Internet Society
Capítulo Brasil

CONTRIBUIÇÃO DO CAPÍTULO BRASILEIRO DA INTERNET SOCIETY AO PROCESSO DE DESENVOLVIMENTO DE POLÍTICA "HABILITADORES DE UMA INTERNET ABERTA, GLOBALMENTE CONECTADA, SEGURA E CONFIÁVEL"

SUMÁRIO EXECUTIVO

A contribuição da ISOC Brasil considera os documentos do PDP na forma, conteúdo e narrativa. Em cada eixo, são apontadas vantagens e deficiências, pois as sugestões formais não resolverão as fragilidades de conteúdo ou narrativa e vice-versa. E uma visão global da ampliação do IIAT aponta sugestões específicas, melhorias abrangentes e reflexões gerais.

A partir das seis questões guia, nossa visão pode ser resumida nas seguintes considerações:

I. Importância e desafios:
   A. O esforço para conceber os habilitadores é em si louvável e valioso, mas tem desafios.
   B. A falta de precisão semântica na formulação das perguntas associadas aos habilitadores pode dificultar a aplicação do Kit de ferramentas ampliado como um padrão.
   C. Uma visão holística e contextualizada na aplicação do Toolkit pode permitir às comunidades saberem melhor das situações umas das outras.

II. Problemas com os exemplos:
   A. As restrições para usuários se conectarem à Internet não devem ser avaliadas em conjunto com as barreiras enfrentadas por quem opera os serviços de conexão ou roteamento, transmissão e comutação.
   B. A *colaboratividade no desenvolvimento, na gestão e na governança* deveria considerar as questões dos pontos de troca de tráfego.
   C. A acessibilidade irrestrita deve tratar adequadamente das questões de censura.
   D. A capacidade disponível deveria considerar os possíveis efeitos negativos de um controle privado não regulamentado.
   E. A confidencialidade de dados de informações, dispositivos e aplicativos deveria considerar as questões do Brasil com o WhatsApp, pois são muito comuns no mundo.
   F. A integridade de informações, aplicativos e serviços deveria citar casos mais relevantes e recentes, como o Pegasus.
   G. A confiabilidade, resiliência e disponibilidade deveria abordar situações de agressões e ameaças online, como violência política contra mulheres.
   H. A responsabilização poderia destacar riscos para liberdade de expressão e censura a conteúdos em mais idiomas que o inglês, especialmente considerando a imprecisão do conceito de terrorismo.
   I. A privacidade poderia citar rastreabilidade.

III. Aplicabilidade no Brasil
   A. Projeto de Lei n. 2630/2020
   B. Lei nº 14.172 / 2021
   C. Tarifação zero
   D. Adesão à Convenção de Budapeste

IV de. Perspectivas:
   A. A adição dos habilitadores aos objetivos aspiracionais no quadro de trabalho ajuda a atuar sobre os temas mais sensíveis aos usuários finais como discurso de ódio, desinformação, vírus de computador.
   B. Apesar da consistência interna, falta ao documento uma ponte com a proposta do ano passado, e uma correlação mais próxima entre propriedade críticas do IWN, objetivos aspiracionais da ISOC e Habilitadores: a narrativa do IIAT deveria criar um elo conceitual mais sólido entre essas 3 peças; e
   C. Outros estudos de caso complexos, olhando para vários países e regiões, deveriam ser desenvolvidos dentro de 12 meses como um teste de resistência coordenado do IIAT.

RELATÓRIO COMPLETO

A Internet Society tem trabalhado no projeto "Internet Way of Networking" (IWN, na sigla em inglês), a fim de promover e ressaltar um conjunto de cinco propriedades críticas da rede:

1. Uma infraestrutura acessível com um protocolo comum;
2. Arquitetura aberta de blocos de construção interoperáveis e reutilizáveis;
3. Gerenciamento Descentralizada e Sistema Único de Roteamento Distribuído;
4. Identificadores globais comuns;
5. Uma rede de propósito geral e tecnologicamente neutra.

Nesse esforço, a ISOC lançou o "Internet Impact Assessment Toolkit" (IIAT), como parte do processo regulatório, destinada à análise de políticas públicas, regulações e práticas privadas. Mas o papel das propriedades críticas na promoção e proteção do IWN como modelo preferido entre outros possíveis e indesejáveis não se mostra suficiente para o alcance do máximo potencial da Internet.

Assim, em expansão do IIAT, foram propostos, como aspectos adicionais de avaliação ligados aos objetivos aspiracionais da ISOC, dez "Habilitadores de uma Internet Aberta, Globalmente Conectada, Segura e Confiável", em uma lista não exaustiva:

1. Acesso fácil e irrestrito;
2. Uso e implantação irrestritas de tecnologias de Internet;
3. Colaboratividade no desenvolvimento, na gestão e na governança;
4. Acessibilidade irrestrita;
5. Capacidade disponível;
6. Confidencialidade de dados de informações, dispositivos e aplicativos;
7. Integridade de informações, aplicativos e serviços;
8. Confiabilidade, resiliência e disponibilidade;
9. Prestação de contas; e
10. privacidade.

O presente Projeto de Desenvolvimento de Políticas (PDP) inclui, portanto, a) uma Introdução atualizada ao Kit de Ferramentas e b) um "livro branco" sobre os habilitadores. Ambas as propostas estão sujeitas a análise da comunidade até 20 de setembro.

A fim de nortear as contribuições, as seguintes questões foram apontadas como guias:

1. Esses habilitadores fazem sentido?
2. Há algo faltando na descrição deles e os exemplos são úteis?
3. Você teria outros exemplos, positivos ou negativos, que gostaria de compartilhar?
4. Trata-se de uma narrativa útil para você e sua comunidade? Os habilitadores ajudariam no uso do kit de ferramentas em seu contexto local ou regional?
5. Você teria sugestões de melhorias ou ideias sobre como este kit de ferramentas pode ser usado pelos membros e aliados da Internet Society?
6. Você teria interesse em produzir sua própria análise usando esta versão expandida do kit de ferramentas?

A partir de nossas respostas a essas seis perguntas norteadoras, estruturamos as seis seções a seguir.

1. Significado dos habilitadores

(Esses habilitadores fazem sentido?)

Em primeiro lugar, gostaríamos de elogiar a Internet Society pelo esforço de desenvolver uma estrutura para apoiar a avaliação das comunidades locais de fatores políticos, jurídicos e tecnológicos que poderiam afetar o ideal de uma Internet "aberta, globalmente conectada, segura e confiável". A abordagem é muito preciosa no propósito de gerar um instrumento adequado para a produção de avaliações padronizadas, exaustivas e completas de projetos de lei, propostas de políticas públicas e ações privadas com potencial impacto sobre a Internet.

É um verdadeiro desafio descrever objetivamente esses habilitadores e relacioná-los um a um com cada objetivo aspiracional da ISOC para a Internet, dado que ambos os grupos de conceitos parecem se conectar intrínseca e transversalmente. Nos termos em que propostos, os habilitadores têm coerência com uma moldura de trabalho abrangente e aplicável à diversidade das situações locais.

No entanto, consideramos que as questões norteadoras apresentadas no PDP podem melhorar. Apesar do objetivo de explicar cada facilitador, o conjunto de questões acaba abrindo interpretações muito amplas para cada conceito, gerando confusão e sobreposição entre diferentes facilitadores.

Por exemplo, a pergunta "*A mudança proposta cria uma barreira de entrada, como custos, despesas administrativas ou outras dificuldades?*" pode se aplicar, em certo contexto, ao habilitador *uso irrestrito e implantação de tecnologias de Internet* em vez de ao proposto *acesso fácil e irrestrito*. Similarmente, a pergunta "*O efeito da mudança é restringir quem pode participar, fechando a Internet?*" poderia se vincular melhor ao habilitador *acesso fácil e irrestrito* do que ao *uso irrestrito e implantação de tecnologias da Internet*.

Portanto, consideramos que as questões devem ser mais bem estruturadas, ou ter um conjunto adicional de explicações, a fim de melhor orientar seu uso.

Também acreditamos que uma visão holística sobre a aplicação do Kit de Ferramentas de Avaliação de Impacto também seria muito interessante. Qualquer caso concreto específico deveria ser sujeito à avaliação à luz do conjunto total de objetivos e habilitadores que compõem o quadro de trabalho, e não em relação a um único habilitador e objetivo.

O IIAT pode ser uma grande oportunidade para as comunidades locais se conhecerem a fundo. O ideal é que cada aplicação do kit de ferramentas produza um estudo de caso oferecido pelos capítulos ISOC, e que deve ser acompanhado por uma exposição socioeconômica que forneça aos atores externos uma visão contextualizada da avaliação de impacto local.

2. lacunas definição e estudos de caso utilidade

(tem algo faltando em sua descrição, e são os exemplos úteis?)

Fácil e acesso irrestrito

A definição do habilitador *acesso fácil e irrestrito* se concentra em tornar os serviços de Internet mais acessíveis e economicamente viáveis para usuários em geral, ao considerar a conexão um direito fundamental. No entanto, os exemplos apresentados no documento tratam de barreiras regulatórias e comerciais para as operadoras.

Essa abordagem aparentemente confunde os direitos de acesso dos usuários com os direitos comerciais das operadoras, de se conectarem à Internet e fornecerem serviços.

O primeiro exemplo apresenta as Diretrizes de Acessibilidade de Conteúdo da Web (WCAG), destinadas a promover o acesso à Internet para pessoas com deficiência – um bom exemplo de acessibilidade e de facilitar os serviços de Internet para todos. O segundo discute o licenciamento de espectro, que visa facilitar o acesso à Internet em áreas mal servidas pela infraestrutura tradicional de fibra e cobre. O terceiro exemplo aponta como, em alguns países, a regulamentação excessiva pode levar à falta de prestação de serviços e gerar monopólios – o que pode enfraquecer o acesso à Internet por falta de concorrência e, portanto, levar ao aumento dos custos para os usuários.

Se o objetivo principal deste habilitador é facilitar "tornar-se parte da Internet", o terceiro exemplo não parece ser adequado. Mesmo em economias nas quais a competição é generalizada e imposta por políticas e regulamentos, pode haver tendências para o desenvolvimento de monopólios.

Uso irrestrito e implantação de tecnologias de Internet

Entendemos que o habilitador *uso irrestrito e implantação de tecnologias de Internet* visa garantir que a infraestrutura da Internet esteja disponível como um recurso para todos "de forma responsável e equitativa". O caso do SecurID da RSA mostra como patentes e segredos comerciais podem ameaçar o desenvolvimento de serviços de Internet e impedir o aprimoramento da tecnologia.

Em oposição, o documento apresenta o protocolo de segurança do OAth, que permite aos usuários compartilhar suas senhas com outros aplicativos sem fornecer dados privados do usuário. Este deveria ser um exemplo de como os programas e protocolos de código aberto podem aprimorar a segurança do usuário. Ambos exemplos são bons para o habilitador em questão e devem ser mantidos como estão.

Colaboratividade No Desenvolvimento, Na Gestão E Na Governança

O habilitador *colaboratividade no desenvolvimento, na gestão e na governança* busca chamar a atenção para possíveis limitações ou restrições na manutenção de uma Internet aberta e colaborativa.

Seu primeiro exemplo discute os *Registries* Regionais da Internet, um mecanismo descentralizado de tomada de decisões que permite o cumprimento e a manutenção deste objetivo. O segundo exemplo se refere aos Pontos de Troca de Trafego (PTT), os quais "oferecem às operadoras de redes comunitárias a oportunidade de se conectarem e trocarem tráfego na Internet".

Este poderia ser um modo eficiente de expandir a abertura da Internet, com o potencial de envolver mais operadoras regionais e, portanto, beneficiar as comunidades locais. Ainda assim, não considera as possibilidades materiais e ativos necessários para que os PTTs sejam implementados, sendo a "fadiga do doador" de equipamentos uma preocupação constante, como apontou o IGF 2016.

Acessibilidade irrestrita

Com relação ao habilitador *acessibilidade irrestrita*, o documento aponta que recursos e tecnologias devem estar disponíveis para os usuários da Internet e que deve ser assegurado que "não haja bloqueio de uso e acesso legítimos a esse recurso por terceiros".

O primeiro exemplo discute o desenvolvimento de outros protocolos de Internet pela comunidade para contornar as limitações impostas pelo uso universal dos endereços IPv4, permitindo uma Internet mais segura e confiável para os usuários. Talvez esse primeiro exemplo pudesse ser reformulado para deixar claro que o foco

não é a escassez de endereços IPv4, mas os esforços da comunidade aberta da Internet para contornar essa limitação.

O segundo exemplo discute a proibição de serviços VoIP em alguns países pelos governos, o que cria "ineficiências econômicas, impõe custos elevados e serve para isolar os usuários naquele país". Isso parece estar mais preocupado com as questões econômicas de bloqueio dessas tecnologias, em vez de destacar a vigilância de ativistas e minorias políticas, ou censura, que são questões graves, como apontado pelo relatório Freedom Of The Net 2020 sobre a Índia.

Capacidade disponível

Com relação ao habilitador *capacidade disponível*, o documento chama atenção à preocupação com medidas que poderiam diminuir a disponibilidade de recursos da Internet, como a largura da banda e outras capacidades.

O primeiro exemplo, sobre o projeto Starlink da SpaceX, parece ingênuo quanto aos interesses econômicos e privados em jogo. Ele desconsidera os efeitos negativos de uma empresa privada com tal impacto na disponibilidade da Internet, bem como outras práticas maliciosas que podem surgir no futuro, como o dumping. Neste ponto, os especialistas estão preocupados que o governo da Alemanha tenha contratado Google e T-Systems para armazenamento de dados de cidadãos.

O controle privado sobre tais capacidades não deveria ser menosprezado, pois poderia levar a profundos efeitos negativos no futuro, especialmente em países do Sul Global – onde atores privados, não raro, tiram vantagem econômica com contratos maliciosos em democracias de baixa intensidade e regimes autoritários.

Confidencialidade de dados de informações, dispositivos e aplicativos

Em relação à *confidencialidade dos dados de informações, de dispositivos e de aplicativos*, o documento preconiza a manutenção da confidencialidade e privacidade das informações dos usuários.

O primeiro exemplo destaca que, sendo "padrão de toda a indústria que requer criptografia quando os dados são enviados pela Internet, o PCI DSS aumenta a confidencialidade dos dados em repouso e em movimento". É um bom exemplo e deve ser mantido como está, assim como o terceiro exemplo, sobre WebPKI.

Mas o segundo, sobre a tentativa do governo de Maurício de descriptografar as comunicações dos usuários com a justificativa de segurança nacional, deveria enumerar mais situações semelhantes, pois essa parece ser uma solicitação muito comum em todo o mundo.

Integridade de informações, aplicativos e serviços

Com relação à *integridade de informações, de aplicativos e de serviços*, o documento trata da integridade de dados e manipulação maliciosa do Sistema de Nomes de Domínio e de sistemas de roteamento. Ambos os exemplos fornecidos satisfazem a compreensão do habilitador. No entanto, o documento não menciona ameaças relevantes à segurança cibernética, como o software Pegasus da NSO, detalhado na seção 3.

Confiabilidade, resiliência e disponibilidade

Com relação ao habilitador *confiabilidade, resiliência e disponibilidade*: o documento propõe que devam os serviços da Internet estar disponíveis de modo previsível para os usuários – considerando que sempre existirá um nível aceitável de erros e outros desafios para as operações normais. Seu primeiro exemplo, *statuspage.io*, mostra o status do serviço dos provedores de Internet. O segundo menciona "bloqueios deliberados da Internet" em alguns países, especialmente durante tempos de agitação civil, o que representa um efeito negativo sobre o

objetivo de uma Internet confiável. Ambos são bons exemplos e devem ser mantidos como estão. No entanto, também seria proveitoso considerar a falha das empresas e do Estado em fornecer mais previsibilidade no tratamento das vítimas de danos online.

Responsabilização

Com relação ao habilitador *responsabilização*, o documento lista os riscos de autoridades não transparentes e procedimentos de tomada de decisão ocultos que podem afetar a confiança dos usuários na Internet.

O exemplo do Fórum Global da Internet para Conter o Terrorismo destaca especialmente a ausência de um banco de dados auditável, que opera com *hashes* e pode levar a erros e equívocos, sem possibilidade de supervisão externa. O documento deveria apontar riscos para a liberdade de expressão, como a censura de conteúdo não anglófono. Além disso, o banco de dados também poderia produzir algum tipo de ruído, já que "terrorismo" é uma categoria altamente controversa e difícil de definir nas ciências sociais.

Privacidade

O documento aponta possibilidades de violação do direito à privacidade dos usuários e propõe que os estes possam entender como suas informações são coletadas, armazenadas e compartilhadas, destacando fortemente a possibilidade de anonimato. Menciona (1) a Lei de Segurança Online do governo britânico; (2) a Lei de Privacidade do Consumidor da Califórnia de 2018 (CCPA); e (3) o GDPR da UE.

O primeiro é citado como um exemplo negativo, pois permite a interrupção da comunicação ponta a ponta, o que seria uma abordagem prejudicial para lidar com os danos online. Nessa mesma direção, sugerimos que o documento também mergulhe, como outro caso relevante, no debate da "rastreabilidade" na Índia e no Brasil, conforme detalhado na próxima seção.

3. Casos de uso adicionais

(Você teria outros exemplos, positivos ou negativos, que gostaria de compartilhar?)

O documento poderia se beneficiar da inclusão dos seguintes estudos de caso.

Primeiro, em relação a ambos habilitadores *capacidade disponível* e *privacidade*, os contratos do governo alemão com o Google e a T-Systems para o armazenamento de dados dos cidadãos devem ser adicionados como exemplo. Conforme destacado anteriormente, essas seções parecem desconsiderar o impacto potencial de empresas privadas tendo tal influência no armazenamento de dados públicos e nas capacidades da Internet. Podem surgir práticas maliciosas, como dumping e contratos prejudiciais para cidadãos em democracias de baixa intensidade e regimes autoritários.

Em segundo lugar, sobre ambos os habilitadores *confidencialidade de dados de informações, dispositivos e aplicativos* e *responsabilização*, poderiam ser adicionadas preocupações sobre os critérios do governo para auditar ou supervisionar as plataformas digitais, tendo como exemplos: (1) os incidentes jurídicos do WhatsApp no Brasil, de juízes tentando prender executivos a ameaças de processo por não descriptografar comunicações dos usuários, apesar do que prevê o Marco Civil da Internet no Brasil; (2) a previsão de "rastreabilidade" discutida tanto na Índia quanto no Brasil (Projeto de Lei nº 2630/2020, vulgo "Lei das Fake News"), e que tornaria as comunicações vulneráveis à vigilância privada e estatal, a pretexto de responsabilizar as plataformas; (3) a recente tentativa de Bolsonaro de modificar o Marco Civil da Internet com a Medida

Provisória nº 1.068/2021, que estabelecia uma regra proibindo as plataformas de moderar conteúdos e perfis, com exceções apenas para uma lista inconsistente e incompleta de "Justas Causas".

Terceiro, em relação ao habilitador *integridade de informações, aplicativos e serviços*, o documento poderia mencionar ameaças à segurança cibernética mais recentes e relevantes, como o software Pegasus da NSO, um estudo de caso paradigmático de perigosos contratos entre o setor privado e governos.

Em quarto lugar, no habilitador *confiabilidade, resiliência e disponibilidade*, a falta de confiabilidade pode ser ilustrada no documento ao descrever episódios ameaçadores e prejudiciais de opressão da esfera pública digital contra segmentos sociais vulneráveis, com instituições públicas e plataformas privadas falhando em fornecer segurança e respostas adequadas após os ataques. Isso está bem documentado, por exemplo, em um relatório do InternetLab e da Revista Azmina sobre a violência política online contra mulheres políticas durante as eleições municipais brasileiras em 2020. Isso poderia servir como um exemplo de um efeito negativo sobre o objetivo de uma Internet confiável como esses ataques e a falta de reações adequadas e equitativas (não apenas no Brasil) enfraquece o habilitador, reduzindo a confiabilidade e a disponibilidade.

4. Utilidade dos habilitadores para o uso do Kit de Ferramentas no contexto do Capítulo Brasileiro

(Trata-se de uma narrativa útil para você e sua comunidade? Os habilitadores ajudariam no uso do kit de ferramentas em seu contexto local ou regional?)

A ISOC Brasil acredita fortemente que o uso dos habilitadores propostos tem o potencial de contribuir para a avaliação de um conjunto de casos no Brasil. Por exemplo, em relação ao mencionado **Projeto de Lei 2630/2020**, (1) o habilitador *confidencialidade dos dados de informações, de dispositivos e de aplicativos* contribui para avaliar as implicações sobre o objetivo de uma Internet aberta, pois o Art. 25 prevê a criação de um Conselho de Transparência e Responsabilidade na Internet; e (2) aos habilitadores *privacidade* e *confidencialidade dos dados da informação, dispositivos e aplicações* contribuem para avaliar as implicações da rastreabilidade, objeto do Art. 10, sobre os objetivos aspiracionais de segurança e confiança.

Outro possível uso dos habilitadores envolve o veto presidencial ao Projeto de Lei nº 3477/2020, posteriormente derrubado pelo Congresso Nacional, o que impôs a sua promulgação. A **Lei nº 14.172, de 10 de junho de 2021**, previu a concessão de R$ 3,5 bilhões em 30 dias, para garantir o acesso à internet a estudantes e professores da educação básica pública. O Presidente impugnou a constitucionalidade da lei perante o Supremo Tribunal Federal (na Ação Direta de Inconstitucionalidade 6926) e afastou o prazo de repasse do dinheiro por meio de uma Medida Provisória (também questionada perante o STF, na ADI 6971). O habilitador *acesso fácil e irrestrito* permite avaliar objetivamente o efeito negativo da opção política do Bolsonaro sobre o objetivo aspiracional de abertura.

O habilitador *alcance irrestrito* contribui para avaliar os impactos sobre o objetivo aspiracional de conexão global decorrentes da comercialização de planos telefônicos de "**tarifação zero**" (*zero rating*) para determinados aplicativos e serviços online.

Ainda, para acompanhar e avaliar os caminhos da aparentemente inevitável adesão do país à Convenção de Budapeste sobre o Crime Cibernético em um futuro breve, dois objetivos aspiracionais poderiam ter sua avaliação facilitada pelos facilitadores: para a segurança, *confidencialidade de dados de informações, dispositivos e aplicativos* e *responsabilização* junto com *integridade de informação, aplicação e serviços*; e para a confiabilidade, *responsabilização* e *privacidade*.

5. Melhorias e sugestões de uso para o kit ampliado de ferramentas

(Você sugeriria melhorias ou idéias sobre como este kit de ferramentas pode ser usado pelos membros e aliados da Internet Society?)

Gostaríamos de, mais uma vez, elogiar o trabalho da ISOC sobre o conceito de "Habilitadores de uma Internet aberta, globalmente conectada, segura e confiável", como uma extensão do IIAT, que já se encontra embasado nas cinco "Propriedades Críticas" do modo de interconexão da Internet.

As propriedades críticas são muito relevantes para avaliar o risco de as políticas prejudicarem os fundamentos da arquitetura da Internet, por exemplo, impondo restrições ao fluxo livre ou roteamento de pacotes através das muitas redes que constroem a Internet. Mas, quando essas cinco propriedades foram propostas, em 2020, foi notada por muitos a sua restrição à arquitetura básica da infraestrutura da Internet.

Tem sido debatido que eles não seriam muito úteis para a comunidade avaliar o impacto de tecnologias e políticas que, de fato, afetam as camadas superiores da Internet, onde os usuários finais interagem diretamente com aplicativos, conteúdo e serviços. A maioria das preocupações atuais dos usuários finais e também dos legisladores e reguladores – como moderação de conteúdo, combate ao discurso de ódio e notícias falsas e segurança do usuário final em relação a malware de vários tipos – não estão diretamente relacionadas a essas cinco propriedades críticas do IWN, e não poderiam ser avaliada apenas sob elas.

Para a maioria dos usuários finais e legisladores, a Internet não é sua infraestrutura – da qual a maioria deles não está sequer ciente: são os aplicativos, serviços e conteúdo que ela oferece à sociedade. A definição do IWN parecia aprisionar a missão da Internet Society nas camadas inferiores da Internet (aparentemente como consequência de sua história e experiência "técnica") e, portanto, longe de muitas preocupações relevantes da atualidade.

A definição estratégica de "habilitadores" move a Internet Society a ampliar o IIAT para abordar essas preocupações, tornando-se assim relevante para uma gama muito maior de partes interessadas e criando um novo e estendido pano de fundo conceitual para seus esforços de advocacy.

No entanto, a estrutura geral resultante parece fragmentada. Agora falta diálogo entre as três peças conceituais: as cinco propriedades críticas do IWN, os quatro objetivos aspiracionais (Internet aberta, conectada globalmente, segura e confiável) e os (até o momento) dez habilitadores desses objetivos.

A proposta fornece "exemplos de diferentes políticas ou tecnologias específicas para um habilitador que avançam ou bloqueiam o objetivo na área identificada". Mas o documento não parece fazer um esforço para usar esses mesmos exemplos para avaliar o impacto dessas tecnologias ou políticas sobre as cinco propriedades críticas do IWN. Habilitadores e Objetivos, de um lado, e Propriedades Críticas, de outro, parecem dois mundos separados, pelo menos pela leitura do documento.

Alguns dos habilitadores podem ser facilmente relacionados aos objetivos aspiracionais e às propriedades críticas. Por exemplo, o objetivo de uma "Internet aberta" - o documento afirma que "uma Internet aberta é uma Internet acessível - é fácil conectar-se à Internet aberta e utilizar seus serviços". Esta afirmação pode ser interpretada como se referindo, por exemplo, tanto à conexão de novas redes (que mapeiam diretamente para as Propriedades Críticas) quanto aos serviços e aplicativos na camada superior da Internet. Um dos habilitadores desse objetivo aspiracional é o *acesso fácil e irrestrito*. Mas nenhum dos três exemplos ilustra como esse habilitador pode ser afetado por tecnologias e políticas públicas relacionadas à infraestrutura da Internet e, portanto, às cinco propriedades críticas. Considerações semelhantes podem ser feitas sobre os outros Objetivos Aspiracionais e exemplos.

Portanto, parece desejável que a Internet Society faça um esforço adicional para criar uma estrutura mais consistente e menos fragmentada, particularmente unindo as cinco Propriedades Críticas, de um lado, e as Metas Aspiracionais e Habilitadores, de outro.

Parece que, na verdade, muitos aspectos e recursos podem ser reconhecidos como um habilitador. A criação de uma lista bastante limitada, com títulos e expressões específicos abertos à interpretação, pode sair pela culatra e gerar confusão em vez de esclarecer o papel de cada facilitador. Apesar de deixar claro que pode haver habilitadores adicionais e que a lista será atualizada, seria melhor simplesmente ter uma definição de trabalho sobre o que facilita os objetivos aspiracionais e o que funciona na outra direção, criando obstáculos e prejudicando aqueles objetivos, ou apenas "desabilitando". A Internet é muito complexa para limitar tanto os habilitadores quanto os desabilitadores da abertura, segurança, confiabilidade e conectividade global a uma lista fechada e confinada de expressões. Deve caber aos *stakeholders* e à comunidade articular tudo o que o possibilita ou não, a partir de um conceito sólido para ambas as categorias, oferecido pela ISOC.

Talvez, como um primeiro e prático passo nessa direção, devam ser buscados exemplos que ilustrem como as tecnologias e políticas impactam não apenas os habilitadores, mas também e principalmente as cinco Propriedades Críticas do Modo de Interconexão da Internet. Em uma perspectiva mais ampla, toda a narrativa do IIAT deve ser adaptada, criando uma ligação conceitual mais sólida para essas três peças: Propriedades Críticas, Metas Aspirativas e Capacitadores.

6. Aplicações de interesse do Brasil para o kit ampliado de ferramentas

(Você teria interesse em produzir sua própria análise usando esta versão expandida do kit de ferramentas?)

ISOC Brasil se propõe a desenvolver, nos próximos meses, estudos de caso mais complexos sobre o uso do IIAT, que deve abranger simultaneamente vários Habilitadores, apontar impactos positivos e negativos em diferentes Objetivos Aspiracionais e permitir a avaliação de seus efeitos nas propriedades críticas do IWN. Exemplos como este podem ajudar a construir uma ponte sólida entre Propriedades Críticas e Ativadores, um link que parece estar faltando na proposta atual para a descrição expandida do IIAT.

A intenção é realizar um teste de resistência do IIAT por meio de tais estudos de caso: mais robustos, desenvolvidos por mais tempo e tendo em mira um grande país do sul global, com realidade complexa e peculiar para o desenvolvimento e uso da Internet. Por coerência, a ISOC Brasil sugere fortemente que outros estudos de caso igualmente complexos, tendo em vista outros países e regiões, sejam desenvolvidos como parte de um esforço coordenado de testes de resistência do IIAT, a se realizarem num prazo de 12 meses. Em seguida, à luz do aprendizado obtido com tais estudos, a ISOC estaria em melhores condições para elaborar uma revisão completa do IIAT, em um novo processo colaborativo com sua comunidade.

CRÉDITOS

Essa contribuição foi elaborada coletivamente por integrantes do Grupo de Trabalho sobre Responsabilidade de Intermediários (GTRI-ISOC Brasil) do Capítulo Brasileiro da Internet Society, que se dispuseram a integrar uma Força Tarefa dedicada ao Processo de Desenvolvimento de Política "Habilitadores de uma Internet Aberta, Globalmente conectada, Segura e Confiável".

Membros da Força-Tarefa Habilitadores do PDP

Alexandre Arns Bruna Martins dos Santos Camila Akemi Giovanna Michelato	Flávio Rech Wagner Paulo Renà da Silva Santarém Raquel Gatto Roberta Battisti	Rodrigo Duarte Thais Aguiar Yasmin CurziGTRI

O **GTRI-ISOC Brasil**, liderado por Bruna Martins dos Santos e Paulo Renná da Silva Santarém, na condição de Consultores Sênior de Políticas Públicas do ISOC Brasil, dá continuidade aos trabalhos do Capítulo sobre o tema da responsabilidade de intermediários. Seu propósito é desenvolver e implementar estratégias para a preservação do regime jurídico previsto no Marco Civil da Internet e para a difusão do Decálogo da ISOC Brasil de Recomendações sobre o Modelo Brasileiro de Responsabilidade de Intermediários.

O **Capítulo Brasileiro da Internet Society** é uma organização da sociedade civil brasileira, sem fins lucrativos, com estrutura autônoma, cujo objetivo é fomentar e promover localmente a missão e os princípios da ISOC.