expressão criada por Dave Clark em 1992 em encontro da IETF. Ver, por exemplo, Andrew L. Russell, "'Rough Consensus and Running Code' and the Internet-OSI Standards War", em *https://pdfs.semanticscholar.org/9ffa/d637b841df9e1904aea2265d0a88fd855d58.pdf*

[4]A Rússia propõe um tratado de segurança cibernética na ONU, que afetaria o comércio eletrônico global e o direito individual à liberdade de expressão. Setenta Estados-Membros da OMC propõem um pacto comercial digital; tal pacto teria consequências para a cibersegurança e o direito à privacidade. O relator especial da ONU sobre privacidade está propondo uma convenção da ONU sobre vigilância; esta convenção teria implicações para a segurança cibernética e o modelo de negócios de muitas corporações globais da Internet.

[5]Ver *https://www.armscontrol.org/factsheets/wassenaar*

WSIS, IGF, a Associação Internacional de Marcas (INTA), ICANN, Trademark Clearinghouse[6] etc. Para temas específicos, existem estes espaços de negociação:

- Comércio digital internacional: G7, G20, OMC, UNCTAD, OCDE, WEF, IGF;
- e-Comércio: OMC, UNCTAD, PNUD, UNCITRAL, OCDE, WEF;
- Desenvolvimento de infraestrutura: Comissões Regionais das Nações Unidas, UIT, UNCTAD, IGF, WSIS;
- Indústria 4.0[7]: G20, G7, WEF, IGF, OCDE;
- Internet das Coisas: G20, G7, ITU-T, IGF, WEF, OCDE;
- Inteligência Artificial: G7, IGF, WEF, OCDE;
- Proteção da Propriedade Intelectual: WIPO, WSIS, IGF, INTA, OCDE, ICANN / Trademarks Clearinghouse.

Os direitos humanos são discutidos no Terceiro Comitê da Assembléia Geral e no Conselho dos Direitos Humanos da ONU (Relatores Especiais para a Liberdade de Expressão e Privacidade na Era Digital), bem como na UNESCO, OIT, Conselho da Europa, OSCE, WSIS, IGF, PNUD, CSTD, Freedom Online Coalition (FOC), Repórteres Sem Fronteiras (RWB), APC, Human Rights Watch (HRW), Comissão Global sobre o Futuro da Trabalho[8] e outros. Para questões específicas, existem plataformas especiais de negociação e discussão, tais como:

- Acesso à Internet: UNESCO, ITU, WSIS, IGF, APC;
- Liberdade de expressão: HRC, UNESCO, Conselho da Europa, OSCE, WSIS, IGF, FOC, RWB, HRW;
- Privacidade na era digital: HRC, UNESCO, Conselho da Europa, WSIS, IGF, FOC, ICANN / Whois;
- Direito à educação: HRC, UNESCO;
- Direito à cultura: HRC, UNESCO;
- Mídia online: HRC, UNESCO, Conselho da Europa, OSCE;
- Futuro do trabalho: HRC, OIT, Comissão Global sobre o Futuro do Trabalho.

As questões técnicas são discutidas pelas chamadas organizações I*, como ICANN, IETF, IAB, ISOC, W3C, RIRs/NRO, bem como o IGF, mas também por organizações intergovernamentais, incluindo os âmbitos do processo pós-CMSI, a UIT e o ETSI. Para um número de questões específicas existem negociações especiais e plataformas de discussão, tais como:

- Endereços IP: RIRs/NRO, IGF, WSIS, ITU;
- Sistema de nomes de domínio: ICANN, IGF, WSIS, ITU;
- Sistema do servidor raiz: ICANN/PTI, IGF;
- Protocolos de Internet: IETF, W3C, IEEE, 3GPP, ITU, ETSI, IGF;
- IoT (Internet das Coisas): ITU-T, IGF, WSIS;
- OTT[9]: ITU-T, IGF.

Por um lado, existe a necessidade objetiva de uma abordagem holística que conecte as negociações e plataformas de discussão governamentais e não-governamentais. Por outro lado, seria uma ilusão esperarmos que todas as questões técnicas e de políticas públicas relacionadas à Internet possam ser reunidas em um único processo de negociação, como foi feito no âmbito das negociações da Convenção das Nações Unidas sobre o Direito do Mar (UNCLOS) ou da Convenção-Quadro das Nações Unidas sobre Mudanças Climáticas (UNFCCC). Uma abordagem mais realista poderia ser a criação de um quadro de relacionamento amplo, descentralizado e flexível para promover e melhorar o nível de comunicação e coordenação, bem como a colaboração formal ou informal entre as várias plataformas. Essas plataformas e

---

[6]Ver *http://www.trademark-clearinghouse.com*

[7]A expressão refere-se às tendências atuais de automação sistemas de inteligência artificial nos processos industriais. Também conhecida como a "quarta revolução industrial". Ver *https://en.wikipedia.org/wiki/Industry_4.0*

[8]Ver *http://www.ilo.org/global/topics/future-of-work/WCMS_569528/lang--en/index.htm*

[9]"Over-the-top": refere-se a serviços de valor agregado sobre redes de telecomunicações utilizando o protocolo Internet.

grupos de negociação poderiam interagir via “ligações” e um mecanismo de “relatoria recíproca”.

Este quadro poderia emergir tanto a partir de um mecanismo existente como o IGF, o WSIS ou uma estrutura derivada da metodologia do NetMundial, mas também em cima desses mecanismos como uma iniciativa nova e independente.

Tal abordagem poderia ser enquadrada como uma conferência descentralizada, informal e global sobre segurança e cooperação no ciberespaço (chamemos de CSCC), que poderia ter como objetivo a elaboração de um “Compromisso Final sobre Segurança e Cooperação no Ciberespaço ” com compromissos juridicamente não vinculantes dos governos, do setor privado, sociedade civil e comunidade técnica.

Uma fonte de inspiração poderia ser a Conferência sobre Segurança e Cooperação na Europa (CSCE) – o chamado “processo de Helsinque”, da década de 1970. A década de 1960 assistiu a um crescente número de conflitos na Guerra Fria entre o Leste e o Oeste. Para reduzir as tensões para evitar uma guerra nuclear, foram efetivados vários tratados e negociações bilaterais e multilaterais, entre os quais o Tratado de Proibição de Testes (1963), o Tratado sobre o Espaço Exterior (1965), o Tratado de Não-Proliferação (1968), as negociações SALT (1969), o Acordo de Berlim (1971) e os tratados bilaterais entre Alemanha Ocidental e União Soviética, Polônia, Tchecoslováquia e Alemanha Oriental (1972/1973).

Tudo isso foi canalizado para a CSCE, que visava reduzir ainda mais as tensões na Europa, para reforçar a cooperação entre o Oriente e o Ocidente e proteger os direitos humanos. O Oriente tinha segurança como sua primeira prioridade. O Ocidente teve os direitos humanos como primeiro prioridade. Mas todos os lados tinham interesses comuns em uma estabilização geral do cenário político e em um aumento da cooperação. As numerosas questões Leste-Oeste foram embaladas em três cestas (Segurança, Economia, Direitos Humanos), foram negociadas individualmente, mas estavam interligadas, o que permitiu concessões assimétricas nos processos de negociação (como o ministro de Relações Exteriores da Inglaterra argumentou em 1972, "sem ovos na cesta 3, não haverá ovos na cesta 1"). O acordo final da CSCE de 1975 não foi juridicamente vinculativo. Contudo, os seus compromissos políticos criaram um quadro bastante estável que evitou um maior crescimento de tensões ocidentais com efeitos colaterais incalculáveis e o risco de uma guerra nuclear; preparou o caminho para os processos de democratização no segunda metade dos anos 80 e permitiu a criação da OSCE, que contribuiu efetivamente para a paz e a compreensão internacional até hoje.[10]

Independentemente de algumas semelhanças entre a CSCE e um possível CSCC, também existem diferenças bastante grandes: a CSCE/OSCE abrange apenas a Europa. UMA CSCC teria que cobrir o mundo inteiro e dar incentivos especiais para países em desenvolvimento do Sul Global e grandes potências, como China, Brasil e Índia, que não fazem parte da CSCE. O modelo CSCE/OSCE é um mecanismo intergovernamental. A CSCC teria que ser multissetorial. A CSCE foi uma plataforma de negociação centralizada. A CSCC teria que ser concebida como um mecanismo descentralizado.

Para tornar tal estrutura viável, é preciso incentivar as diferentes partes interessadas em todas as regiões. Deve derivar-se de mecanismos e acordos existentes, como os documentos ou as decisões da Assembléia Geral da ONU estabelecendo que o direito internacional e os direitos humanos são relevantes tanto no mundo offline como no online.

Há quatro opções para avançar em um processo para uma possível CSCC de modo que resulte no mencionado compromisso final:

Opção 1: Fórum de Governança da Internet (IGF)

O IGF foi criado pela CMSI/WSIS em 2005 como uma plataforma de discussão – não é um órgão de negociação. No entanto, a renovação do mandato do IGF pela reunião da WSIS+10 de 2015 incluiu a expectativa de resultados mais tangíveis. A concepção do IGF dá ao MAG, o comitê organizador de cada IGF, muita flexibilidade para orquestrar a discussão de forma a vincular as organizações existentes e plataformas de negociação intergovernamentais e não-governamentais isoladas para o ambiente multissetorial do IGF, de modo que este funcione como uma câmara de compensação. O MAG poderia convidar diferentes organizações envolvidas com as questões dos quatro grupos temáticos já mencionados, para relatar anualmente ao IGF, para discutir os relatórios em um ambiente multissetorial e para enviar “mensagens” a suas plataformas de negociação.

Opção 2: o processo da WSIS +20

A próxima revisão da CMSI/WSIS está agendada para 2025 (WSIS+20). Pode-se imaginar uma

[10]Ver *https://www.osce.org/*

reestruturação do processo preparatório que vá além da Agenda de Túnis e use a "abordagem dos quatro grupos temáticos". Isso permitiria que os setores governamentais e não-governamentais negociassem novos compromissos políticos como parte de uma nova Declaração WSIS+20. Tais compromissos não substituiriam os tratados intergovernamentais que são negociados em comissões especiais entre os governos para a segurança cibernética, comércio digital ou direitos humanos, mas eles conectariam as várias questões em uma estrutura abrangente de políticas de governança da Internet – algo como uma CSCC – e ampliariam o horizonte para os criadores de tratados, criando uma percepção melhor sobre possíveis efeitos colaterais não intencionais das regulamentações intergovernamentais setoriais.

Opção 3: O processo NetMundial+5

O Encontro NetMundial (São Paulo, abril de 2014) adotou um "Roteiro da Governança da Internet". Este roteiro pode ser usado como ponto de partida para o lançamento de uma CSCC. Existem discussões para convocar uma conferência NetMundial+5 em 2019 (como um pré-evento para o 14º IGF agendado para Berlim em novembro de 2019) que analisará a implementação dos princípios e do roteiro da Declaração NetMundial de Governança da Internet.

Opção 4: Um novo processo independente

Pode-se imaginar também que atores estatais e não estatais concordam em estabelecer um novo processo independente para uma CSCC, visando a elaboração de um abrangente "Compromisso Final sobre Segurança e Cooperação no Ciberespaço".

Apêndice

Siglas mencionadas neste texto

Sigla	Nome	URL
3GPP	Third Generation Partnership Project (padrões de telefonia móvel)	http://www.3gpp.org/
APC	Associação para o Progresso das Comunicações	https://www.apc.org/
ASEAN	Associação das Nações do Sudeste da Ásia	http://asean.org/
AU/UA	União Africana	https://au.int/
BRICS	Grupo de países emergentes constituido por Brasil, Rússia, Índia, China e África do Sul	http://infobrics.org/
OSCE	Organização sobre Segurança e Cooperação na Europa	https://www.osce.org/
CSTD	Comissão da ONU de Ciência e Tecnologia para o Desenvolvimento	http://unctad.org/en/Pages/CSTD.aspx
DNS	Sistema de nomes de domínio da Internet	https://en.wikipedia.org/wiki/Root_name_server
ETSI	Instituto de Padrões de Telecomunicação da Europa	http://www.etsi.org/
EU/UE	União Europeia	http://europa.eu/
FOC	Freedom Online Coalition	https://freedomonlinecoalition.com/
G20	Estrutura intergovernamental de um grupo de 20 países	https://en.wikipedia.org/wiki/G20
G7	Estrutura intergovernamental de um grupo de sete países	https://en.wikipedia.org/wiki/Group_of_Seven
GCCS	Conferência Global sobre o Ciberespaço	https://en.wikipedia.org/wiki/GCCS
GCSC	Comissão Global sobre a Estabilidade do Ciberespaço	https://cyberstability.org/
GCSCC	Conferência Global sobre Segurança e Cooperação no Ciberespaço	
GDPR	Regulação Geral de Proteção de Dados (Europa)	https://www.eugdpr.org/
GFCE	Forum Global sobre Perícia Cibernética	https://www.thegfce.com/
HRW	Human Rigths Watch	https://www.hrw.org/
IAB	Conselho de Arquitetura da Internet	https://www.iab.org/
IANA	Internet Assigned Numbers Authority	https://www.iana.org/

ICANN	Internet Corporation for Assigned Names and Numbers	https://www.icann.org/
ICT/TIC	Tecnologias de informação e comunicação	---
IEEE	Instituto de Engenheiros Elétricos e Eletrônicos	https://www.ieee.org/
IETF	Força-Tarefa de Engenharia da Internet	http://ietf.org/
IGF	Forum da ONU sobre a Governança da Internet	https://www.intgovforum.org/multilingual/
ILO/OIT	Organização Internacional do Trabalho	http://www.ilo.org/global/lang--en/index.htm
INTA		
ISOC	Internet Society	
ITU-T	Setor de padronização da União Internacional da Telecomunicação	https://www.itu.int/en/ITU-T/Pages/default.aspx
ITU/UIT	União Internacional da Telecomunicação	https://www.itu.int/en/Pages/default.aspx
LAWS	Lethal Autonomous Weapons Systems	https://www.un.org/disarmament/update/pathways-to-banning-fully-autonomous-weapons/
MAG	Multistakeholder Advisory Group – IGF	https://www.intgovforum.org/multilingual/content/about-mag
MSC	Conferência de Segurança de Munique	https://www.securityconference.de/en/
NATO/OTAN	Organização do Tratado do Atlântico Norte	https://www.nato.int/
NetMundial	Encontro mundial multissetorial sobre a governança da Internet promovido, São Paulo, abril de 2014	http://netmundial.br/
NRO	Number Resource Organization	https://www.nro.net/
OECD/OCDE	Organização para a Cooperação e o Desenvolvimento Econômico	http://www.oecd.org/
OSCE	Organização para a Segurança e Cooperação na Europa	https://www.osce.org/
PTI (ICANN)	Public Technical Identifiers	https://pti.icann.org/
RIRs	Registros Regionais de Números de Internet	https://www.nro.net/about-the-nro/regional-internet-registries/
RWB/RSF	Repórteres Sem Fronteiras	https://rsf.org/en
UNCITRAL	Comissão das Nações Unidas para o Direito Mercantil Internacional	http://www.uncitral.org/uncitral/en/index.html

UNCLOS	Convenção das Nações Unidas sobre o Direito do Mar	https://en.wikipedia.org/wiki/United_Nations_Convention_on_the_Law_of_the_Sea
UNCTAD	Conferência das Nações Unidas sobre Comércio e Desenvolvimento	http://unctad.org/en/Pages/Home.aspx
UNDP/PNUD	Programa das Nações Unidas para o Desenvolvimento	http://www.undp.org/
UNESCO	Organização Educacional, Científica e Cultural das Nações Unidas	https://en.unesco.org/
UNFCCC	Convenção-Quadro das Nações Unidas sobre Mudança Climática	https://unfccc.int/
UNGGE	Grupo de Especialistas Governamentais da ONU no Campo da Informação e Telecomunicação	https://dig.watch/processes/ungge
W3C	Consórcio World Wide Web	https://www.w3.org/
WEF	Forum Econômico Mundial	https://www.weforum.org/
WGEC	Grupo de Trabalho da ONU sobre Cooperação Aprimorada	http://unctad.org/en/Pages/CSTD/WGEC-2016-to-2018.aspx
WIPO/OMPI	Organização Mundial da Propriedade Intelectual	http://www.wipo.int/portal/en/index.html
WSIS/CMSI	Cúpula Mundial sobre a Sociedade da Informação	http://www.itu.int/net/wsis/
WTO/OMC	Organização Mundial do Comércio	https://www.wto.org/