PROTECT THE STACK

Infrastructure Providers Should Not Be Content Police

Proteja a stack: fornecedores de infraestrutura não devem policiar conteúdo

Os prestadores de serviços de infraestruturas da internet estão sob pressão para desempenhar um papel mais importante no policiamento dos conteúdos e na participação online. Alguns estão decidindo intervir sozinhos. Esta é uma tendência perigosa que deve terminar agora.

Os pedidos para que toda a "stack" lute para acabar com o discurso prejudicial é compreensível em alguns casos, porém, isso causará várias consequências não intencionais, particularmente para os usuários menos poderosos. Sujeito a raras exceções, os governos não devem exigir tais intervenções e as empresas de infraestrutura não devem intervir voluntariamente.

Histórico

Os usuários e formuladores de políticas estão familiarizados com plataformas como Facebook, Twitter ou YouTube. Mas esses serviços não são a internet. Na verdade, a comunicação e o comércio online também dependem de um amplo leque de prestadores de serviços, incluindo ISPs e empresas de telecomunicações, como Comcast, Orange, MTN, Airtel, Movistar ou Vodafone; registradores de nomes de domínio, como Namecheap ou GoDaddy; serviços de suporte, como Amazon Web Services (AWS), autoridades de certificação (como Let's Encrypt), processadores de pagamento, como PayPal e M-PESA, email, serviços de mensagens e muito mais. Vistos em conjunto, às vezes, esses provedores são chamados de "stack de tecnologia".

A maioria dos usuários usa a internet sem pensar em todos os serviços de infraestrutura subjacentes. Mas esses serviços são essenciais para a expressão, privacidade e segurança online. E quando esses provedores – muitos dos quais têm pouco ou nenhum contato com os usuários – intervêm com base no conteúdo, suas escolhas podem ter enormes impactos nos direitos humanos que podem ser difíceis ou impossíveis de sanar.

As armadilhas e riscos específicos para a expressão e privacidade podem variar dependendo da natureza do serviço. Mas para cada provedor de infraestrutura, alguma combinação das seguintes preocupações será aplicada. Vistos em conjunto, eles

demonstram poderosamente por que, com raras exceções, os provedores de infraestrutura devem ficar fora do policiamento de conteúdo.

Uma observação sobre “stack”

Stack é um termo emprestado da ciência da computação e engenharia de software, usado para descrever uma combinação de ferramentas, processos, linguagens de programação e mecanismos usados em combinação para construir um aplicativo ou produto. Neste contexto, usamos para descrever a internet como a conhecemos, os provedores de serviços, plataformas, processos e vários outros atores que possibilitam a web moderna.

A stack de tecnologia inclui plataformas de conteúdo geradas pelo usuário, como Facebook e Twitter, bem como os provedores de infraestrutura mencionados acima. As plataformas de mídia social ficam no topo da stack, enquanto os principais provedores de infraestrutura, como seu ISP, ficam na parte inferior, com uma ampla variedade de intermediários, como processadores de pagamento e registradores, entre outros, entre eles.

Os riscos para os direitos humanos

1. A maioria dos serviços de infraestrutura não pode adaptar suas práticas de intervenção para que sejam necessárias e proporcionais.

Em geral, as plataformas têm várias opções de moderação. Em contraste, muitos serviços de infraestrutura não podem direcionar sua resposta com a precisão que os padrões de direitos humanos exigem. O Twitter bloqueia tweets específicos; o Amazon Web Services nega atendimento a um site ou conta inteira, o que significa que suas intervenções, inevitavelmente, afetam muito mais do que o discurso censurável que motivou a ação. O sequestro governamental de serviços de telecomunicações para interromper a internet para um país inteiro é particularmente terrível.

Ações terríveis também ocorrem no nível do domínio, onde os registradores que se opõem ao discurso em um site não visam apenas o discurso, mas suspendem e/ou cancelam o registro de todo o site. Por exemplo, o ARTIGO 19 documentou vários exemplos de “abuso de DNS”: a suspensão e o cancelamento do registro de nomes de domínio como meio de sufocar a dissidência.

Podemos tirar uma lição aqui do contexto de direitos autorais, onde também vimos registradores de nomes de domínio e provedores de hospedagem encerrarem sites inteiros em resposta a avisos de violação direcionados a um único documento. Pode ser possível que alguns serviços se comuniquem diretamente com os clientes quando estiverem preocupados com um conteúdo específico e solicitem que ele seja retirado. Mas se esse pedido for rejeitado, o serviço tem apenas o instrumento contundente de remoção completa à sua disposição. E alguns serviços podem não ter uma maneira viável de se comunicar diretamente com a fonte do conteúdo.

2. Aviso e recurso significativos raramente são possíveis, especialmente para os menos poderosos.

As normas de direitos humanos e os princípios de devido processo legal exigem que os prestadores de serviços notifiquem os usuários de que seu discurso e/ou conta foi – ou será – retirado e ofereça aos usuários a oportunidade requerer compensação. Em nível da infraestrutura, tal notificação e oportunidades de compensação podem ser impossíveis. Com frequência, os serviços não podem se comunicar diretamente com os usuários da internet, uma vez que, no geral, os serviços não têm uma relação direta com o comentarista ou o público para a expressão em questão. E, ao contrário de hospedeiros de conteúdo em nível de plataforma, que podem deixar um aviso explicativo no local original de uma postagem removida (em uma prática às vezes chamada de "túmulo"), os provedores de infraestrutura normalmente não têm a capacidade prática de notificar os futuros usuários sobre as maneiras pelas quais o provedor impediu o acesso ao conteúdo.

Assim, por exemplo, se um usuário descobre que um link enviado por um amigo não funciona, para ele não é fácil saber se houve um problema com o link, se o proprietário retirou o site voluntariamente ou se ele foi bloqueado. Os usuários de um serviço que depende de um processador de pagamento também podem se assustar ao descobrir que o serviço desapareceu porque, sem o conhecimento deles, o processador desligou o pagamento para esse serviço. Na Argentina, por exemplo, a Uber foi interrompida durante a noite graças a uma ordem judicial exigindo que um processador de pagamentos bloqueasse os pagamentos ao serviço.

Os usuários essencialmente estão obrigados pelos termos e condições de cada serviço na cadeia, do comentarista ao público, mesmo que possam não saber o que são esses serviços ou como contatá-los. Dadas as consequências potenciais das violações e a dificuldade de navegar nos processos de recursos de serviços anteriormente invisíveis (supondo que tal processo exista), muitos usuários simplesmente evitarão compartilhar opiniões controversas. Da mesma forma, quando um provedor de serviços não tem

relação com o comentarista ou público, as retiradas serão muito mais fáceis e baratas para o negócio do que uma análise de nuances do discurso de um determinado usuário.

3. As intervenções baseadas em conteúdo no nível da infraestrutura causam danos colaterais que prejudicam desproporcionalmente os grupos menos poderosos.

Quem tem poder e influência inevitavelmente explora todos os sistemas de censura para suprimir vozes e ideias impopulares. Na verdade, o bloqueio de infraestrutura é uma ferramenta favorita dos governos autoritários. Durante um período de agitação social em outubro de 2019, os usuários da internet no Equador enfrentaram repetidos bloqueios de rede. A Nigéria exigiu que os ISPs banissem o Twitter durante meses. Graças a uma aplicação excessiva das sanções dos EUA, a AWS bloqueou os usuários iranianos de seus serviços. A Cloudflare negou atendimento a uma instância da Mastodon que hospedava um coletivo de profissionais do sexo com sede na Austrália, citando os regulamentos dos EUA. E, claro, vários países fecharam completamente a internet.

Além disso, mesmo os decisores bem-intencionados subestimam regularmente o discurso dos povos marginalizados. No nível da plataforma, as empresas que se envolvem na moderação de conteúdo refletem e reforçam consistentemente o viés contra as comunidades marginalizadas. Não faltam exemplos: O Facebook decidiu, em meio à ascensão do movimento #MeToo, que a declaração “homens são lixo” constitui discurso de ódio; o Twitter decidiu usar cláusulas de assédio para encerrar o relato verificado de um proeminente ativista antitortura egípcio; várias decisões de moderação de conteúdo impediram mulheres de cor de compartilhar com seus amigos e seguidores histórias de assédio que sofreram; o Twitter decidiu marcar tweets contendo a palavra “queer” como ofensivos, independentemente do contexto.

Mesmo os pacientes que não podem pagar medicamentos prescritos são afetados. Em um esforço para policiar o uso da palavra “opioide” e palavras afins em hashtags, o Instagram fechou e proibiu contas que “pareciam” vender opioides. Uma consequência foi o encerramento da conta da PharmacyChecker, que dá informações de verificação e preço sobre farmácias online que ajudam os pacientes e seus cuidadores a pagar medicamentos através da importação, mas não vendem medicamentos.

Não há razão para pensar que as empresas de infraestrutura serão melhores do que as plataformas para tomar estas decisões e muitas razões para pensar que serão piores.

4. Os atores estatais e privados podem tentar se apoderar de qualquer caminho de intervenção baseado em conteúdo e expandir o controle sobre ele.

Os caminhos de intervenção, uma vez estabelecidos, podem proporcionar aos atores estatais, patrocinados pelo estado e privados outras ferramentas para controlar o diálogo público. Uma vez que os processos e ferramentas para interferir na expressão são desenvolvidos ou expandidos, as empresas podem esperar uma enxurrada de exigências para aplicá-los de forma mais ampla. No nível da plataforma, os atores estatais e patrocinados pelo estado têm ferramentas de sinalização específicas para silenciar a dissidência. E a Cloudflare, que presta uma variedade de serviços, incluindo proteções contra ataques DDos, relata que, depois de retirar os serviços de segurança de um site de teoria da conspiração de sites neonazistas, assistiu a um aumento dramático nas solicitações dos regimes autoritários de que fizesse o mesmo em relação às organizações de direitos humanos.

No contexto dos direitos autorais, os atores privados exploram regularmente processos fáceis de remoção para silenciar os críticos. Não há razão para esperar que isso seja diferentes em nível da infraestrutura.

5. A falta de concorrência e os custos de mudança dificultam ou impossibilitam responsabilizar algumas empresas por erros ou exageros.

Quando um ISP decide encerrar a conta de um usuário individual, em grande parte do mundo, nenhum outro provedor está disponível: o usuário é, de fato, expulso da vida online. Em outras camadas da stack, como o sistema de nome de domínio (DNS), há vários provedores para escolher – um comentarista cujo nome de domínio está congelado pode levar seu site para outro lugar. Mas a existência de alternativas por si só não é suficiente; é preciso avaliar os custos e a facilidade de mudar de provedor. Raramente há uma alternativa barata ou fácil. Em alguns locais, os atores governamentais podem estar intimamente ligados às empresas de infraestrutura; por exemplo, o governo do Quênia tem 35% de participação na empresa de telecomunicações Safaricom. E mesmo quando a troca for fácil, não será de grande ajuda se todos os provedores em um determinado nível da stack escolherem ou forem pressionados a censurar o mesmo conteúdo, comentaristas e/ou pontos de vista. Finalmente, o problema pode ser agravado quando os provedores de serviços são menores e, portanto, potencialmente mais vulneráveis à pressão dos governos e atores privados.

6. Os requisitos de intervenção podem ser contraproducentes.

Intervir para atingir o discurso online pode realmente prejudicar os objetivos deste. Por exemplo, os esforços para policiar o conteúdo “extremista” levaram ao bloqueio ou

apagamento do trabalho de jornalistas e defensores dos direitos humanos para documentar o terrorismo e outras atrocidades. A pressão para bloquear o acesso a serviços de internet em países específicos prejudicou os esforços para ajudar as pessoas a contornar a censura do governo e acessar informações precisas.

7. Infrastructure-level content-based interventions may undermine fundamental internet protocols and compromise security.

Some content-based interventions from infrastructure providers, such as inserting Deep Packet Inspection (DPI) on the network or blocking DNS queries, may reshape the internet's architecture to the detriment of privacy and security. For example, if operators of DNS resolvers began redirecting queries for certain domains based on content alone, it would vastly complicate efforts to make DNS resistant to malicious tampering, because computers cannot distinguish "good" redirections from attempts at website spoofing. If certificate authorities decide they will revoke digital certificates for some websites because they object to their content, the "chain of trust" upon which much internet security depends will be compromised. In addition, by violating a key design principle of the open internet, infrastructure level interventions may accelerate its fragmentation, as people build new infrastructure to bypass such interventions and existing infrastructure providers are faced with conflicting rules and blocking in one country or another based on which they obey.

8. Inconsistent rules are inevitable.

Infrastructure providers, like all service providers that operate across multiple jurisdictions, already face conflicting requirements based on the rules and values of the countries in which they operate. Complying with those conflicting rules is both expensive and, sometimes, impossible. By engaging in content policing, they invite new sets of obligations that may lead to a proverbial race to the bottom, e.g., blocking as much content, across the service, as is required to satisfy the most censorious jurisdiction.

Conclusão

The internet is an essential resource for billions of people around the world. We use it to communicate, to organize, to protest, to work, to learn, to buy and sell, to access government services and more. If the internet is to continue to play that role, we need it to be strong, flexible and secure. We need infrastructure providers to stay focused on their core mission: supporting a robust and resilient internet. That mission is far more important, and more protective of human rights, than attempting to build out content-based intervention processes that will inevitably cause more harm than good.

Assinado

Access Now

American Civil Liberties Union (ACLU)

ARTICLE 19

ARTICLE 19 México y Centroamérica

ASEAN Youth Forum

Asociación por los Derechos Civiles (ADC)

Asociația pentru Tehnologie si Internet (ApTI)

Association for Progressive Communications (APC)

Bits of Freedom

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)

Chaos Computer Club (CCC)

Citizen D / Državljan D

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Comun.al, Laboratorio de resiliencia digital

Data Privacy Brasil Research Association

Derechos Digitales - América Latina

Digitale Gesellschaft Schweiz (Switzerland)

Don't Delete Art (DDA)

Electronic Frontier Foundation (EFF)

Epicenter.works - for digital rights

European Center for Not-for-Profit Law (ECNL)

European Digital Rights (EDRi)

Fight for the Future (FFTF)

Förderverein Informationstechnik und Gesellschaft (Fitug e.V.)

Foundation for Media Alternatives (FMA)

Freemuse

Fundación Huaira

Fundación InternetBolivia.org

Fundación Karisma

Fundación Vía Libre

Global Forum for Media Development (GFMD)

Hiperderecho

Homo Digitalis

Instituto Nupef

Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC)

Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec)

Instituto de Referência em Internet e Sociedade (IRIS)

Intervozes - Coletivo Brasil de Comunicação Social

IT-Pol Denmark

Kandoo

Masaar - Technology and Law Community

National Coalition Against Censorship (NCAC)

Open Knowledge Foundation

OpenMedia

Open Rights Group

Red en Defensa de los Derechos Digitales (R3D)

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)

SeguDigital

SMEX

Southeast Asia Freedom of Expression Network (SAFEnet)

TAPOL

Taraaz

The Sex Workers Project of the Urban Justice Center

The Tor Project

The William Gomes Podcast

The Woodhull Freedom Foundation

Usuarios Digitales