PROTECT THE STACK

Infrastructure Providers Should Not Be Content Police

Protege la pila (stack): por qué los proveedores de infraestructuras no deben vigilar los contenidos

Los proveedores de servicios de infraestructura de Internet están siendo presionados para que desempeñen un mayor papel en la vigilancia de los contenidos y la participación en línea. Algunos están decidiendo intervenir por su cuenta.

Se trata de una tendencia peligrosa a la que hay que poner fin ahora.

Aunque el llamamiento a reclutar a toda la "pila" en la lucha para acabar con el discurso dañino puede ser comprensible en algunos casos, conducirá a una serie de consecuencias no deseadas, especialmente para los usuarios menos poderosos. Salvo raras excepciones, los gobiernos no deberían exigir tales intervenciones y las empresas de infraestructuras no deberían intervenir voluntariamente.

Antecedentes

Los usuarios y los responsables políticos están muy familiarizados con plataformas como Facebook, Twitter o YouTube. Pero esos servicios no son Internet. De hecho, la comunicación y el comercio en línea también dependen de un amplio abanico de proveedores de servicios, entre ellos los ISP y las telecos, como Comcast, Orange, MTN, Airtel, Movistar o Vodafone; registradores de nombres de dominio como Namecheap o GoDaddy; servicios de soporte como Amazon Web Services (AWS), autoridades de certificación (como Let's Encrypt), procesadores de pago como PayPal y M-Pesa, correo electrónico, servicios de mensajería y otros. En conjunto, estos proveedores se denominan a veces "pila tecnológica".

La mayoría de los usuarios utilizan Internet sin pensar en todos esos servicios de infraestructura subyacentes. Pero esos servicios son esenciales para la expresión, la privacidad y la seguridad en línea. Y cuando estos proveedores -muchos de los cuales tienen poco o ningún contacto con los usuarios- intervienen en función del contenido, sus decisiones pueden tener enormes repercusiones en los derechos humanos que pueden ser difíciles o imposibles de reparar.

Las dificultades y los riesgos específicos para la expresión y la privacidad pueden variar en función de la naturaleza del servicio. Pero para todos los proveedores de infraestructuras, se aplicará alguna combinación de las siguientes preocupaciones. En

conjunto, demuestran poderosamente por qué, salvo raras excepciones, los proveedores de infraestructuras deben mantenerse al margen de la vigilancia de contenidos.

Una nota sobre "la pila"

La pila (o "The Stack" es un término tomado de la informática y la ingeniería de software, que se utiliza para describir una combinación de herramientas, procesos, lenguajes de programación y mecanismos utilizados en combinación para construir una aplicación o un producto. En este contexto, lo utilizamos para describir Internet tal y como la conocemos, los proveedores de servicios, las plataformas, los procesos y otros agentes que hacen posible la web moderna.

La pila tecnológica incluye plataformas de contenido generado por el usuario, como Facebook y Twitter, así como la gama de proveedores de infraestructura mencionados anteriormente. Las plataformas de redes sociales se sitúan en la parte superior de la pila, mientras que los proveedores de infraestructura básica, como su proveedor de servicios de Internet, se encuentran en la parte inferior, con una amplia gama de intermediarios -incluidos los procesadores de pago y los registradores, entre otros- situados en el medio.

Los riesgo para los derechos humanos

1. La mayoría de los servicios de infraestructura no pueden adaptar sus prácticas de intervención para que sean necesarias y proporcionadas.

Las plataformas suelen tener diversas opciones de moderación. En cambio, muchos servicios de infraestructura no pueden dirigir su respuesta con la precisión que exigen las normas de derechos humanos. Twitter bloquea tuits específicos; Amazon Web Services deniega el servicio a un sitio o una cuenta entera, lo que significa que sus intervenciones afectan inevitablemente a mucho más que el discurso censurable que motivó la acción. El secuestro gubernamental de los servicios de telecomunicaciones para interrumpir Internet en todo un país es especialmente atroz.

Las acciones atroces también se producen en el ámbito de los dominios, donde los registradores que se oponen a la expresión de un sitio web no se centran solo en esa expresión, sino que suspenden y/o anulan el registro de todo el sitio. Por ejemplo, ARTICLE 19 ha documentado múltiples casos de "abuso de DNS": la suspensión y anulación del registro de nombres de dominio como medio para sofocar la disidencia.

Podemos tomar una lección aquí del contexto de los derechos de autor, donde también hemos visto a registradores de nombres de dominio y proveedores de alojamiento cerrar sitios enteros en respuesta a avisos de infracción dirigidos a un solo documento. Es posible que algunos servicios se comuniquen directamente con los clientes cuando estén preocupados por un contenido específico y soliciten su retirada. Pero si esa solicitud es rechazada, el servicio sólo tiene a su disposición el instrumento contundente de la retirada completa. Y algunos servicios pueden no tener una forma viable de comunicarse directamente con la fuente del contenido.

2. La notificación y la apelación significativas rara vez son posibles, especialmente para los menos poderosos.

Las normas de derechos humanos y los principios del debido proceso exigen que los proveedores de servicios notifiquen a los usuarios que su discurso y/o su cuenta han sido -o serán- retirados de la red, y que ofrezcan a los usuarios la oportunidad de buscar reparación. En el ámbito de la infraestructura, esta notificación y las oportunidades de reparación pueden ser imposibles. Los servicios de infraestructura a menudo no pueden comunicarse directamente con los usuarios de Internet, ya que normalmente no tienen una relación directa con el orador o la audiencia de la expresión en cuestión. Y a diferencia de los anfitriones de contenidos a nivel de plataforma, que pueden dejar un aviso explicativo en la ubicación original de una publicación eliminada (en una práctica a veces llamada "tombstoning"), los proveedores de infraestructura suelen carecer de la capacidad práctica de notificar a los futuros usuarios sobre las formas en que el proveedor ha impedido el acceso a los contenidos.

Así, por ejemplo, si un usuario descubre que un enlace enviado por un amigo no funciona, no puede saber fácilmente si hubo un problema con el enlace, si el propietario retiró el sitio voluntariamente o si fue bloqueado. Los usuarios de un servicio que depende de un procesador de pagos también pueden sorprenderse al ver que el servicio desaparece porque, sin saberlo, el procesador cerró el pago a ese servicio. En Argentina, por ejemplo, Uber dejó de funcionar de la noche a la mañana gracias a una orden judicial que obligaba a un procesador de pagos a bloquear los pagos al servicio.

Los usuarios están obligados a cumplir las condiciones de cada servicio en la cadena que va desde el orador hasta la audiencia, aunque no sepan cuáles son esos servicios o cómo contactar con ellos. Dadas las posibles consecuencias de las infracciones, y la dificultad de navegar por los procesos de apelación de los servicios previamente invisibles (suponiendo que tal proceso exista), muchos usuarios simplemente evitarán compartir opiniones controvertidas por completo. Por otra parte, cuando un proveedor de servicios no tiene relación con el orador o la audiencia, la retirada de contenidos será mucho más fácil y barata para la empresa que un análisis matizado del discurso de un determinado usuario.

3. Las intervenciones basadas en el contenido en cuanto a infraestructura causan daños colaterales que perjudican desproporcionadamente a los grupos menos poderosos.

Los que tienen poder e influencia explotan inevitablemente todos los sistemas de censura para suprimir las voces e ideas impopulares. De hecho, el bloqueo de la infraestructura es una herramienta favorita de los gobiernos autoritarios. Durante un período de agitación social sostenida en octubre de 2019, los usuarios de Internet en Ecuador se enfrentaron a repetidos bloqueos de la red. Nigeria exigió a los ISP que prohibieran Twitter durante meses. Gracias a una aplicación excesiva de las sanciones de Estados Unidos, AWS ha bloqueado a los usuarios iraníes de sus servicios. Cloudflare denegó el servicio a una instancia de Mastodon que alojaba a un colectivo de trabajadoras sexuales con sede en Australia, alegando la normativa estadounidense. Y, por supuesto, varios países han cerrado Internet por completo.

Además, incluso los responsables bienintencionados infravaloran habitualmente la expresión de los pueblos marginados. En el ámbito de las plataformas, las empresas que se dedican a la moderación de contenidos reflejan y refuerzan sistemáticamente los prejuicios contra las comunidades marginadas. Los ejemplos abundan: Facebook decidió, en pleno auge del movimiento #MeToo, que la afirmación "los hombres son basura" constituye un discurso de odio; Twitter decidió utilizar las disposiciones sobre acoso para cerrar la cuenta verificada de una destacada activista egipcia contra la tortura; varias decisiones de moderación de contenidos impidieron a las mujeres de color compartir con sus amigos y seguidores las historias de acoso que sufren; Twitter decidió marcar como ofensivos los tuits que contienen la palabra "queer", independientemente del contexto.

Incluso los pacientes que no pueden permitirse los medicamentos recetados se ven afectados. En un esfuerzo por vigilar el uso de la palabra "opioide" y palabras relacionadas en los hashtags, Instagram cerró y prohibió cuentas que "parecían" vender opioides. Una de las consecuencias fue el cierre de la cuenta de PharmacyChecker, que proporciona información sobre verificación y precios de las farmacias en línea que ayudan a los pacientes y a sus cuidadores a costear la medicación mediante la importación, pero que no vende medicamentos.

No hay ninguna razón para pensar que las empresas de infraestructuras serán mejores que las plataformas a la hora de hacer estas llamadas, y sí muchas razones para pensar que serán peores.

4. Los actores estatales y privados pueden intentar apropiarse de cualquier vía de intervención basada en los contenidos y ampliar su control.

Las vías de intervención, una vez establecidas, pueden proporcionar a los actores estatales, patrocinados por el Estado y privados, herramientas adicionales para controlar el diálogo público. Una vez que se desarrollen o amplíen los procesos y las herramientas para interferir en la expresión, las empresas pueden esperar una avalancha de demandas para aplicarlas de forma más amplia. En el ámbito de las plataformas, los actores estatales y patrocinados por el Estado han convertido en armas las herramientas de señalización para silenciar la disidencia. Y Cloudflare, que proporciona una variedad de servicios, incluida la protección contra los ataques DDos, informa que, después de retirar los servicios de seguridad de un sitio neonazi de teoría de la conspiración, vio un aumento dramático de las solicitudes de los regímenes autoritarios para que hiciera lo mismo con respecto a las organizaciones de derechos humanos.

En el contexto de los derechos de autor, los actores privados se aprovechan regularmente de los procesos de retirada fáciles para silenciar a los críticos. No hay razón para esperar que las cosas sean diferentes en el ámbito de las infraestructuras.

5. La falta de competencia y los costes de cambio hacen que sea difícil o imposible responsabilizar a algunas empresas por sus errores o extralimitaciones.

Cuando un ISP decide cerrar la cuenta de un usuario individual, en la mayor parte del mundo no hay ningún otro proveedor disponible: el usuario queda efectivamente fuera de línea. En otras capas de la pila, como el sistema de nombres de dominio (DNS), hay múltiples proveedores entre los que elegir: un orador cuyo nombre de dominio esté congelado puede llevar su sitio web a otro lugar. Pero la existencia de alternativas no es suficiente; hay que evaluar los costes y la facilidad para cambiar de proveedor. Rara vez hay una alternativa barata o fácil. Y en algunos lugares, los agentes gubernamentales pueden estar estrechamente vinculados a las empresas de infraestructuras; por ejemplo, el gobierno de Kenia tiene un 35% de la propiedad de la empresa de telecomunicaciones Safaricom. E incluso cuando el cambio es fácil, no servirá de nada si todos los proveedores de un determinado nivel de la pila eligen, o son presionados, para censurar los mismos contenidos, oradores y/o puntos de vista. Por último, el problema puede agravarse cuando los proveedores de servicios son más pequeños y, por tanto, potencialmente más vulnerables a las presiones de los gobiernos y los agentes privados.

6. Los requisitos de intervención pueden ser contraproducentes.

Intervenir en la expresión en línea puede socavar los objetivos a los que se supone que sirve. Por ejemplo, los esfuerzos por vigilar los contenidos "extremistas" han llevado a bloquear o borrar el trabajo de periodistas y defensores de los derechos humanos que

documentan el terrorismo y otras atrocidades. La presión para bloquear el acceso a los servicios de Internet en determinados países ha socavado los esfuerzos para ayudar a la gente a eludir la censura del gobierno y acceder a información precisa.

7. Las intervenciones basadas en contenidos a nivel de infraestructura pueden socavar los protocolos fundamentales de Internet y comprometer la seguridad.

Algunas intervenciones basadas en el contenido por parte de los proveedores de infraestructuras, como la inserción de la Inspección Profunda de Paquetes (DPI) en la red o el bloqueo de las consultas DNS, pueden remodelar la arquitectura de Internet en detrimento de la privacidad y la seguridad. Por ejemplo, si los operadores de los resolutores de DNS comenzaran a redirigir las consultas de ciertos dominios, basándose únicamente en el contenido, se complicarían enormemente los esfuerzos para hacer que el DNS sea resistente a la manipulación maliciosa, porque los ordenadores no pueden distinguir las redirecciones "buenas" de los intentos de falsificación de sitios web. Si las autoridades de certificación deciden revocar los certificados digitales de algunos sitios web porque se oponen a su contenido, la "cadena de confianza" de la que depende gran parte de la seguridad de Internet se verá comprometida. Además, al violar un principio de diseño clave de la Internet abierta, las intervenciones a nivel de infraestructura pueden acelerar su fragmentación, ya que la gente construye nuevas infraestructuras para eludir dichas intervenciones y los proveedores de infraestructuras existentes se enfrentan a normas contradictorias y a bloqueos en uno u otro país en función de lo que obedezcan.

8. Las normas incoherentes son inevitables.

Los proveedores de infraestructuras, como todos los proveedores de servicios que operan en varias jurisdicciones, ya se enfrentan a requisitos contradictorios basados en las normas y valores de los países en los que operan. Cumplir esas normas contradictorias es caro y, a veces, imposible. Al participar en la vigilancia de los contenidos, invitan a nuevos conjuntos de obligaciones que pueden conducir a una proverbial carrera hacia el fondo, por ejemplo, bloquear tantos contenidos, en todo el servicio, como sea necesario para satisfacer a la jurisdicción más censora.

Conclusión

Internet es un recurso esencial para miles de millones de personas en todo el mundo. Lo utilizamos para comunicarnos, organizarnos, protestar, trabajar, aprender, comprar y vender, acceder a servicios gubernamentales y mucho más. Para que Internet siga desempeñando ese papel, necesitamos que sea fuerte, flexible y segura. Necesitamos que los proveedores de infraestructuras se centren en su misión principal: apoyar una Internet robusta y resistente. Esa misión es mucho más importante, y más protectora de

los derechos humanos, que intentar crear procesos de intervención basados en los contenidos que inevitablemente causarán más daño que beneficio.

Firmado

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