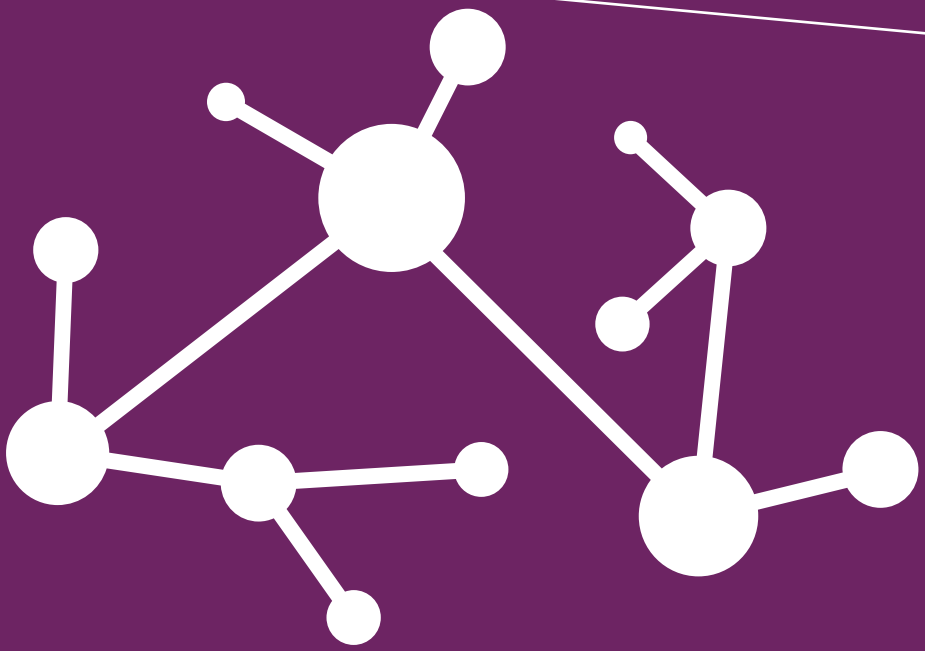
ARTICLE 19



Conectando: liberdade de expressão, empresas de telecomunicações e provedores de internet

Junho 2017

ARTIGO 19
Rua João Adolfo, 118, 8o andar
São Paulo- SP
Brasil
T: +55 11 30570071
E: comunicacao@artigo19.org
W: www.artigo19.org
Tw: @artigo19
Fb: facebook.com/artigo19brasil

© ARTIGO 19, 2017

Esse trabalho é distribuído conforme a licença Creative Commons 2.5 Atribuição -Não-Comercial-Compartilhamento pela mesma licença. Você é livre para copiar, distribuir e exibir este trabalho e para fazer trabalhos derivados, desde que:

1) dê crédito à ARTIGO 19;

2) não utilize esta obra para fins comerciais;

3) distribua quaisquer trabalhos derivadas desta publicação sob uma licença idêntica a esta.

Para acessar o texto legal completo desta licença, visite: http://creativecommons.org/licenses/by-ncsa/2.5/legalcode.

A ARTIGO 19 gostaria de receber uma cópia de quaisquer materiais em que as informações deste relatório sejam usadas.

Os Princípios foram desenvolvidos como parte da Iniciativa Espaço Cívico financiada pela Cooperação para o Desenvolvimento Internacional da Suécia, Sida. Sida não compartilha necessariamente das opiniões aqui expressas. A ARTIGO 19 tem a responsabilidade exclusiva pelo conteúdo do documento.

Sumário Executivo

Nessas diretrizes políticas, a ARTIGO 19 analisa as responsabilidades das empresas de telecomunicações (telcos) e provedores de serviços de Internet (ISPs) por proteger e respeitar os direitos humanos, em particular o direito à liberdade de expressão e por reparação em caso de violações desses direitos.

A ARTIGO 19 considera que a extensão das responsabilidades das telcos e ISPs pelos direitos humanos reflete o papel fundamental que essas empresas desempenham em permitir que os indivíduos exerçam o seu direito à liberdade de expressão. Essas diretrizes políticas exploram os contornos destas responsabilidades. Nosso ponto de partida são os Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos (os Princípios Orientadores), que exigem das telcos e ISPs que integrem salvaguardas de direitos humanos e mitiguem impactos sobre os direitos humanos.

Recomendamos que, a fim de garantir que as empresas de telecomunicações e ISPs cumpram com as suas responsabilidades no que diz respeito aos direitos humanos, em particular com os Princípios Orientadores, eles devem assegurar que, em suas operações, será incorporada a abordagem dos princípios fundamentais de direitos humanos, nomeadamente:

- **respeito pelos direitos humanos:** os termos de serviço devem estar disponíveis e acessíveis ao público, formulados com precisão suficiente para permitir que os usuários compreendam suas implicações e possam regular sua conduta em conformidade e restringir o exercício dos direitos humanos dos usuários apenas quando necessário para atingir um objetivo legítimo e proporcional a esse objetivo;

- **participação**: os usuários devem ter o direito de participar nas decisões que implicam seus direitos humanos. Os termos de serviço devem ser baseados na obtenção de consentimento expresso e livre dos usuários e devem garantir que os usuários serão notificados de medidas que potencialmente violem seus direitos humanos;

- **empoderamento**: os usuários devem estar suficientemente informados e capacitados para se envolver com os termos de serviço e contestá-los sob certas circunstâncias. Os usuários devem ter o controle sobre suas informações pessoais de uma forma que seja consistente com o direito à liberdade de expressão;

- **não-discriminação e igualdade:** os usuários de Internet devem ter acesso não-discriminatório à Internet, seus conteúdos on-line e dados pessoais devem ser tratados igualmente e sem discriminação;

- **responsabilidade ética:** os termos de serviço devem ser transparentes e claros sobre as condições em que os direitos humanos dos usuários serão restritos. Em particular, os termos de serviço devem divulgar como e em que condições telcos e ISPs irão responder a requisições do governo e pedidos de divulgação de dados pessoais. Os termos de serviço devem fornecer uma solução eficaz para indivíduos contestarem tais decisões.

As diretrizes políticas também fornecem recomendações detalhadas sobre medidas específicas que são implantadas por empresas de telecomunicações e ISPs a mando do Estado - incluindo desligamentos de rede (shutdowns), vigilância estatal, a geração e retenção de determinados dados pessoais, a proibição de determinadas aplicações ou serviços voluntariamente em alguns casos ou impulsionados por interesses comerciais. As recomendações específicas abordam como o setor privado deve trazer tais práticas em conformidade com o direito internacional dos direitos humanos estabelecido.

Índice

Introdução

O acesso à Internet - bem como a conectividade digital de maneira mais ampla[1] - já não é mais reservada somente a quem possui grandes fortunas, mas tornou-se um requisito essencial para todos, independentemente do status econômico ou educacional. É através de tecnologias digitais que a população do século XXI aprende, ganha, atua, movimenta e exerce uma série de direitos humanos, em particular os direitos à liberdade de expressão e informação, reunião e associação e educação.[2]

As tecnologias digitais tornaram-se também o meio pelo qual os Estados realizam uma gama de serviços sociais e públicos. Como resultado, alguns argumentam que a Internet - e sua espinha dorsal dos protocolos-chave e infraestrutura - pode ser considerada um bem público global que fornece benefícios para todos no mundo.[3]

Embora os Estados tenham muitas obrigações com relação à Internet, o acesso a ela é, na maioria das circunstâncias, mediada por atores privados. As empresas de telecomunicações (telcos) e provedores de serviços de Internet (ISPs) (em conjunto, os provedores) conectam os indivíduos com o complexo de infraestrutura de fios, cabos e satélites que lhes permitem "estar on-line." Além disso, os emergentes provedores comunitários representam uma forma alternativa de inclusão digital, desempenham um papel importante na diversificação do conglomerado de acesso à Internet e contribuem para a pluralidade e diversidade de modelos de conexão Internet. Provedores agem como um portal entre indivíduos e seu gozo dos direitos humanos e desempenham um papel crítico em permitir que as pessoas acessem serviços públicos e conectem-se com a informação do mundo.

Provedores frequentemente tomam medidas, a pedido dos governos, que ameaçam os direitos humanos dos indivíduos. Isto inclui desligar redes, restringir o uso de determinados serviços e aplicações, facilitar a desconexão punitiva do acesso para a violação de direitos autorais, facilitar a vigilância do governo e proibir a criptografia e o anonimato on-line. Mudanças e desafios emergentes, desde o advento das redes 5G até a intensificação dos debates sobre aplicação da lei para acesso a dispositivos criptografados, elevam este debate a um patamar ainda mais alto.

Cada vez mais, nós também estamos testemunhando provedores tomarem medidas em nome da conformidade com seus termos de serviço (também chamados de "termos e condições"), que prejudicam e põem em perigo os

direitos humanos, incluindo o direito à liberdade de expressão e informação. Essas medidas incluem ações unilaterais, como restringir o acesso a conteúdo on-line; gerar, reter e vender informações pessoais dos usuários e priorização de determinados tipos de conteúdo com base em sua origem, destino ou prestador de serviços.

Para agravar a assimetria de poder entre provedores e usuários, há falta de transparência e prestação de contas sobre como os termos de serviço são interpretados e aplicados. Tamanho, complexidade e linguagem legalista obscurecem a intenção dos termos de serviço. A natureza de "via de mão única" da relação entre provedores e usuários inibe o escrutínio genuíno ou negociação dos termos dessa relação. Os indivíduos raramente têm o direito de contestar a maioria dos termos de serviço ou até mesmo serem informados sobre as decisões adversas feitas por provedores, por exemplo, facilitar a vigilância do governo, divulgar dados a terceiros, prejudicar a neutralidade de rede ou desconexão de acesso. Os termos de serviço são frequentemente uma caixa preta que - sob o pretexto dos usuários terem consentido - ofuscam, ao invés de esclarecerem, o papel dos provedores e as suas obrigações contratuais para com seus usuários.

A ARTIGO 19 acredita que a compreensão do papel e das responsabilidades dos atores privados é essencial para proteger a liberdade de expressão e informação, bem como outros direitos humanos on-line. Assim, essas diretrizes políticas exploram os contornos dessas responsabilidades. Nosso ponto de partida são os Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos (os Princípios Orientadores), também conhecidos como os Princípios Ruggie, que exigem que provedores integrem salvaguardas de direitos humanos, mitiguem impactos sobre os direitos humanos em suas operações, publiquem relatórios de transparência e forneçam soluções eficazes para violações dos direitos humanos. Recomendamos que, a fim de garantir a conformidade com os Princípios Orientadores, os provedores estabeleçam termos de serviço que incorporem os princípios fundamentais de uma abordagem baseada no respeito por direitos humanos, participação, empoderamento, igualdade e responsabilidade ética.

O escopo deste documento

Uma complexa teia de atores constitui o setor responsável pela construção, fornecimento e manutenção dos componentes físicos e técnicos que compõem a Internet e garantem a conectividade. Para efeitos de atribuir responsabilidades a respeito dos direitos à liberdade de expressão e informação, a ARTIGO 19 sugere que esses atores privados podem ser divididos nas seguintes categorias:[4]

- **atores que prestam serviços essenciais, a fim de obter acesso à Internet**: esses incluem empresas de telecomunicações, provedores de acesso à Internet, operadores de rede e pontos de troca de tráfego;

- **atores que prestam serviços essenciais, a fim de obter acesso a informações na Internet:** esses incluem ICANN, registros e registradores de nomes de domínio, serviços de hospedagem web e buscadores;

- **atores que facilitam o compartilhamento de informações na Internet:** esses incluem plataformas de mídias sociais, blogs, fóruns on-line e e-commerce oferecendo serviços ou distribuição de conteúdo;

- **atores que produzem conteúdos:** isso inclui jornais e outros produtores de conteúdo, sejam autores individuais ou empresas;

- **outros atores**: incluindo fabricantes de computadores ou outros hardwares, desenvolvedores de softwares, empresas provedoras de serviços de armazenamento de dados ou serviços de nuvem e empresas de cibersegurança, que são essenciais para o fornecimento de segurança de rede.

Nós também poderíamos descrever esses atores como provedores de serviços na camada física, camada lógica, camada de conteúdo e camada social da Internet, respectivamente. As discussões sobre políticas pertinentes à proteção dos direitos humanos, incluindo o direito à liberdade de expressão, permeiam todas as quatro camadas; considerando que as mudanças políticas sobre uma camada terá um impacto direto sobre as outras, de uma forma ou outra.[5]

Nessas diretrizes políticas, nos concentramos em telcos e ISPs, as entidades privadas ou estatais que fornecem e mantêm a camada técnica da Internet, oferecendo aos indivíduos acesso à Internet por meio de serviços móveis ou de linha fixa. As diretrizes políticas se aplicam a ambos os provedores comerciais e comunitários.

Devido à complexidade e ao escopo dessa questão por si própria, não serão aqui abordadas entidades do setor privado que hospedam conteúdo (tais como provedores de hospedagem) ou aqueles que fornecem serviços e aplicações on-line (tais como plataformas de mídias sociais ou aplicativos de mensagens). Também excluímos redes de entrega conteúdo(CDNs), pontos de troca de tráfego (PTTs) e outras entidades cujos clientes são empresas ao invés de indivíduos; bem como a gama de outros atores privados cujas ações

têm implicações para a liberdade de expressão no contexto digital, incluindo fabricantes de hardware e desenvolvedores de software, produtores de conteúdo e detentores de direitos autorais, empresas prestadoras de armazenamento de dados ou serviços em nuvem, ou empresas de cibersegurança. Estes serão abordados em diretrizes políticas separadas da ARTIGO 19.

Essas diretrizes políticas baseiam-se em trabalhos anteriores da ARTIGO 19, que abordaram os papéis e responsabilidades dos intermediários no contexto da liberdade de expressão e de informação on-line[6] e também fornecem recomendações específicas tanto para os Estados e provedores nas respectivas áreas dessas diretrizes políticas.

Padrões internacionais aplicáveis

O setor de telecomunicações tem evoluído de diversas formas mundo afora. Em muitos lugares, as telecomunicações eram inicialmente monopólios estatais, que já se tornaram totalmente ou parcialmente privatizados e os mercados de telecomunicações foram abertos a novos atores , sejam nacionais ou estrangeiros.[7] Em outros contextos, o setor de telecomunicações sempre foi totalmente privado.[8]

No entanto, os Estados ainda têm interesses próprios em muitas empresas de telecomunicações em todo o mundo. Mesmo em mercados totalmente privatizados, o legado da propriedade estatal e o papel regulador do Estado continuam a caracterizar a relação estreita entre as empresas de telecomunicações e governos. Esta relação também é composta pela estrutura para licenciamento de telecomunicações, o que requer que telcos cumpram com os termos estipuladas pelo governo a fim de operar.

ISPs são mais propensos a serem atores privados, tendo surgido com o nascimento da Internet para fornecer a chamada "conectividade de última milha": ligando os usuários individuais com infraestrutura de telecomunicações existentes. Considerando que é menos provável que um ISP seja legado de propriedade estatal ou haja forte influência sobre ISPs, em muitos países ISPs operam como monopólios devido à falta de concorrência. Em alguns contextos, inclusive em comunidades rurais ou pobres, a falta de incentivos comerciais para ISPs para operarem vê recair para o Estado a obrigação de fornecer "conectividade de última milha". Recentemente, temos visto o surgimento de provedores de internet comunitários[9] que estão diversificando as oportunidades para acessar a Internet.

Todos os provedores - quer estatal, privado ou comunitário - têm a responsabilidade de respeitar e proteger os direitos humanos dos usuários de Internet, em particular os direitos à liberdade de expressão e informação e à privacidade. Essas responsabilidades, conforme elaborado sob os Princípios Orientadores, incluem deveres positivos para mitigar os impactos adversos aos direitos humanos, publicar relatórios de transparência e permitir vias de recurso.

Direito à liberdade de expressão e informação

O direito à liberdade de expressão é garantido no artigo 19 da Declaração Universal dos Direitos Humanos (DUDH), no Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP), bem como nos tratados regionais[10]. Ele engloba o direito não só de transmitir, mas também de buscar e receber informações e ideias de todos os tipos, independentemente de fronteiras. O direito de acesso à informação é cada vez mais aceito no direito internacional como parte integrante do direito à liberdade de expressão.[11]

O direito de acesso à Internet não é explicitamente reconhecido como tal pelo direito internacional e regional atual dos direitos humanos. No entanto, a evolução em determinadas legislações nacionais, juntamente com a evolução do direito internacional e regional de direitos humanos, está se movendo para incentivar todos os Estados a permitirem o acesso à Internet para todos.[13] O acesso à Internet também tem sido reconhecido como indissociavelmente ligado ao exercício da liberdade de expressão, como o relator especial da ONU sobre a liberdade de expressão e de opinião (Relator Especial sobre FOE)[12] observou em seu relatório de 2011:

> [...] o acesso à informação, a capacidade de exercer o direito à liberdade de expressão e a participação que a Internet proporciona a todos os setores da sociedade é essencial para uma sociedade verdadeiramente democrática.[14]

O direito de liberdade de expressão não é absoluto e pode ser limitado de acordo com condições rigorosas. Limitações admissíveis à liberdade de expressão são definidos no chamado "teste de três partes", que exigem que todas as restrições:

- estejam **previstas em lei**;
- Tenham um **objetivo legítimo** - exaustivamente previsto no artigo 19, parágrafo 3 do PIDCP para incluir: (a) o respeito dos direitos e da reputação de outrem; ou (b) a proteção da segurança nacional ou da ordem pública ou da saúde ou da moral públicas;
- são **necessárias e proporcionais** a esse objetivo.[15]

Essas limitações admissíveis aplicam-se igualmente às restrições à liberdade de expressão que ocorrem on-line. É importante ressaltar que a questão da proporcionalidade assume maior peso no contexto on-line uma vez que, devido à natureza da Internet, quaisquer restrições aos direitos humanos têm o potencial de afetar centenas de milhões de usuários de Internet. Avaliar se uma medida restritiva particular que afeta a Internet equivale a uma violação das normas de direitos humanos, portanto, requer uma compreensão diferenciada

das implicações técnicas e práticas para a liberdade de expressão e para a privacidade e reconhecimento dos impactos interjurisdicionais das restrições de acesso a serviços on-line e conteúdo. measure, which affects the Internet, amounts to a violation of human rights standards thus requires a nuanced understanding of the technical and practical implications for freedom of expression and privacy, and recognition of the cross-jurisdictional impacts of restrictions on access to online services and content.

Na Declaração Conjunta sobre a Liberdade de Expressão e a Internet de 2011, os quatro mandatos especiais para a liberdade de expressão[16] enfatizaram que, no contexto do acesso à Internet, a conformidade com o teste limitações admissíveis implica, entre outras coisas, que:

- medidas para bloquear sites específicos, serviços ou aplicações ou para negar às pessoas o direito de acessar a Internet são medidas extremas, que devem satisfazer os requisitos rigorosos do teste de três partes de limitações admissíveis;

- não deve haver discriminação no tratamento dos dados e tráfego da Internet com base no dispositivo, conteúdo, autor, origem e/ou destino do conteúdo, serviço ou aplicação;

- intermediários da Internet devem ser transparentes sobre todas as práticas de gerenciamento de tráfego ou de informação que empregam e informações relevantes sobre tais práticas devem ser disponibilizada de forma acessível a todos;

- cortar o acesso à Internet, ou a partes da Internet, para as populações inteiras ou segmentos do público (desligar o acesso à Internet) nunca pode ser justificado, inclusive conforme a ordem pública ou de segurança nacional.

Em junho de 2016, o Conselho de Direitos Humanos da ONU (CDH), em resposta a uma série de Estados que recentemente desligaram a Internet ou ferramentas de comunicação digital, inequivocamente condenou

> [...] Medidas para prevenir ou interromper o acesso ou divulgação de informações intencionalmente on-line em violação da lei internacional dos direitos humanos e clamou todos os Estados a absterem-se e cessarem tais medidas.[17]

A declaração fortemente redigida do Conselho de Direitos Humanos da ONU refletiu a gravidade do impacto de desligamentos de rede no gozo do direito à liberdade de expressão. Embora a resolução não elabore sobre quando a restrição ou interrupção do acesso à Internet violam o direito internacional, a Comissão de Direitos Humanos da ONU (Comitê de DH), que supervisiona o cumprimento dos signatários com as disposições do PIDCP, já havia estipulado que proibições totais de sites ou ferramentas equivalerão a uma violação:

> Quaisquer restrições à operação de sites, blogs ou qualquer outro baseado na Internet, eletrônico ou outro sistema de difusão de informação, incluindo sistemas para suportar tal comunicação, tais como os provedores de serviços Internet ou buscadores, só são admissíveis na medida em que sejam compatíveis com o parágrafo 3. Restrições permitidas geralmente devem ser específicas a conteúdos; proibições genéricas de funcionamento de determinados sites e sistemas não são compatíveis com o parágrafo 3. Também é incompatível com o parágrafo 3 proibir um site ou um sistema de divulgação de informações a partir de material publicado apenas com base que pode ser crítico ao governo ou ao sistema político-social defendido pelo governo.[18]

Direito à privacidade

O direito à liberdade de expressão está intimamente ligado com o direito à privacidade, em particular no contexto da Internet. A privacidade age como um escudo para garantir que as pessoas possam compartilhar ideias e buscar informações on-line sem serem submetidas à vigilância arbitrária e ilegal, monitoramento e coleta de dados, garantindo que elas possam exercer seus direitos de liberdade de expressão de forma confidencial e, se assim o desejarem, de forma anônima. Dessa forma, o direito à privacidade funciona para criar as condições necessárias para o livre e pleno exercício da liberdade de expressão e de informação on-line.

O direito à privacidade, consagrado no artigo 12 da DUDH, no artigo 17 do PIDCP e em tratados regionais,[19] proíbe a interferência ilegal na privacidade de um indivíduo, lar, correspondência e família. À medida que a Internet e as tecnologias digitais têm evoluído, entendimentos sobre a privacidade têm se expandido para incluir dados pessoais de um indivíduo, com a proteção de dados pessoais tendo sido derivada do direito à privacidade.

Proteção de dados pessoais

A primeira declaração internacional sobre o escopo do direito à proteção dos dados pessoais foi as Diretrizes da OCDE sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais de 1980, que desde então foi complementada pela Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados Pessoais (conhecida como Convenção 108)[20], as Diretrizes da Assembleia Geral da ONU para a Regulamentação dos Arquivos Informatizado de Dados Pessoais de 1990. Hoje, existem mais de 100 leis nacionais de privacidade de dados em todo o mundo,

Hoje, existem mais de 100 leis nacionais de privacidade de dados em todo o mundo, quase metade das quais são de fora da Europa[22] e muitas delas replicam de perto os padrões europeus. O Tribunal Europeu de Direitos Humanos e do Tribunal de Justiça da União Europeia (TJUE) estiveram na vanguarda de articular os contornos do direito à proteção de dados pessoais no que se refere à privacidade.[23] Instrumentos regionais que abordam essa questão também foram adotados pela Associação de Nações do Sudeste Asiático (ASEAN) e da União Africana.[24]

O direito à privacidade não é um direito absoluto; ele pode ser restringido conforme o mesmo teste de três partes mencionado acima aplicável à liberdade de expressão.[25] Como tal, atividades que interferem na privacidade dos indivíduos - como a vigilância objetiva da comunicação on-line ou a geração, coleta, retenção e uso de dados pessoais - podem ser justificadas desde que estejam em conformidade com a lei, necessárias para atender um determinado objetivo e proporcional a esse objetivo.

No contexto das atividades que envolvem a geração, coleta, retenção e uso de dados pessoais on-line, a lei de proteção de dados[26] prescreve restrições e salvaguardas para garantir que o processamento de dados não infringe o direito dos usuários de Internet à privacidade. Embora a regulação da proteção de dados seja diferente entre países e regiões, todas as leis de proteção de dados têm princípios comuns que dizem respeito ao tratamento de dados pessoais on-line:

equidade e legalidade: isso inclui a obrigação de obter o consentimento informado de um indivíduo antes de processar seus dados pessoais;

- **propósitos limitados**: os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas e não utilizados para outros fins incompatíveis;

- **minimização dos dados**: os dados devem ser limitados ao estritamente necessário, devendo ser adequados e relevantes;

- **precisão:** dados pessoais devem ser precisos e atualizados;

- **armazenamento limitado:** dados pessoais identificáveis não devem ser mantidos por mais tempo do que o necessário;

- **segurança e integridade:** as organizações devem adotar medidas técnicas ou organizacionais adequadas para garantir que os dados armazenados estejam

seguros;

- **responsabilidade ética e transparência:** as organizações devem ser transparentes sobre como elas estão processando dados e responsáveis por cumprir os princípios de proteção de dados.[27]

Responsabilidades do setor privado

Existe atualmente orientação considerável, na forma dos Comentários Gerais do Comitê de Direitos Humanos e observações finais, relatórios de relatores especiais e a jurisprudência dos tribunais regionais sobre as responsabilidades dos Estados no contexto da proteção do direito à liberdade de expressão e de informação na Internet.[28] No entanto, subsistem relativamente poucos materiais articulando as responsabilidades daqueles atores privados que mantêm e fornecem acesso à Internet e que muitas vezes atuam para facilitar a interferência do Estado no acesso à Internet.

Uma notável exceção são dois relatórios do Relator Especial sobre Liberdade de Expressão, incluindo o seu relatório 2017 para o Conselho de Direitos Humanos que analisou o papel e as responsabilidades do setor de acesso à Internet na promoção do direito à liberdade de expressão.[29] O relatório elabora sobre o atrito que surge quando obrigações legais domésticas do ISP conflitam com o direito internacional dos direitos humanos, em particular no contexto de desligamentos de rede, bloqueio de conteúdo, aplicação de direitos autorais, vigilância de comunicações e de interferência com a neutralidade de rede. O Relator Especial sobre FOE centrou-se nos deveres dos Estados de respeitar a liberdade de expressão no contexto de duas interferências particularmente graves: desligamentos da rede e vigilância das comunicações, bem como deveres dos Estados de assegurar a liberdade de expressão, proibindo priorização paga e regulação de serviços zero rating. Ele então passou a explorar os contornos da responsabilidade corporativa neste contexto, consubstanciando as obrigações dos atores do setor privado para realizar a devida diligência, abraçar salvaguardas de direitos humanos por design, construir influência, adotar estratégias de mitigação, publicar relatórios de transparência e garantir reparações eficazes estejam no lugar.

O marco estabelecido nos Princípios Orientadores sobre Empresas e Direitos Humanos: Implementação das Nações Unidas "Marco Proteger, Respeitar e Reparar[30] (os Princípios Orientadores) - ao lado dos anteriores dez princípios do Pacto Global da ONU,[31] - fornece um ponto de partida para articular o papel do setor privado no que diz respeito aos direitos humanos e à Internet.[32] Os Princípios Orientadores reconhecem a responsabilidade das empresas por respeitar os direitos humanos, independente de obrigações do Estado ou a implementação dessas obrigações, por:

- fazer uma declaração pública de compromisso de respeito dos direitos humanos, aprovado pela alta administração ou de nível executivo;

- a realização de avaliações de impacto de direitos humanos a fim de identificar, prevenir e mitigar os potenciais impactos negativos sobre os direitos humanos de operações de uma empresa;

- incorporar salvaguardas de direitos humanos por design, a fim de mitigar os impactos adversos, construir influência e agir coletivamente, a fim de fortalecer o poder vis-à-vis as autoridades governamentais;

- rastreamento e comunicação de desempenho, riscos e exigências do governo;

- fazendo reparações disponíveis quando impactos sobre os direitos humanos adversos são causados.

Algum trabalho tem sido desenvolvido para aplicar os Princípios Orientadores para as circunstâncias específicas de telcos e ISPs. Notavelmente, em 2013, o Diálogo Indústria de Telecomunicações (TID) desenvolveu o seu próprio conjunto de princípios orientadores para informar as políticas e os processos de seus membros internos.[33] A Iniciativa de Rede Global (GNI), que se concentra mais em empresas de Internet e intermediários do que as empresas de telecomunicações, também emitiu seus próprios princípios[34], que o Índice de Direitos Digitais Ranking de Responsabilidade de Corporativa usa - juntamente com os Princípios Orientadores das Nações Unidas - para classificar o desempenho de empresas de internet e de telecomunicações em uma base anual.[35]

Considerando que os princípios TID e GNI concentram-se principalmente no fornecimento de orientações às empresas sobre a forma como elas devem responder às demandas do governo, o Ranking de Direitos Digitais (RDR) olha para as obrigações dos ISPs quando se tratam de termos de serviço. RDR prescreve um conjunto de indicadores para ajudar a avaliar a adesão das empresas aos princípios de direitos humanos. Esses indicadores incluem, nomeadamente:

- a disponibilidade de termos de serviço e políticas de privacidade;

- notificação de alterações dos termos de serviço e de restrições ao conteúdo ou de acesso;

- quais são as informações divulgadas nos termos de serviço, tais como:

    - se a empresa proíbe determinados tipos de conteúdo ou atividades;

    - em que circunstâncias a empresa pode restringir os serviços aos usuários;

    - o processo que a empresa emprega para avaliar e responder a pedidos de governos para restringir conteúdos ou serviços;

    - quais são as informações de usuário que a empresa recolhe, com quem compartilha e por quanto tempo eles as mantêm;

- se o usuário da Internet pode acessar todas as informações que a empresa detém sobre eles;

- publicação de relatórios de transparência sobre solicitações governamentais e privadas para remover, filtrar ou restringir o conteúdo ou acesso ou para fornecer acesso aos dados armazenados ou comunicações em tempo real;

- publicação de dados sobre o volume e a natureza das medidas tomadas para fazer cumprir os termos de serviço;

- publicação de dados sobre gerenciamento da rede;

- se a empresa notifica os usuários de Internet quando seus dados foram solicitados pelos governos e terceiros;

- se a empresa implanta padrões da indústria de criptografia e segurança e permite aos usuários criptografar seu conteúdo.[36]

Esses indicadores, embora não sejam exaustivos e totalmente abrangentes, fornecem orientações de base importante para garantir que os termos de serviço levem em conta e não prejudiquem os direitos dos usuários de Internet à liberdade de expressão e à privacidade.

Medidas que comprometem os direitos humanos dos usuários

Uma série de medidas empregadas por empresas de telecomunicações e ISPs ameaça seriamente os direitos dos indivíduos à liberdade de expressão e à privacidade. Algumas dessas medidas são tomadas a pedido do Estado ou estão sujeitas a obrigação legal. Tais medidas incluem desligamentos de rede, vigilância estatal, geração e retenção de certos dados ou a proibição de determinadas aplicações ou serviços. Outras medidas são tomadas de forma voluntária, incluindo aquelas movidas por interesses comerciais: a geração e análise de quantidades excessivas de dados pessoais, por exemplo, ou a implementação de esquemas de priorização paga. Nesta seção, analisamos as práticas tomadas pelas telcos e ISPs que têm implicações para os direitos humanos. As recomendações específicas sobre como o setor privado deve trazer tais práticas em conformidade com o direito internacional dos direitos humanos são abordadas na seção seguinte.

Retirada de acesso

Desligamentos da rede

A centralidade da Internet para o exercício da liberdade de expressão na era moderna aumentou o apelo dos Estados para usar desligamentos em toda a rede para suprimir o acesso e disseminação de informações e ideias progressistas e dissidentes. Como resultado, a frequência de desligamentos da rede integrais e parciais, particularmente durante eleições[37] e outros tempos de agitação política, tem aumentado significativamente em anos recentes[38]. Desligamentos também têm sido utilizados durante os exames de admissão à universidade sob os auspícios da prevenção de cola[39] e durante os protestos e manifestações[40] para impedir que pessoas acessem comunicações móveis e de Internet.

Desligamentos de rede são efetuadas pelos provedores, agindo a mando - e muitas vezes em resposta às demandas diretas - dos Estados. Em algumas circunstâncias, tais exigências são baseadas em marcos legislativos nacionais, como os referentes a emergências e ameaças à segurança nacional[41], enquanto outros Estados aplicam pressão ou solicitam a cooperação de provedores para desligar redes na ausência de qualquer lei regulamento. Independentemente da existência de legislação nacional que se proponha autorizar desligamentos da rede, medidas generalizadas desse tipo nunca são permitidas conforme o direito internacional de direitos

humanos.[42]

Leis de respostas graduais

Desde 2009, vários países adotaram leis e políticas destinadas a penalizar infratores reincidentes de direito autorais por meio da desconexão punitivas de seu acesso à Internet. Leis de resposta graduais, também conhecidos como leis dos "três avisos e você está fora", envolvem retirada do acesso à Internet por empresas de telecomunicações de usuários responsáveis por múltiplas violações de direitos autorais.[43] Em algumas circunstâncias, os provedores cumprem voluntariamente com tais regimes, desconectam da Internet os usuários na ausência de ordens executivas ou judiciais.[44]

Quando o acesso à Internet é uma condição tão central para o gozo dos direitos humanos, retirar o acesso dos indivíduos torna-se uma interferência punitiva e séria para o direito à liberdade de expressão e outros direitos humanos. Como resultado, não pode ser considerado proporcional conforme o direito internacional de direitos humanos, independentemente de justificativa avançada.[45]

Restrições sobre o acesso

Provedores restringem, interferem e discriminam o tráfego de rede que eles manejam de maneiras diferentes. Uma categoria limitada de tais restrições é justificada por referência ao gerenciamento da rede, o que exige priorizar algum tráfego de rede para a governança eficaz dos fluxos de rede. No entanto, uma série de outras medidas seja de conteúdos, aplicações e serviços estão sendo priorizadas ou bloqueadas. Isso inclui:

- **priorização paga**, uma medida de angariação de receitas que vê provedores aceitando pagamentos de plataformas e provedores de serviços para priorizar o conteúdo com base na origem, destino ou fornecedor de serviços, entregando algumas categorias de conteúdo da Internet em velocidades mais altas, enquanto deliberadamente retardam ou reduzem outras categorias.

- **arranjos de taxa zero (zero rating)**, no qual provedores oferecem acesso a determinados conteúdos ou serviços gratuitamente e restringem o acesso a outros conteúdos ou serviços. Embora tais arranjos sejam vendidos como provedores de acesso a comunidades carentes que não seriam capazes de custear o acesso à Internet, eles têm o efeito de reduzir os conteúdos que os usuários são capazes de acessar, travando o livre fluxo de informações e fechando os usuários em "jardins murados"[46]. Alguns argumentam que "a

taxa zero é a única adequada para cenários onde a banda é extremamente cara ou onde a demanda por largura de banda é muito superior à oferta e a taxa zero é usada para incentivar o uso menor da banda", mas mesmo em tais situações deve-se evitar os danos de distorcer o consumo de conteúdo, a liberdade de expressão e privacidade, acesso a mercados e outros danos.[47] Assim, proporcionar acesso irrestrito à Internet completa é uma solução melhor do que a taxa zero a determinados conteúdos.

- **proibição de aplicações e serviços**: em diversos países, aplicações tais como voz sobre IP[48] ou aplicativos de mensagens instantâneas[49] e serviços s como redes privadas virtuais[50] são indisponibilizadas por provedores voluntariamente ou a pedido dos governos.

Cada uma dessas medidas viola um pilar primitivo e fundamental da Internet aberta: a neutralidade de rede. A neutralidade de rede (ou agnosticismo de conteúdo[51]) sustenta que o tráfego da rede - os "pacotes" que carregam conteúdo na Internet - não deve ser tratado de forma diferente com base em sua origem, destino ou fornecedor de serviços ou com base do tipo de serviço ou aplicação. Garantir a neutralidade de rede significa que os provedores não podem usar o seu controle sobre a infraestrutura de Internet para bloquear, desacelerar ou priorizar o acesso a conteúdo de determinadas origens ou provedores, para certos tipos de conteúdo ou para determinadas aplicações ou serviços.

A neutralidade de rede é um pré-requisito para assegurar o exercício igual e não discriminatório dos direitos à liberdade de expressão e informação. Sem ela, não há condições equitativas e a capacidade de usuários individuais para determinar como eles se relacionam com conteúdos e aplicações on-line é severamente prejudicada. Medidas para minar a neutralidade de rede também ameaçam o direito à privacidade e à proteção de dados, uma vez que dar efeito aos esquemas de priorização pode envolver provedores sujeitarem o tráfego de rede a um nível mais invasivo de escrutínio utilizando, por exemplo, inspeção profunda de pacotes.

A neutralidade de rede também é ameaçada pela iminente desenvolvimento do 5G, a próxima geração de conexão com a Internet móvel e as vastas capacidades expandidas que o 5G permitirá. Como as redes 5G serão capazes de atender a um conjunto extremamente diversificado de necessidades, o risco de que os provedores optem por criar "vias rápidas" para determinados tipos de conteúdo, por tratar alguns pacotes de dados com prioridade ou por reduzir a largura de banda é aumentado.[52] Em julho de 2016, algumas das maiores empresas de telecomunicações do mundo assinaram o Manifesto 5G[53] reivindicando a

necessidade de padrões de neutralidade de rede, aumentando os temores de que os direitos de liberdade de expressão serão subjugados a considerações de eficiência de rede.[54]

Porque elas interferem com os direitos à liberdade de expressão e informação, para as medidas que violam a neutralidade de rede estarem em conformidade com os padrões internacionais de direitos humanos, elas devem satisfazer o teste de limitações permitidas. A esse respeito, as medidas acima expostas levantam uma série de preocupações:

- **legalidade:** Não só esquemas de priorização paga e arranjos de zero de rating não estão previstos em lei como são muitas vezes proibidos por regulamento interno. Um número de países já proibiram serviços de zero-rating[55] ou promulgaram legislação interna exigindo que serviços taxa zero se abstenham de interferir excessivamente com a capacidade dos usuários para acessar o conteúdo livremente.[56] Em novembro de 2015, a União Europeia adotou regras sobre a neutralidade de rede que proíbem o bloqueio, redução ou discriminação no que diz respeito ao conteúdo on-line, aplicações e serviços, salvo exceções, tais quais: o cumprimento das obrigações legais, manutenção da integridade da rede e o gerenciamento de congestionamentos da rede em casos excepcionais e situações temporárias.[57]

- **necessário para satisfazer um objetivo legítimo e proporcional a esse objetivo:** restrições ao acesso a determinados conteúdos on-line, aplicações e serviços são suscetíveis de ser justificadamente necessárias para assegurar quer o respeito por direitos ou pela reputação de outrem ou para a proteção da ordem pública ou à moral. É possível que alguma priorização de conteúdo de rede possa ser justificável em situações excepcionais de urgência, por exemplo, por questão de segurança nacional ou de emergência de saúde pública. Em tais circunstâncias, no entanto, a fim de serem restrições proporcionais sobre o acesso, essas teriam de ser temporárias e limitadas às medidas estritamente necessárias para a solução da emergência.

Geração, retenção e divulgação de dados

Os provedores de internet estão situados em um ponto único da cadeia de valor das comunicações, um ponto que potencialmente lhes dá acesso a quantidades extraordinárias de informações sobre seus usuários. Desde dados de identificação recolhidas até dados de pagamentos, desde informações geolocalizadas de quando os usuários acessam um serviço até os detalhes dos sites que visitam e aplicativos que eles usam, desde o tamanho e tipo de conteúdo que os usuários

fazem o download até o conteúdo de mensagens de texto e, em alguns casos, de e-mails. Como tal, telcos e ISPs lidam com uma extensa quantidade de dados altamente privados e pessoais sobre seus usuários.

Certa quantidade de acesso aos dados pessoais pelos provedores é necessária. Claramente para faturamento da assinatura dos usuários, por exemplo, ou para conectar usuários de Internet a sites específicos. No entanto, a maioria dos dados que os provedores lidam só precisa ser mantida momentaneamente, não havendo determinantes de gerenciamento de tráfego para a sua retenção no longo prazo.

No entanto, com o aumento da comercialização de dados pessoais, as empresas de telecomunicações estão descobrindo os benefícios financeiros de geração, coleta e retenção de grandes volumes de dados pessoais que não são essenciais para a entrega do serviço, mas que juntos permitem que as empresas criem perfis monetários dos usuários. A revenda de dados pessoais a terceiros pode levar a um amplo compartilhamento dessas informações com empresas de publicidade e corretores de dados. Onde as empresas de telecomunicações oferecem serviços gratuitos, tais como redes Wi-Fi públicas, eles podem recolher ainda mais dados e compartilhar esses dados não só com pessoas jurídicas, mas também com os Estados.

Os Estados também estão alertas para o valor dos dados pessoais para as agências policiais e de inteligência e estão colocando obrigações cada vez mais onerosas aos provedores de telecomunicações para gerar e reter dados pessoais dos assinantes, de suas comunicações e de sites e aplicações[58] que eles acessam para facilitar os objetivos de vigilância do governo. Leis de retenção obrigatória de dados - que exigem dos operadores gerar, registrar dados e armazenar registros de comunicações por até dois anos - agora podem ser encontradas em países de todo o mundo.[59] Políticas de registro de nomes reais, que exigem aos operadores gravarem e verificarem a identidade dos usuários de serviços até mesmo pré-pagos também têm se proliferado.

Os dados sobre o uso pessoal de um indivíduo da Internet - "metadados" - podem ser tão sensíveis quanto o conteúdo de suas comunicações. Por esta razão, há um crescente reconhecimento judicial que os metadados merecem as mesmas proteções legais como a aplicável para o conteúdo. A Corte Interamericana de Direitos Humanos confirmou isso no contexto das chamadas telefônicas, afirmando:

[O direito à privacidade] aplica-se a conversas telefônicas independentemente

do seu conteúdo e pode até mesmo incluir tanto as operações técnicas destinadas a gravar este conteúdo gravando-o e ouvindo-o ou qualquer outro elemento do processo de comunicação; por exemplo, o destino ou origem das chamadas que são feitas, a identidade dos falantes, a frequência, hora e duração das chamadas, aspectos que podem ser verificados sem a necessidade de gravar o conteúdo da chamada, gravando a conversa. Em resumo, a proteção da privacidade se manifesta no direito que outros diferentes daqueles conversando podem não obter ilegalmente informações sobre o conteúdo das conversas telefônicas ou outros aspectos inerentes ao processo de comunicação, tais como as mencionadas.[60]

Como o TJUE observou, os dados manipulados por empresas de telecomunicações, tomado como um todo,

> [...] são suscetíveis a permitir conclusões muito precisas a ser desenhada sobre a vida privada das pessoas cujos dados foram retidos, tais como hábitos diários, lugares permanentes ou temporárias de residência, movimentos diários ou outros, as atividades realizadas, as relações sociais dessas pessoas e os ambientes sociais frequentados por eles. Em particular, que os dados fornecem os meios [...] de estabelecer um perfil dos indivíduos em questão, informações que não são menos sensíveis, tendo em conta o direito à privacidade, que o conteúdo real das comunicações.

A interferência acarretada por essa legislação [...] levanta questões referentes à compatibilidade não só com [os direitos à privacidade e à proteção de dados pessoais], mas também com a liberdade de expressão [...].[61]

Onde os Estados impõem requisitos sobre os provedores de gerar e conservar os dados, esses requisitos não irão respeitar o direito internacional dos direitos humanos quando constituem medidas generalizadas, que não são "nem necessárias nem proporcionais."[62]

O TJUE estipulou que a conformidade com os direitos de privacidade e liberdade de expressão exige do Estado estabelecer uma ligação entre os dados a serem retidos e o objetivo específico a ser perseguido, limitar a retenção de dados para períodos específicos de tempo, crimes ou localizações geográficas.[63]

Para além da retenção de dados imposta pelos Estados, os provedores devem limitar a quantidade de dados pessoais que necessitam armazenar sobre seus usuários, inclusive para fins de publicidade. Fazê-lo seria aumentar a sensação de privacidade dos usuários de Internet e empoderá-los a exercer seus direitos de livre expressão destituídos pelo temor de monitoramento. Além disso, asseguraria

que os provedores são capazes de cumprir com suas obrigações conforme os princípiosde proteção de dados, que obriga as empresas a minimizar a quantidade de dados que coletam e a excluir dados pessoais identificáveis uma vez que não sejam mais necessários. Ademais, as empresas não estão autorizadas a usar os dados coletados para uma finalidade - tais como facilitar o acesso dos usuários de Internet a aplicativos de mensagens - para outra finalidade incompatível, como a publicidade, sem primeiro obter o consentimento informado do usuário individual.

Facilitação da vigilância estatal

Embora os provedores de telecomunicações há muito tempo atuam como intermediários para a vigilância do governo, o escopo, diversidade e a gravidade atual dessas ações fazem os programas de intercepção anteriores parecerem pequenos. Na época de interceptações postais de correio e escutas terrestres era possível ver as telcos facilitando o acesso do Estado para uma pequena porcentagem de correspondência pessoal e telefonemas. Já os provedores de hoje são o canal através do qual quase toda comunicação, comércio, informação e conhecimento do mundo viajam. Como a computação promove avanços, os custos de armazenamento despencaram e as ambições de vigilância dos governos cresceram cada vez mais. Os provedores estão sendo requisitados - em alguns casos, forçados - a operar e potencializar aparatos de monitoramento global, em muitos casos, em violação das normas internacionais de direitos humanos.

Além de cumprir com os pedidos de acesso aos dados pessoais, de comunicação e de conteúdo (como abordado acima), há uma série de meios através dos quais as empresas de telecomunicações facilitam a vigilância do governo:

- adaptação de infraestruturas de telecomunicações ou remoção de proteções para permitir a vigilância do Estado;

- instalação de equipamentos de vigilância do Estado diretamente na infraestrutura de telecomunicações;

- autorização para ter acesso direto ou controle sobre a infraestrutura de telecomunicações para fins de vigilância.

Considerando a vigilância por parte das autoridades governamentais pode ser uma interferência justificável com base nos direitos humanos, ela deve respeitar o teste

de limitações permitidas. No contexto da vigilância das telecomunicações, as seguintes considerações são relevantes:

- **legalidade:** considerando que as medidas de vigilância devem ter uma base no direito interno e serem compatíveis com o Estado de Direito, em muitos países, a vigilância é um esforço completamente desregulado ou falha em não cumprir requisitos da lei. Leis de vigilância devem ser suficientemente claras e precisas para permitir aos indivíduos uma indicação adequada das circunstâncias em que as suas comunicações podem ser interceptadas e monitoradas.[64] Elas também devem indicar o alcance do poder discricionário concedido ao Executivo ou ao juiz para poder ordenar a vigilância e ser acompanhada de salvaguardas específicas.[65]

- **necessária para satisfazer um objetivo legítimo e proporcional a esse objetivo:** porque instrumentos internacionais de direitos humanos não prescrevem uma lista exclusiva de objetivos para os quais a vigilância pode ser legitimamente realizadas, os direitos humanos centram-se, ao invés disso, nas salvaguardas para prevenção contra o abuso das leis de vigilância, tais como leis que especificam processos de autorização, de supervisão e limites para a duração da vigilância.[66] As autorizações devem ser específicas, emitidas por autoridade judicial independente e sujeitas à existência de uma suspeita razoável contra a pessoa em causa.[67]

Satisfazer o teste de proporcionalidade requer um exame se teria sido possível alcançar o objetivo por meios menos intrusivos. Exige também levar em conta o impacto de direitos humanos da medida; no contexto das medidas de vigilância, que afetam potencialmente centenas de milhões de usuários de rede particulares, o teste da proporcionalidade muitas vezes deixará de ser satisfeito.

Reparações para as violações dos direitos humanos

Apesar de ser considerado um dos principais pilares dos Princípios Orientadores, as responsabilidades do setor privado por fornecer acesso a reparações efetivas são muitas vezes negligenciadas na elaboração de políticas. Na verdade, fornecer uma reparação eficaz para as violações dos direitos humanos tem sido chamado de "o pilar esquecido" do marco dos Princípios Orientadores. Além disso, os Princípios Orientadores se concentram principalmente sobre o dever do Estado para facilitar a correção e, como resultado, pensar sobre as responsabilidades do setor privado a esse respeito permanece subdesenvolvido.

Algumas recomendações foram desenvolvidas por organizações da sociedade civil. Por exemplo, o Plano de Reparações das Telcos da Access Now descreve os aspectos processuais e materiais de reparação no contexto de empresas de telecomunicações.[68] O Plano de Reparações baseia-se em uma orientação mais geral de organizações como o Conselho Europeu[69] Setor TIC Guia da Comissão Europeia sobre a implementação dos Princípios Orientadores sobre Empresas e Direitos Humanos[70] e fala especificamente para as etapas processuais e materiais que telcos e ISPs devem tomar a fim de permitir a reparação de violações dos direitos humanos dos usuários de Internet. Ele afirma que as empresas de telecomunicações devem apresentar uma ampla gama de medidas, nomeadamente:

Medidas processuais

- incorporar a questão da reparação em diligência com a ajuda de todas as partes interessadas antes de entrar em novos mercados ou oferecer novos serviços nos mercados existentes;

- procurar implementar mecanismos de reclamação que são acessíveis e seguros para os indivíduos;

- responder rapidamente e eficazmente às reclamações trazidas aos mecanismos de reclamação da empresa.

Medidas materiais

- investigar e descobrir maneiras de cessar ou alterar atividades que contribuem para os impactos adversos de direitos humanos de forma eficaz e oportuna;

- entrevistar executivos e funcionários que supervisionam e conduzem essas atividades violadoras de direitos e rever as políticas relevantes. Esclarecer se o pessoal desviou-se da política ou a política em si falhou. Para minimizar os riscos de reincidência, rever as políticas, reciclar funcionários e comunicar mudanças de política para o pessoal, parceiros de negócios e ao público;

- preservar as provas, sempre que possível e publicar quando for o caso, particularmente quando obstáculos fazem o acesso a uma reparação efetiva impossível no curto prazo. Nos casos em que o Estado instigou as atividades violadoras de direitos pelas empresas de telecomunicações, a evidência pode informar a busca de uma vítima para reparação eficaz, especialmente onde os Estados negam seu papel na vigilância ilegal, censura ou interferência na rede;

- após consulta às pessoas afetadas, reconhecer e pedir desculpas conforme apropriado para quaisquer contribuições para os abusos de direitos humanos. Em muitos casos, desculpas e garantias de não repetição podem percorrer um longo caminho no sentido de reparar a contribuição da telco para os danos que as vítimas sofreram;

- submeter-se à investigação independente ou supervisão em curso conduzida de forma independente da telco e com acesso total aos funcionários corporativos e registros. Os inquéritos devem proceder de forma transparente, com um prazo disponível publicamente e em coordenação com várias partes interessadas, incluindo a sociedade civil, especialistas legais e regulatórios e funcionários do governo. Supervisão contínua é necessária quando a mesma forma de violação tenha ocorrido repetidamente ou quando a infração é determinada como sendo o resultado de problemas sistêmicos dentro da empresa;

- organizar e participar em entidades regionais ou setoriais, com participação estruturada de múltiplas partes interessadas, para esclarecer e mitigar qualquer papel que as telcos desempenham em violações sistemáticas dos direitos humanos. Estes órgãos devem aderir às melhores práticas de transparência e responsabilidade ética, a ser determinado e atualizado em consulta com outras partes interessadas e de acordo com, horários regulares

disponíveis publicamente. Mudanças políticas e outros resultados devem também ser coordenados e avaliados em relação aos parâmetros estabelecidos;

- compensar as vítimas e as comunidades afetadas. Compensação como uma reparação para os abusos de direitos humanos tornou-se compreensível à luz do "Fundo Fiduciário para as Vítimas" do Tribunal Penal Internacional. Se o setor de telco estabeleceu um fundo desse tipo, poderia beneficiar de apoio setorial, tanto financeiro como moral, e desenhar sobre a vasta experiência das maiores telcos, fundações, governos, investidores e interessados da sociedade civil.

Os princípios articulados acima, embora não sejam abrangentes, fornecem uma base robusta para começar uma discussão sobre as responsabilidades das empresas de telecomunicações e ISPs para fornecer às vítimas de violações dos direitos humanos uma reparação eficaz. Quando aplicado às medidas violadoras de direitos humanos mais comuns cometidas por empresas de telecomunicações e ISPs, a ARTIGO 19 entende que a observância desses princípios requer que os provedores tomem várias medidas para remediar as violações da liberdade de expressão (veja a seção final).

Recomendações da ARTIGO 19

Recomendações gerais

A ARTIGO 19 sugere que os provedores adotem uma abordagem baseada nos direitos humanos para as suas operações, incorporando os seguintes princípios e recomendações. Também recomendamos que os provedores participem e procurem apoiar iniciativas de autorregulação para monitorar e promover os direitos humanos em conformidade com estas recomendações.

Recomendação 1: Conformidade com os princípios de direitos humanos internacionais

Telcos e ISPs devem assegurar que suas operações estejam adequadas às normas de direitos humanos internacionalmente reconhecidas. Onde as leis locais e exigências estatais conflitam com estes padrões, provedores devem procurar conformar-se aos princípios internacionais de direitos humanos na medida do possível.

Provedores não devem agir sobre quaisquer requisições estatais que manifestamente interferem nos direitos humanos a menos que tais ordens sejam emitidas por uma autoridade judicial independente e tenham esgotado todos os recursos disponíveis para contestá-las. Trabalhar em colaboração com empresas do mesmo setor para contestar exigências e envolver o público e a sociedade civil em tais exigências pode aumentar a influência dos provedores. É fundamental que os provedores implementem todas as requisições do Estado de uma maneira que minimize o impacto nos usuários finais individuais.

Sempre que possível, os provedores devem publicar informações sobre solicitações ou requisições emitidas por Estados que interferem nos direitos humanos. Se os provedores são colocados sob obrigações de sigilo, eles devem considerar a adoção de abordagens inovadoras, tais como mandado canário (um método em que os provedores são capazes de informar aos seus usuários se foram apresentadas a eles requisições do governo para facilitar a vigilância) para dar aos indivíduos uma indicação da existência de solicitações ou requisições.

Os provedores devem resistir ativamente a eventuais solicitações ou requisições

que poderiam tomar o controle da infraestrutura de telecomunicações do provedor e colocá-lo nas mãos do governo. Isto inclui, por exemplo, o governo exigir para fornecer acesso direto à infraestrutura dos provedores de serviços. Os provedores devem ir a todos os graus possíveis para evitar esta eventualidade.

Os provedores devem avançar em medidas inovadoras para melhorar os direitos das pessoas, em particular os direitos à liberdade de expressão e à privacidade, mesmo se tais medidas frustrem ou previnam solicitações e demandas do Estado. Isso inclui a aplicação de criptografia avançada para redes de telecomunicações, minimizando os dados recolhidos e retidos, a fim de minimizar o risco de revelação forçada.

Recomendação 2: Garantia de clareza e acessibilidade

Termos de serviço dos provedores devem estar disponíveis e publicamente acessíveis, formulados com precisão suficiente para permitir que as pessoas compreendam as suas implicações e regulem suas condutas em conformidade.

Os termos de serviço devem ser escritos em linguagem clara e não devem se esconder atrás de referências obscuras para cumprimento das leis locais. Eles devem listar explicitamente a legislação pertinente que as telcos devem cumprir e devem prever para o indivíduo as circunstâncias em que elas podem estar sujeitas a solicitações do Estado ou exigências que teriam impacto sobre os direitos do indivíduo à liberdade de expressão e privacidade. Os provedores devem explorar formas inovadoras de comunicar o impacto dos termos de serviço para seus usuários, incluindo o uso de iconografia, imagens e explicação interativa do seu conteúdo.

Os termos de serviço devem comprometer provedores ao cumprimento dos princípios internacionais de direitos humanos, na medida do possível. Eles devem assegurar aos indivíduos que os provedores irão contestar os pedidos e exigências estatais para retirada de acesso, restrição de serviços e aplicações, acesso a dados pessoais e cooperação com a vigilância do estado.

Os termos de serviço devem assegurar aos indivíduos que o provedor nunca vai desconectar os indivíduos à Internet como uma medida voluntária ou punitiva.

Os indivíduos devem ser capazes de acessar os termos de serviço dos provedores de uma forma livre e fácil. Ele deve ser acessível em uma variedade de formatos que levem em conta as diferenças de alfabetização, educação, idade e capacidade. Os termos de serviço devem usar a linguagem mais simples possível.

Recomendação 3: Participação

Termos de serviço devem oferecer aos indivíduos o direito de participar nas decisões que afetam seus direitos humanos

Os termos de serviço devem ser baseados na obtenção do consentimento informado e expresso dos indivíduos. A esse respeito, os termos de serviço devem exigir uma indicação explícita e não ambígua de consentimento dos indivíduos aos termos da relação com a telco. Consentimento para o uso, geração, análise e retenção de dados pessoais para certas finalidade só se aplica aos propósitos em que o provedor tenha divulgado diretamente para o indivíduo. Quando a telco pretende recolher mais dados pessoais ou usar os dados existentes de uma forma diferente e imprevista, eles precisam obter novo consentimento informado e não confiar apenas nos iniciais.

Os termos de serviço devem garantir indivíduos serão notificados de medidas que terão impacto sobre os seus direitos humanos. A esse respeito, os termos de serviço devem informar as pessoas sobre as circunstâncias sob as quais elas não serão notificadas, por exemplo, quando existir ordens de silêncio no contexto de vigilância.

Recomendação 4: Empoderamento dos indivíduos

Indivíduos devem estar suficientemente informados e capacitados para se envolver com os termos de serviço e contestá-los conforme certas circunstâncias.

Os termos de serviço devem indicar aos indivíduos quando eles têm o direito de contestar os termos da relação e como eles podem fazê-lo. Os indivíduos devem ser informados sobre os mecanismos de reclamação e de reparação disponíveis para permitir reclamações e solicitações de alterações relativas aos termos de serviço.

Os termos de serviço devem informar as pessoas do seu direito, a qualquer momento, de acessar todos os dados pessoais que os provedores mantém sobre elas e de solicitar a alteração ou supressão desses dados pelas telcos, bem como pelas subsidiárias com as quais os dados poderiam ter sido compartilhados como parte de qualquer acordo. Os indivíduos devem ter o direito de exportar os dados pessoais em um formato aberto e acessível.

Os provedores devem apoiar iniciativas de letramento digital concebidas para educar os usuários de Internet sobre a melhor forma de proteger a segurança e privacidade de suas informações on-line e, assim, facilitar a capacitação dos usuários. Eles também devem se envolver em uma cooperação de toda a indústria sobre as normas de portabilidade de dados, para garantir que a mudança entre provedores é uma realidade facilmente atingível e implementável para os usuários.

Recomendação 5: Não-discriminação e igualdade

Termos de serviço devem garantir que os indivíduos receberão acesso a conteúdos, aplicações e serviços sem discriminação.

A neutralidade de rede deve ser garantida nos termos de serviço. Os provedores devem garantir aos indivíduos que não discriminam o conteúdo das comunicações, com base em origem, destino ou fornecedor de serviços, ou que não restringem de forma alguma o conteúdo, aplicativos ou serviços que um indivíduo pode acessar, exceto no caso de exceções reconhecidas e, se necessário, para gerenciamento de tráfego. Serviços gratuitos não devem ser condicionados ao acesso restrito a conteúdos, aplicações ou serviços.

Os termos de serviço devem indicar aos indivíduos que o provedor está sujeito a ordens judiciais para restringir conteúdos, aplicações ou serviços e que os indivíduos serão notificados imediatamente se tais pedidos são recebidos. Os termos de serviço devem avisar aos usuários sobre o uso potencial de ordens de silêncio e as medidas que a telco tem colocado em prática para superá-las, como os mandados canários.

Medidas aceitáveis para gerenciamento de rede devem ser explicadas ao indivíduo de uma forma que seja clara e de fácil compreensão. Os usuários individuais devem ser capazes de participar em processos de monitoramento independentes e transparentes que garantam que a neutralidade de rede seja respeitada.

Os provedores devem publicar relatórios regulares de transparência, incluindo os detalhes de todas as ordens a que a telco está sujeita, de acordo com as quais o acesso a determinados conteúdos, aplicações ou serviços são restritos. Os provedores devem também publicar, pelo menos anualmente, informações sobre as práticas de gerenciamento de rede.

Recomendação 6: Responsabilidade ética

Nos termos de serviço, os provedores devem ser claros e transparentes sobre as condições em que os direitos humanos dos indivíduos serão restritos. Em particular, os termos de serviço devem divulgar como e em que condições os provedores irão responder às demandas do governo. Os termos de serviço devem fornecer uma via para indivíduos contestar tais decisões.

Os termos de serviço devem indicar explicitamente as circunstâncias que podem levar a uma violação da liberdade de expressão e ao direito à privacidade dos indivíduos. Eles devem mencionar as condições em que o provedor irá aceitar ou acatar às solicitações e exigências do Estado. Eles também devem indicar como os indivíduos podem acessar informações sobre os tipos e os números de pedidos e demandas a que o provedor tenha sido objeto e com o qual tenha cumprido.

Os termos de serviço devem definir em detalhes como os indivíduos podem acessar mecanismos de reclamação e de remediação para reclamar ou contestar a adesão da telco aos seus termos de serviço.

Recomendações específicas

Recomendações sobre desligamentos de rede (shutdowns)

Em face de solicitações ou exigências para facilitar medidas que violam claramente padrões de direitos humanos, os provedores têm a responsabilidade por respeitar princípios internacionais de direitos humanos, na medida do possível.[71] Isso implica a responsabilidade de tomar as seguintes medidas com relação a desligamentos de rede:[72]

Preparação e previsão

Identificar leis internas que poderiam ser usadas para ordenar desligamentos da rede;

- consultar atores locais da sociedade civil, companhias parceiras e outras fontes de informações para identificar situações em que o Estado pode ordenar um desligamento da rede;

- educar os funcionários sobre a possibilidade de um desligamento da rede e

elaborar uma estratégia de tomada de decisão, incluindo uma estratégia de comunicação pública para ser usada

Estratégias de resistência

- pedir esclarecimentos do governo quanto à intenção, duração e escopo do desligamento;
- esgotar os recursos internos para contestar a ordem relevante, inclusive empregando contestações legais perante às autoridades judiciais;
- coordenar respostas com os pares, a fim de aumentar influência.

Mitigação e comunicação

- identificar os indivíduos potencialmente afetados e comunicar-lhes o fato do desligamento, a sua projeção de duração e alcance, e proporcionar-lhes os caminhos para a obtenção de informações adicionais;
- manter o controle da infraestrutura do provedor durante todo o processo;
- disputar e limitar o desligamento (geograficamente e temporalmente), na medida do possível;
- restaurar o acesso assim que possível.

Os termos de serviços devem indicar claramente as condições sob as quais o acesso dos indivíduos à Internet será retirado como resultado de um desligamento da rede imposta pelo Estado. Em particular, em seus termos de serviços provedores devem comprometer-se:

- não dar efeito a desligamentos de rede a menos que todas as vias internas para contestar o desligamento foram esgotadas;
- notificar os indivíduos imediatamente de um próximo desligamento e regularmente fornecendo-lhes informações atualizadas sobre o desligamento;
- fornecer aos indivíduos mecanismos de queixa e solução para remediar eventuais impactos negativos do desligamento que a telco está em uma posição para resolver.

Recomendações sobre leis de respostas graduais

Termos de serviços dos provedores devem indicar aos indivíduos se uma lei resposta graduais aplica-se no seu país de operação e deve indicar claramente as condições em que será retirado o acesso dos indivíduos de acordo com tais leis.

Em seus termos de provedores de serviços devem comprometer-se a:

- nunca desconectar um indivíduo da Internet como uma medida voluntária ou punitiva;
- apenas desconectar um indivíduo da Internet se uma ordem de desconexão é emitida por uma autoridade judicial independente;
- notificar um indivíduo imediatamente se uma ordem de desconexão é recebida;
- contestar a ordem de desconexão em nome do indivíduo até que todas as vias internas forem esgotadas.

Recomendações sobre neutralidade de rede

Provedores devem abster-se de aplicar voluntariamente medidas que violam o princípio da neutralidade de rede. Onde eles estão sob a obrigação legal de restringir o acesso a serviços ou aplicações específicos, devem fazê-lo de uma forma que garanta a sua conformidade com os princípios internacionais de direitos humanos, na medida do possível. A esse respeito, os termos de serviço dos provedores devem comprometer-se a:

- não discriminar ou priorizar o conteúdo com base na origem, destino ou fornecedor de serviços ou tipo de aplicação ou serviço;
- não restringir de qualquer forma os conteúdos, aplicações ou serviços que um usuário pode acessar, exceto para fins de gerenciamento de rede - e restringir essa priorização ao que é estritamente necessário;
- não condicionar a prestação de serviços gratuitos a acesso restrito a conteúdos, aplicações ou serviços;
- só restringir o acesso a conteúdos, aplicações ou serviços se uma ordem é

emitida por uma autoridade judicial independente;

- notificar os usuários imediatamente se tal ordem é recebida;
- contestar essas ordens até que todos as vias internas sejam esgotadas;
- publicar regularmente detalhes de quaisquer ordens que a telco esteja sujeita, de acordo com as quais o acesso a determinados conteúdos, aplicações ou serviços esteja restrito;
- publicar regularmente informações sobre as práticas de gerenciamento de rede;
- submeter-se a monitoramento externo independente das medidas de gerenciamento de tráfego e explicar aos usuários como eles podem participar desses processos;
- Abster-se de recorrer a medidas de gerenciamento de tráfego que invadem a privacidade (como inspeção profunda de pacotes).

Provedores poderiam, no entanto, considerar alternativas "positivas" a taxa zero (zero rating), como incentivar provedores de serviços terceiros a oferecer versões de seus serviços com o uso mais eficiente de dados para todos os usuários de Internet (por exemplo, usando uma melhor compressão, menor taxa de bits de áudio e/ou menor resolução de vídeo).

Recomendações sobre proteção de dados

Provedores devem usar seus termos de serviços para comunicar claramente e explicitamente com indivíduos com relação aos dados pessoais requeridos, gerados, coletados e armazenados sobre eles. Eles devem comprometer-se a:

obter sempre o consentimento informado do indivíduo ao usar seus dados pessoais para uma finalidade nova ou incompatível;

exigir que os indivíduos revelem o montante mínimo de dados pessoais necessários para o fornecimento de acesso a telecomunicações;

- informar as pessoas sobre como seus dados pessoais são usados, o tempo

que é mantido e com quem é compartilhado;

- exclusão de dados pessoais identificáveis tão logo que eles não sejam mais necessários para fornecer acesso ao indivíduo;

- permitir que os indivíduos acessem e examinem, a qualquer tempo, os dados pessoais mantidos pela telco e os fins que estão sendo colocados;

- permitir que os indivíduos retirarem seu consentimento a qualquer momento para o processamento de seus dados pessoais;

- garantir que os dados pessoais estejam protegidos por medidas organizacionais e técnicas de segurança;

- notificar os indivíduos imediatamente se ordens obrigatórias de retenção de dados são recebidas;

- notificar os indivíduos imediatamente se pedidos de acesso a dados de assinantes ou dados de comunicações ou conteúdos são recebidos;

- contestar tais ordens em nome do indivíduo até que todas as vias internas foram esgotadas;

- notificar os indivíduos se seus dados pessoais foram divulgados a uma autoridade governamental ou terceiros;

- publicar regularmente os detalhes de todos os pedidos que a telco esteja sujeita, de acordo com a qual os dados são gerados, retido ou divulgados;

- publicar regularmente informações sobre dados pessoais, de comunicação e de conteúdo que estão sendo divulgados às autoridades governamentais ou terceiros;

- fornecer aos indivíduos um mecanismo de reclamação ou remediação para contestar a divulgação de dados pessoais, em violação dos termos de serviço.

Recomendações sobre vigilância

Embora alguns pedidos ou demandas de assistência dos provedores para a vigilância do Estado possam ser justificados, provedores são mais capazes de garantir que eles assumam as suas responsabilidades por proteger e promover os direitos humanos, se eles resistem a quaisquer pedidos ou ordens que visam tomar o controle da infraestrutura de telecomunicações, afastando-a do provedor e colocando-a nas mãos do governo. Aquiescência a esses pedidos cria um precedente perigoso, induzindo uma expectativa por parte do Estado de que a telco continuará a modificar os seus produtos e serviços de acordo com as preferências do Estado. Excessividades devem ser evitadas em todas as circunstâncias.

Os provedores devem também avançar em medidas inovadoras para melhorar a liberdade de expressão e o direito à privacidade dos indivíduos, mesmo se tais medidas frustrem ou impedem os objetivos de vigilância do Estado. Isso inclui, principalmente, a aplicação de criptografia avançada para redes de telecomunicações.

Os provedores devem comunicar aos seus usuários em seus termos de serviço como eles vão responder às solicitações e exigências do Estado para facilitar a vigilância. Esta informação deve ser completa e franca e não se esconder atrás de referências genéricas ao cumprimento das leis locais. Os provedores devem comprometer-se a:

- robustamente examinar qualquer pedido ou demanda dos Estados para adaptar ou modificar infraestrutura de telecomunicações existente ou instalar capacidades de vigilância;

- esgotar todos os recursos disponíveis para contestar qualquer pedido ou demanda de retroalimentar ou de modificar a infraestrutura ou de instalar as capacidades de vigilância;

- resistir ativamente - inclusive usando a pressão pública, ação coletiva e ameaças de retirada do mercado - a qualquer pedido ou a demanda pelos Estados para acesso direto a redes de telecomunicações;

- publicação de informações, na maior medida possível, sobre quaisquer medidas tomadas para adaptar ou modificar a infraestrutura ou instalar vigilância ou fornecer acesso direto;

- sempre que possível, notificar os usuários individuais de medidas específicas de vigilância a que estiveram sujeitos;

- providenciar um mecanismo de reclamações ou de mediação para permitir aos indivíduos a contestar a decisão dos provedores de cumprir com pedidos ou exigências.

Recomendações sobre reparações

Telcos e ISPs devem assegurar que existem mecanismos de reclamação e de reparação locais para tratar dos impactos negativos de suas ações que o provedor esteja em posição para remediar.

Práticas de transparência robustas podem ser uma das medidas corretivas73, fornecendo aos usuários afetados o direito de ser ouvido sobre o impacto da infração para suas vidas. Além disso, a prestação de informação aos usuários afetados sobre a natureza, o alcance e a origem das violações dos direitos humanos podem empoderá-los. No contexto de desligamentos de rede, por exemplo, informar os usuários com atualizações regulares e contínuas irá colocá-los em uma posição mais forte para mitigar os efeitos negativos do desligamento.

No caso de demandas graves e sistemáticas estatais destinadas a facilitar abusos de direitos humanos, telcos e ISPs devem considerar se a conformidade com as normas internacionais de direitos humanos poderia ser melhor alcançada através da cessação das operações de negócios em um país ou contexto particular.

A retirada de operações é uma reparação que pode enfraquecer os direitos humanos dos usuários de Internet: pode privar os usuários de conectividade temporariamente ou permanentemente, aumentar os custos de conectividade e facilitar o crescimento dos mercados monopolistas. No entanto, quando as empresas de telecomunicações são repetidamente colocadas sob pressão do governo para facilitar graves violações dos direitos humanos, em especial de vigilância e desligamentos de rede, o dano causado aos usuários através de tais infrações, sem dúvida, supera o mal da retirada.

Em tais circunstâncias, as empresas de telecomunicações devem realizar uma avaliação abrangente - em consulta com as partes interessadas - da necessidade, efeitos e impacto potencial sobre usuários de cessar atividades empresariais no país em questão. A decisão de cessar as suas operações de negócios deve ser tomada como um último recurso e somente após consulta com outras entidades do setor sobre a possibilidade de impulsionar uma ação coletiva contra o governo.

Além disso, empresas de telecomunicações e ISPs devem considerar as seguintes ações corretivas específicas:

Para desligamentos de rede

- fornecer informações completas, por todos os meios eficazes, sobre a existência e a extensão do desligamento, e, se possível, sobre a existência de soluções de acesso alternativo (e das implicações da utilização de tal solução);

- imediatamente restaurar a conectividade de rede na primeira oportunidade disponível;

- convidar e gravar as contas de usuários, permitindo que aqueles cuja conectividade foi restrita possam explicar e documentar as suas experiências de desligamento;

- considerar estender o crédito em conta ou promoções como forma de compensação universal ou alterando a data de pagamento das contas;

- tomar medidas para compensar indivíduos que sofreram perdas financeiras demonstráveis ou danos substanciais como resultado do desligamento;

- convocar imediatamente uma discussão setorial para contemplar como impulsionar ação coletiva contra novoos desligamentos impostos pelo governo.

Para leis de respostas graduais

- imediatamente restaurar a conectividade do indivíduo afetado na primeira oportunidade possível, seja depois de contestar com sucesso a ordem de desconexão ou após o término do período de desconexão;

- tomar medidas para compensar indivíduos que sofreram perdas financeiras demonstráveis ou danos substanciais como resultado da desconexão.

Para a neutralidade de rede

- desculpar-se aos usuários e fornecer informação completa e abrangente sobre as medidas tomadas pela telco para priorizar, discriminar ou restringir o conteúdo particular;

- fornecer garantias para os usuários que o seu futuro acesso à rede não será objeto de priorização, discriminação ou restrição;

- adotar medidas de transparência daqui para frente para permitir uma supervisão independente das medidas de gerenciamento de rede;

- apoiar indivíduos em ações legais para buscar reparação ou compensação por parte do Estado.

Por quebra de proteção de dados

- fornecer aos usuários afetados informação completa e abrangente sobre os dados pessoais gerados, retidos e divulgados sobre eles;

- fornecer garantias de que os dados pessoais foram apagados e que quaisquer terceiros a quem os dados pessoais foram divulgados foram convidados a apagar os dados;

- tomar medidas para compensar indivíduos que sofreram perdas financeiras demonstráveis ou danos substanciais como resultado da geração, retenção e divulgação de dados pessoais.

Para a vigilância

- notificar o usuário afetado e fornecer informações completas e abrangentes sobre o tipo e o escopo da vigilância a que ele foi submetido;

- convidar e gravar as contas de usuários afetados, permitindo-lhes explicar e documentar as suas experiências em matéria de vigilância;

- tomar medidas para compensar indivíduos que sofreram perdas financeiras demonstráveis ou danos substanciais como resultado da vigilância;

- apoiar indivíduos para fazer ação legal para buscar reparação ou compensação por parte do Estado, inclusive por contestar a legalidade de vigilância sempre que necessário.

Sobre a ARTIGO 19

A ARTIGO 19 é uma organização internacional de direitos humanos, fundada em 1987, que defende e promove a liberdade de expressão e direito à informação em todo o mundo.

Seu mandato provém da Declaração Universal dos Direitos Humanos, que garante o direito à liberdade de expressão e informação. Um meio cada vez mais importante de expressão e de procurar, receber e difundir informações é através de tecnologias de informação e comunicação, como a Internet. A ARTIGO 19 tem promovido as liberdades da Internet há mais de 10 anos e é ativa no desenvolvimento de políticas e práticas relativas à liberdade de expressão e à Internet através de nossa rede de parceiros, associados e contatos de especialistas.

ARTIGO 19 encoraja as organizações e indivíduos para nos dar retorno sobre como estas diretrizes políticas estão sendo usadas. Por favor, envie sua opinião para comunicacao@artigo19.org

Esta publicação é total ou parcialmente financiado pelo Governo da Suécia. O Governo da Suécia não compartilha necessariamente as opiniões aqui expressas. A ARTIGO 19 assume a responsabilidade por seu conteúdo.

Referências

1. A importância de telefones celulares vai muito além da comunicação interpessoal; por exemplo, no Sul Global, a telefonia móvel tem desempenhado um papel importante na promoção da responsabilidade democrática, proporcionando acesso à informação, e propagando campanhas nacionais eficazes; ver, por exemplo, artigo 19, Quênia: padrões de livre expressão devem orientar luta contra a "falsificação" telefones celulares,11 de outubro de 2011.
2. Ver, por exemplo, Conselho de Direitos Humanos, Resolução promoção, proteção e gozo dos direitos humanos na Internet,/ HRC/32/L.20, adotada em 27 de Junho de 2016.
3. Ver, por exemplo, Persbericht WRR, Policy Brief No. 2: Núcleo público da internet: uma agenda internacional para a governança da Internet,10 de abril de 2015; ou Jacob Kastrenakes, Obama diz FCC deve reclassificar Internet como um utilitário, The Verge, 10 de novembro de 2014.
4. Ver ARTIGO 19, Liberdade de expressão e do setor privado na era digital: Apresentação ao Relator Especial das Nações Unidas,2016.
5. 5 C. Cath, N. ten Oever & D O'Maley, Desenvolvimento de mídia na Era digital: Cinco maneiras de se envolver em Governança da Internet,de Março de 2016.
6. Estes incluem, em particular, as seguinte diretrizes políticas da ARTIGO 19:

- Intermediários Internet: Dilema de Responsabilidade (Agosto de 2013) que incide sobre os modelos de responsabilidade aplicável aos atores que operam na camada de conteúdo (tais como provedores de hospedagem) e a camada social, (tais como plataformas on-line) da Internet;
- Liberdade de Expressão Sem Filtros: Como bloqueio e filtragem afetam a liberdade de expressão (Dezembro de 2016), que examina a compatibilidade de bloqueio e filtragem de conteúdo on-line com as normas internacionais e fornece recomendações para governos e empresas;
- Direito ao esquecimento (Março de 2016), que fornece recomendações abrangentes sobre como garantir a proteção do direito à liberdade de expressão no que diz respeito ao chamado "direito ao esquecimento";
- Os Princípios Globais para a Liberdade de Expressão e Privacidade (Março de 2017) que fornecem uma marco analítico sistemático para avaliar como a liberdade de expressão e privacidade se reforçam mutuamente, e determinar os limites que podem ser colocados em ambos os direitos quando eles estão em conflito, on-line e off;

- Policy Brief: Responsabilidade Corporativa da ICANN para respeitar os direitos humanos (2015 de outubro), que expõe as razões que os princípios orientadores da ONU sobre Empresas e Direitos Humanos (UNGPs) são o marco mais apropriado para ICANN a seguir em sua missão de desenvolver políticas e processos de direitos humanos, e, em seguida, apresenta as opções de como ICANN pode começar a implementá-las.

7. Por exemplo, a British Telecom, a mais antiga empresa de telecomunicações do mundo, foi inicialmente transferida para o controle do Estado sob o Post Office e mais tarde tornou-se uma empresa privatizada, o precursor do BT Group Plc; ver, por exemplo, BT, Origens da BT. No Brasil, o Código de 1963 Telecomunicações estabeleceu um monopólio concedido pelo Estado, seguida da criação da Embratel em 1965 e a organização posterior do sistema Telebrás em 1972 com uma série de telecomunicações regionais, a Embratel (responsável por chamadas interestaduais e internacionais) e CPqD (uma unidade de I & D); veja A.Musacchio & SGLazzarin, empresas públicas no Brasil: histórico elições,OCDE, 2014.

8. Por exemplo, nos EUA; veja RW Sorte & J. Eisenberg, A Evolução da Indústria e Efeitos sobre a EUA Telecomunicações,NPA, 2016.

9. Ver, por exemplo, artigo 19, Brasil: ARTIGO 19 lança guia sobre provedores de internet comunitários ,19 de Janeiro de 2017.

10. Convenção Europeia sobre Direitos Humanos (artigo 10), a Carta da União Europeia dos Direitos Fundamentais (artigo 11), a Convenção americana sobre Direitos Humanos (artigo 13), a Carta Africano dos Direitos Humanos e dos Povos (artigo 9.º) e a Declaração de Direitos Humanos da ASEAN (artigo 23).

11. Ver, por exemplo, o Comitê de Direitos Humanos da ONU, Comentário Geral nº34,aprovada em Julho de 2011.

12. Declaração Conjunta sobre a Liberdade de Expressão e a Internet, relator especial da ONU sobre a Liberdade de Opinião e Expressão (Relatora Especial sobre FOE), a Organização para a Segurança e Cooperação na Europa (OSCE) Representante para a Liberdade dos Meios de Comunicação, a Organização dos

Estados Americanos (OEA) Relator especial sobre a Liberdade de Expressão e a Comissão Africana dos Direitos Humanos e dos Povos (CADHP) Relator especial para a Liberdade de Expressão e Acesso à Informação, 01 de junho de 2011; Resolução Internet HRC, op.cit.

13. Ver, por exemplo Comitê da ONU Administrativo de Coordenação, Declaração da Comissão Administrativa de Coordenação sobre o acesso universal aos serviços de comunicação e informação básicos, ACC / 1997/4, 25 Junho de 1997; Assembléia Geral da ONU,a Declaração Millennium UN, aprovada pela GA, 18 de setembro de 2000, A / RES /55/2; ONU eITU, a Declaração de Princípios: um desafio global para o novo milénio, Cúpula Mundial sobre a Sociedade da Informação,WSIS-03 / GENEBRA / DOC /4-E,12 de dezembro de 2003; de maio de 2011 Relatório do Relator Especial sobre FOE: comunicações de e para governos,op.cit., Para 60; GA da ONU, Relatório do Relator Especial sobre FOE, 10 de agosto de 2011, A / A / 66/290, parágrafos 61 e 63; OCDE, Recomendação do Conselho da OCDE sobre os Princípios para a Formulação de Políticas Internet,13 de dezembro de 2011, Princípio 2; HRC resolução Internet, op.cit.,ONU GA, Transformando o nosso mundo: 2030 Agenda para o Desenvolvimento Sustentável, 21 de outubro de 2015, A / RES / 70/1, meta 9.c; a página de Fórum de Governança da Internet;Direitos de Internet e princípios dinâmicos da coalizão, Fórum de Governança da Internet da ONU, Carta dos direitos humanos e princípios para a internet de agosto de 2014,4ª edição; ou Conselho da Europa, Comité de Ministros, Recomendação No.R (99) 14 sobre serviço comunitário universal relativo aos novos serviços de comunicação e informação,9 de Setembro de 1999. Em nível nacional, países europeus têm reconhecido o direito de acesso e à Internet em seus marcos jurídicos, quer através de constituições, leis ou decisões judiciais; ver, por exemplo, República da Estónia, Lei da Informação Pública, 15.11.2000, artigo 33 e da Constituição da República da Estónia, 29 de junho de 1992, artigo 44; A Constituição da Grécia, tal como revisto pela resolução parlamentar de 06 de abril de 2001, artigo 5A.2, República da Finlândia, Comunicações Ato para o Mercado, 393/2003, 363/2011 alterações, Seção 60c (2); Reino de Espanha, a Lei de Economia Sustentável, 2/2011, 4 de março de 2011, artigo 52.

14. O 2011 Relatório do Relator Especial sobre FOE à Assembleia Geral da ONU, op.cit., Parágrafo 87.

15. Este teste foi atualizado em numerosos instrumentos

internacionais de direitos humanos, mais notavelmente no Comentário Geral do Comitê de Direitos Humanos No. 34.

16. 2011 Declaração Conjunta, op.cit.
17. HRC resolução Internet, op.cit.
18. Comentário Geral No. 34, op.cit. para 43.
19. Ver a Convenção Europeia dos Direitos do Homem (artigo 8), a Carta dos Direitos Fundamentais (artigo 7) e na Convenção Americana sobre Direitos Humanos (artigo 11).
20. A Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal,28 de Janeiro de 1981..
21. Diretrizes Assembléia Geral da ONU para o tratamento informatizado dos dados pessoais, tal como adotadas pela Resolução da Assembleia Geral 45/95 de 14 de dezembro de 1990 .
22. G. Greenleaf, Leis de Privacidade de dados Asiático (Oxford, Oxford University Press: 2014), 55. Para obter detalhes sobre cada uma das estruturas internas, consulte Baker Hostetler, 2015 Internacional compêndio de dados leis de privacidade.
23. Ver, por exemplo: Tribunal Europeu (TEDH) decisões em Leander v Suécia, App..No. 9248/81, 26 de Março de 1987; S. e Marper v. Reino Unido,App. Nos 30562/04 e 30566/04, 4 de Dezembro de 2008.; . Malone v Reino Unido,No. 8691/79, 2 de agosto de 1984; . Copland v Reino Unido, nº 62617/00, 3 de abril de 2007; Klass e Outros contra a 1978.;Alemanha,No. 5029/71, 06 de setembro de TEDH, .Uzun vAlemanha,n ° 35623/05, 2 de Setembro de 2010; ou as decisões do Tribunal de Justiça da União Europeia (TJUE) no C-293/12 e C-594-12, Digital Rights Ireland contra Irlanda,2014/08/04; ou C-362/14, v Schrems dados Proteção Comissário,2015/10/06.
24. Em 2012, a ASEAN adotaram uma Declaração dos Direitos Humanos, que faz referência especificamente à proteção de dados pessoais, e em 2014 a União Africano aprovou uma convenção sobre Cyber Security e Proteção de Dados Pessoais.
25. Em suas observações finais de sua revisão de 2014 a conformidade dos EUA com as suas obrigações nos termos do artigo 17 do PIDCP, o Comitê observou que as interferências com o direito à privacidade devem estar de acordo "com os princípios da legalidade, necessidade e proporcionalidade;" CCPR / C / EUA / CO / 4, parágrafo 22. Este sentimento ecoado do relator especial sobre FOE em seu relatório 2013 sobre a privacidade e comunicações de vigilância, que afirmou que "[o] marco do artigo 17 do PIDCP permite restrições necessárias, legítimas e proporcionais ao direito à privacidade por meio

de limitações admissíveis", o teste do que deve ser entendida a ser nos mesmos termos que a aplicável nos termos do artigo 19, parágrafo 3, apesar do artigo 17 que não contenham tal linguagem explícita. O Alto Comissariado da ONU para os Direitos Humanos, em seu relatório de 2014, o direito à privacidade na era confirmou a interpretação do relator especial, afirmando: "[...] fontes oficiais apontam para os princípios fundamentais da legalidade, necessidade e proporcionalidade. ..;"a / BQ / 27/37, para 23.

26. refletido nas orientações da OCDE 1980 relativa à proteção da privacidade e fluxos transfronteiriços de dados pessoais; Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados Pessoais (conhecida como Convenção 108); e as Diretrizes da ONU para a regulamentação dos arquivos informatizados de dados pessoais.
27. Estes princípios são tomadas a partir do artigo 5 do Regulamento Geral de Proteção de Dados, mas eles refletem amplamente Princípios da Comissão Federal de Comércio dos os EUA, os princípios consagrados na OCDE e Diretrizes da ONU, a Convenção 108 e da Diretiva Proteção de Dados, que informaram regulamentos de proteção de dados em mais de cem países ao redor do mundo.
28. Estes incluem o Comentário Geral No. 34, op.cit., HRC resolução Internet op.cit.;de 2011 Declaração Conjunta op.cit.; Relatórios do Relator Especial sobre a liberdade de expressão na Internet (A / 66/290, 2011), de vigilância e o direito à privacidade (A / HRC / 23/40, de 2013), o acesso à informação (A / 68/335, 2014), e a proteção das fontes e dos informadores (a / 70/361, 2015); decisões do TEDH em Delfi AS v. Estónia [GC], aplicativo. No. 64569/09, 16 de junho de 2015; Conselho Editorial da Pravoye Delo & Shtekel v.Ucrânia,App. No. 33014/05, 5 de maio de 2011; Niskasaari & Otavamedia Oy v.Finlândia,App. No. 32297/10, parágrafos 9 e 54-59, 23 de junho de 2015; Mosley v. Reino Unido,App. No. 48009/08, § 129, 10 de maio de 2011; Animal v Defenders International. Reino Unido [GC] App. No. 48876/08, § 119, ou Ahmet Yıldırım v.Turquia,App. No. 3111/10, § 67, CEDH 2012.
29. Relatório do Relator Especial sobre FOE e o setor de acesso à Internet e telecomunicações, A / HRC / 35/22, 30 de março de 2017. Maio do Relator Especial 2016 relatório à Assembléia Geral (A / BQ / 32/28) também é instrutivo.
30. op.cit.
31. Pacto Global ds Nações Unidas é uma da ONU iniciativa para incentivar as empresas em todo o mundo a adotar políticas sustentáveis e socialmente responsáveis e a informar sobre a sua execução,
32. Os Princípios Orientadores foram lançados em 2008 sob a liderança do Representante Especial da ONU John Ruggie. Eles construído sobre o trabalho do Pacto Global

da ONU, lançada em 2000 para incentivar as empresas a desenvolver práticas empresariais responsáveis.

33. Telecomunicações Diálogo Princípios Orientadores,12 de Março de 2013.
34. Global Network Initiative, princípios globais sobre liberdade de expressão e privacidade,desenvolvidos por empresas, investidores, organizações da sociedade civil e acadêmicos.
35. Ranking de Direitos Digitais, Índice de Responsabilidade Corporativa
36. Graduação de Direitos Digitais, 2015 Índice Corporate Accountability.
37. CDT, Internet estrangulamento do Irã: Inaceitável Agora ,3 de julho de 2013; Software Freedom Law Center Índia, Shutdowns Internet na Índia,de 2016; Acesso Agora, Gâmbia desliga Internet na véspera daseleições, 30 de Novembro de 2016.
38. Ver a CDT, a Rede Shutdowns Timeline,11 de Setembro de 2014.
39. Por exemplo, na Índia, Argélia, Etiópia, Iraque e Azerbaijão; veja Relator Especial sobre FOE 2017 Relatório, op.cit.
40. D. O'Brien, Crackdown Internet da Venezuela transforma em Blackout Regional, FEP, 20 Fevereiro de 2014
41. Ver, por exemplo, as observações preliminares do Relator Especial sobre FOE no final da sua visita a Tajikistan, 9 de março de 2015;
42. Comentário Geral No. 34, op.cit.,Pará 43.
43. Existem tais leis na Coreia do Sul, Nova Zelândia, França e Reino Unido; outros países, como a Austrália, consideraram e abandonaram essa abordagem.
44. A Lei Hadopi francesa, adotada em 2009, permitiu a suspensão do acesso à Internet até que as disposições pertinentes foram consideradas ilegais em 2013. Houve um programa também voluntário "seis avisos" nos EUA (assim chamada do Sistema de Alerta de Copyright) que funcionava com o mesmo efeito; o programa foi aposentado em janeiro de 2017.
45. Relator Especial das Nações Unidas sobre FOE, Relatório para a HRC, junho de 2011 (A / HRC / 17/27), parágrafo 78.
46. A. Futter & A. Gillwald, taxa zero serviços de Internet: O que é para ser feito?, Research ICT Africa.
47. J. Malcolm, C. McSherry & K.Walsh, Zero Avaliação: O que é e qual sua importância,18 de fevereiro de 2016
48. eradores de telecomunicações em conexões 3G e 4G em janeiro de 2016 e conexões ADSL em fevereiro de 2016. Na China, os serviços VoIP que não são oferecidos por empresas de telecomunicações estatais são proibidos.
49. No Brasil, Whatsapp foi temporariamente bloqueado em 2016; ver artigo 19, Brasil: serviços WhatsApp bloqueados em todo o país em violação da liberdade de expressão,22 de julho de 2016.
50. Em 2016, o presidente dos Emirados Árabes emitiu uma série de leis federais especiais relacionadas aos crimes de Internet, incluindo um regulamento que proíbe qualquer pessoa nos Emirados Árabes Unidos de fazer uso de redes privadas virtuais (VPN).
51. Agnosticismo de conteúdo refere-se a noção de que o tráfego de rede é tratado de forma idêntica, independentemente da carga útil, com alguma exceção em que se trata de manuseamento eficaz do tráfego, por exemplo, quando se trata de atrasar pacotes sensíveis, com base no cabeçalho. Agnosticismo de conteúdo

impede discriminação baseada em carga útil contra pacotes; see N. ten Oever, Human Rights Protocol Considerations Research Group, Research into Human Rights Protocol Considerations draft-irtf-hrpc-research-11.

52. Veja, por exemplo, ARTIGO 19, Nosso futuro 5G: Luz no final do túnel ou Internet fast-lane para a elite ?, 15 de setembro de 2016.
53. 5 Manifesto para implantação oportuna de 5G na Europa, 7 de julho de 2016.
54. Veja, por exemplo, The Register, o manifesto 5G dos operadores da UE perde o ponto, 13 de julho de 2016;
55. Como o Chile, Noruega, Holanda, Finlândia, Islândia, Estônia, Letônia, Lituânia, Malta e Japão.
56. Veja, por exemplo, FCC, Proteção e Promoção da Internet Aberta, FCC 15-24, 12 de março de 2015.
57. Ver Comissão Europeia, Nosso Compromisso com a Neutralidade da Rede, outubro de 2015.
58. Em 2016, o Reino Unido promulgou a Lei dos Poderes de Investigação, que exige que os provedores de telecomunicações gerem e retenham os "registros de conexão com a Internet" por até 12 meses.
59. A Austrália é o país que adotou tal lei. Em 2014, a Diretiva Europeia de Retenção de Dados foi invalidada, revogando as leis de retenção de dados em toda a Europa, embora tenham sido promulgados regimes de retenção de dados subsequentes. Nos EUA, a retenção de dados é obrigatória pelo USA Freedom Act desde 2015. Antes disso, a Seção 215 da Lei Patriot impôs requisitos similares.
60. Corte Interamericana de Direitos Humanos, Escher et. Al. V. Brasil, 6 de julho de 2009, parágrafo 114.
61. Ver, CJEU, Watson e outros contra UK 698/15 (processos apensos C-203/15, C-698/15), 21 de dezembro de 2016, parágrafos 99-101.
62. Alto Comissário das Nações Unidas para os Direitos Humanos Navi Pilla, O direito à privacidade na era digital, parágrafo 27.
63. CJEU, Watson e outros contra UK, op.cit., Parágrafos 105-106.
64. ECtHR, Zakarov v Russia, App. No. 47143/06, 4 de dezembro de 2015, parágrafo [229].
65. ECtH, Weber e Saravia v Alemanha, App. No. 54934/00, parágrafo. [95]
66. Veja, por exemplo, as Observações finais do Comitê de RH para os EUA (CCPR / C / USA / CO / 4), 2014, parágrafo 22.
67. TEDH, Zakarov contra Rússia, op.cit. Para [260].
68. Acesse agora, pilar esquecido: o plano de remédio da Telco, maio de 2013.
69. Recomendação CM / Rec (2014) 6 do Comitê de Ministros aos Estados membros sobre um Guia de Direitos Humanos para usuários de Internet, Conselho da Europa.
70. Guia do Setor de TIC da Comissão Europeia sobre Implementação dos Princípios Orientadores das Nações Unidas sobre Negócios e Direitos Humanos, 2013.
71. Os Princípios Orientadores, op.cit., Princípio 23 - Questões de Contexto
72. Grande parte desta orientação é tirada do Guia do Setor das TIC da Comissão Europeia sobre a Implementação dos Princípios Orientadores das Nações Unidas sobre Negócios e Direitos Humanos, p. 53.
73. Cf. O relatório de 2017 do Relator Especial sobre FOE, op.cit.

ARTIGO 19 Rua João Adolfo, 118, 8o andar São Paulo- SP Brasil
T: +55 11 30570071

E: comunicacao@artigo19.org W: www.artigo19.org Tw: @artigo19 Fb: facebook.com/artigo19brasil

© ARTICLE 19