PROTECT THE STACK

Infrastructure Providers Should Not Be Content Police

حماية الحزمة التكنولوجية: يجب ألا يكون مقدمي البنية التحتية شرطة المحتوى

يتعرض مقدمو خدمات البنية التحتية للإنترنت لضغوط للعب دور أكبر في مراقبة المحتوى والمشاركة عبر الإنترنت. البعض منهم قرر التدخل من تلقاء نفسه. وهذا توجه خطير يجب أن ينتهي الآن.

في حين أن الدعوة إلى تطويع "الحزمة التكنولوجية" الكاملة في العمل على إنهاء الخطاب المضر قد تكون مفهومة في بعض الحالات، إلا أنها ستؤدي إلى مجموعة من العواقب غير المقصودة، خاصة بالنسبة للمستخدمين/ات من الفئات المهمشة/ الضعيفة. مع مراعاة استثناءات نادرة، يجب ألا تطلب الحكومات مثل هذه التدخلات ويجب ألا تتدخل شركات البنية التحتية طواعية.

الخلفية

المستخدمون/ات وصناع/ صانعات السياسات على دراية كبيرة بالمنصات مثل فيسبوك أو تويتر أو يوتيوب. لكن هذه الخدمات ليست الإنترنت. في الواقع، تعتمد الاتصالات والتجارة عبر الإنترنت أيضًا على مجموعة واسعة من مزودي الخدمة، بما في ذلك مزودي خدمات الإنترنت وشركات الاتصالات، مثل كومكاست أو أورنج أو أم تي أن أو أرتيل أو موڤيستار أو ڤودافون؛ مسجلي اسم المجال مثل نيم چيبب أو وسلطات الشهادات (مثل ليتس أنكربت) ومعالجات الدفع مثل پايبال (AWS) غو دادي؛ خدمات الدعم مثل خدمات أمازون للشبكة "وأم-بيسا والبريد الإلكتروني وخدمات المراسلة والمزيد. هؤلاء المزودين جميعا مجتمعين، يُطلق عليهم أحيانًا اسم "الحزمة التكنولوجية.

يستخدم معظم المستخدمين/ات الإنترنت دون التفكير في كل خدمات البنية التحتية الأساسية. لكن هذه الخدمات ضرورية للتعبير عبر الإنترنت والخصوصية والأمان. وعندما يتدخل هؤلاء المزودون – وكثير منهم ليس لديه اتصال يذكر بالمستخدمين/ات – بناءً على المحتوى، يمكن أن يكون لخياراتهم تأثيرات هائلة على حقوق الإنسان قد يكون من الصعب أو المستحيل تصحيحها.

قد تختلف المزالق والمخاطر المحددة للتعبير والخصوصية تبعًا لطبيعة الخدمة. ولكن بالنسبة لكل مزودي للبنية التحتية، سيكون من المهم الاطلاع على المحاذير التالية. مجتمعة، توضح بقوة لماذا، مع استثناءات نادرة، يجب على مزودي البنية التحتية الابتعاد عن مراقبة المحتوى.

ملاحظة حول "الحزمة التكنولوجية "

الحزمة التكنولوجية مصطلح مستعار من علوم الكمبيوتر وهندسة البرمجيات، يستخدم لوصف مجموعة من الأدوات والعمليات ولغات البرمجة والآليات المستخدمة معًا لبناء تطبيق أو منتج. في هذا السياق، نستخدمه لوصف الإنترنت كما نعرفه، ومزودي الخدمة، والمنصات، والعمليات، والعديد من اللاعبين الآخرين الذين يجعلون الانترنت الحديث ممكنًا.

تتضمن الحزمة التكنولوجية منصات المحتوى التي ينشئها المستخدم مثل فيسبوك وتويتر بالإضافة إلى مجموعة من مزودي البنية التحتية المشار إليهم أعلاه. تقع منصات وسائل التواصل الاجتماعي في الجزء العلوي من المجموعة، بينما يقع موفرو البنية التحتية الأساسية مثل مزودوا خدمة الإنترنت في الجزء السفلي، مع وجود مجموعة واسعة من الوسطاء – بما في ذلك معالجات الدفع والمسجلين وكل الآخرين الذين يقعون في الوسط.

المخاطر على حقوق الإنسان

1. معظم خدمات البنية التحتية لا تستطيع تكييف ممارسات التدخل الخاصة بها لتكون ضرورية ومتناسبة.

غالبًا ما تحتوي المنصات على مجموعة متنوعة من خيارات الإشراف. على النقيض من ذلك، لا يمكن للعديد من خدمات البنية التحتية أن توجه تقديم الخدمة إلى (AWS) استجابتها بالدقة التي تتطلبها معايير حقوق الإنسان. تويتر يحظر تغريدات محددة؛ ترفض خدمات أمازون للشبكة موقع أو حساب كامل، مما يعني أن تدخلاتها تؤثر حتماً أكثر بكثير من الخطاب المرفوض الذي حفز الإجراء. يعد اختطاف الحكومة لخدمات الاتصالات السلكية واللاسلكية لتعطيل الإنترنت في دولة بأكملها أمرٌ فظيع بشكل خاص.

تحدث أيضًا الإجراءات الفظيعة على مستوى النطاق، حيث لا يُستهدف المُسجِلون الذين يعترضون على خطاب على الموقع الالكتروني لا يستهدفون هذا الخطاب فحسب، بل يقومون بتعليق و/أو إلغاء تسجيل الموقع بالكامل. على سبيل المثال، قامت منظمة المادة 19 بتوثيق حالات متعددة من "إساءة استخدام DNS": تعليق وإلغاء تسجيل أسماء النطاقات كوسيلة لخنق المعارضة.

يمكننا أن نتعلم درسًا هنا من سياق حقوق الطبع والنشر، حيث رأينا أيضًا أن مسجلي أسماء النطاقات وموفري الاستضافة يغلقون مواقع بأكملها ردًا على إشعارات الانتهاك التي تستهدف مستندًا واحدًا. قد يكون من الممكن لبعض الخدمات التواصل مباشرة مع العملاء حيث يشعرون بالقلق بشأن جزء معين من المحتوى ويطلبون إزالته. ولكن إذا تم رفض هذا الطلب، فإن الخدمة لديها فقط أداة واحدة حادة وهي للإزالة الكاملة تحت تصرفها. قد لا تتوفر لبعض الخدمات طريقة قابلة للتطبيق للتواصل مباشرة مع مصدر المحتوى على الإطلاق.

2. نادرًا ما يكون الإشعار الجاد والاستئناف ممكنًا، خاصة بالنسبة للأشخاص المهمشين.

تتطلب معايير حقوق الإنسان ومبادئ الإجراءات القانونية أن يقوم مقدمو الخدمة بإخطار المستخدمين/ات بأن كلامهم/ن و/أو حسابهم/ن قد تم - أو سيتم - اغلاقها، وإتاحة الفرصة للمستخدمين/ات لطلب الإنصاف. على مستوى البنية التحتية، قد يكون هذا الإخطار وفرص الإنصاف مستحيلة. غالبًا ما تكون خدمات البنية التحتية غير قادرة على التواصل مباشرة مع مستخدمي/ات الإنترنت نظرًا لأن الخدمات عادة لا تتمتع بعلاقة مباشرة مع المتحدث/ة أو الجمهور للحديث عن محل الخلاف. وعلى عكس مستوى المنصات مستضيفة المحتوى، الذين يمكنهم ترك إشعار توضيحي في الموقع الأصلي للمنشور المحذوف (في ممارسة تسمى أحيانًا بـ"رجم القبور")، يفتقر موفرو البنية التحتية عادةً القدرة العملية لإعلام المستخدمين/ات المستقبليين/ات بالطرق التي قد يقوم فيها المزود بإعاقة الوصول إلى المحتوى.

وبالتالي، على سبيل المثال، إذا اكتشف/ت المستخدم/ة أن رابطا أرسله صديق/ة لا يعمل، فلن ت/يتمكن بسهولة من معرفة ما إذا كانت هناك مشكلة في الرابط، أو ما إذا كان المالك قد أوقف الموقع طواعية، أو ما إذا كان قد تم حظره. قد يجد مستخدمو/ات الخدمة التي تعتمد على معالج

الدفع أيضًا الخدمة اختفت لأنه، غير معروف بالنسبة لهم/ن، أن المعالج منع الدفع لتلك الخدمة. في الأرجنتين، على سبيل المثال، تم قطع خدمة أوبر بين عشية وضحاها بفضل أمر محكمة يطلب من معالج الدفع منع تحويل الأموال إلى الخدمة.

يلتزم المستخدمون/ات بشكل أساسي بشروط وأحكام كل خدمة في السلسلة من المتحدث/ة إلى الجمهور، على الرغم من أنهم/ن قد لا يعرفون ما هي هذه الخدمات أو ما يربطها بهم/ن. نظرًا للعواقب المحتملة للانتهاكات، وصعوبة التنقل في عمليات الاستئناف للخدمات غير المرئية سابقًا (بافتراض وجود مثل هذه العملية)، سيتجنب العديد من المستخدمين/ات ببساطة مشاركة الآراء المثيرة للجدل تمامًا. وبالمثل، في حالة عدم وجود علاقة بين مقدم الخدمة والمتحدث/ة أو الجمهور، ستكون عمليات الإزالة أسهل بكثير وأرخص للشركة من إجراء تحليل دقيق لخطاب مستخدم/ة معين/ة.

3. تتسبب التدخلات القائمة على المحتوى على مستوى البنية التحتية في أضرار جانبية من شأنها إلحاق الضرر بشكل غير متناسب بالمجموعات المهمشة.

أولئك الذين يتمتعون بالسلطة والنفوذ يستغلون حتماً جميع أنظمة الرقابة لقمع الأصوات والأفكار غير المتداولة. في الواقع، يعد حظر البنية التحتية أداة مفضلة للحكومات الاستبدادية. خلال فترة الاضطرابات في أكتوبر 2019، واجه مستخدمو/ات الإنترنت في الإكوادور عمليات حظر متكررة للشبكة. طلبت نيجيريا من مزودي خدمة الإنترنت حظر تويتر لأشهر. بفضل التطبيق الواسع للولايات المتحدة العقوبات، وقد المستخدمين/ات الإيرانيين/ات من خدماتها. رفضت كلاود فلار تقديم الخدمة إلى ماستودون الذي (AWS) منعت خدمات أمازون للشبكة استضاف مجموعة المشتغلين/ات بالجنس في أستراليا، نقلاً عن اللوائح الأمريكية. وبالطبع قامت عدة دول بإغلاق الإنترنت تمامًا.

علاوة على ذلك، حتى صانعي القرار ذوي النوايا الحسنة يقللون بشكل منتظم من أهمية خطاب الشعوب المهمشة. على مستوى المنصة، تعكس الشركات التي تشارك في الإشراف على المحتوى باستمرار التحيز ضد المجتمعات المهمشة. الأمثلة كثيرة: قررت فيسبوك، في خضم صعود أن عبارة "الرجال قمامة" تشكل خطاب كراهية. قرر موقع تويتر استخدام أحكام التحرش لإغلاق حساب موثق لناشط ،MeToo# حركة مصري بارز مناهض للتعذيب؛ منعت قرارات الإشراف المختلفة على المحتوى النساء ذوات البشرة الملونة من مشاركة قصص التحرش التي يتعرضن لها مع أصدقائهن ومتابعيهن؛ قرر تويتر وضع علامة على التغريدات التي تحتوي على كلمة "كوير" على أنها مسيئة، بغض النظر عن السياق.

حتى المرضى الذين لا يستطيعون تحمل تكاليف الأدوية يتأثرون. في محاولة لمراقبة استخدام كلمة "أفيوني" والكلمات ذات الصلة في الهاشتاج، أغلق انستاغرام وحظر الحسابات التي "ظهرت" لبيع المواد الأفيونية. كانت إحدى النتائج إغلاق حساب فارماسي تشيكر الذي يوفر معلومات التحقق والأسعار حول صيدليات الإنترنت التي تساعد المرضى ومقدمي الرعاية لهم/ن على ، PharmacyChecker الوصول للأدوية بتكلفة أقل من خلال الاستيراد، ولكنه لا يبيع الأدوية.

لا يوجد سبب للاعتقاد بأن شركات البنية التحتية ستكون أفضل من المنصات في التعامل مع هذه الإجراءات، والعديد من الأسباب للاعتقاد بأنها ستكون أسوأ.

4. قد تسعى الجهات الحكومية والخاصة إلى اختطاف أي مسار تدخل قائم على المحتوى وتوسيع نطاق السيطرة عليه.

قد تزود مسارات التدخل، بمجرد إنشائها، الجهات الحكومية والخاصة التي ترعاها الدولة والجهات الخاصة بأدوات إضافية للتحكم في النقاش العام. بمجرد تطوير أو توسيع العمليات والأدوات اللازمة للتدخل في التعبير، يمكن للشركات أن تتوقع سيلًا من المطالب لتطبيقها على نطاق أوسع. على مستوى المنصة، استخدمت الدولة والجهات الفاعلة التي ترعاها الدولة أدوات الإبلاغ كسلاح لتسكيت المعارضين/ات. وتفيد شركة كلاود فلار، التي توفر مجموعة متنوعة من الخدمات، بما في ذلك الحماية من هجمات قطع الخدمة، أنه بعد أن سحبت خدمات الأمن من موقع نظرية المؤامرة النازية الجديدة، شهدت زيادة كبيرة في الطلبات من الأنظمة الاستبدادية التي تود فعل الشيء ذاته لمنظمات تعني بحقوق الإنسان.

في سياق حقوق النشر، تستغل الجهات الفاعلة الخاصة بانتظام عمليات الإزالة السهلة لإسكات النقاد. لا يوجد سبب لتوقع أن تكون الأمور مختلفة على مستوى البنية التحتية.

5. عدم وجود المنافسة وتكاليف التحويل تجعل من الصعب أو المستحيل تحميل بعض الشركات المسؤولية عن الأخطاء أو التجاوزات.

عندما يقرر مزود خدمة الإنترنت إغلاق حساب مستخدم/ة، في كثير من أنحاء العالم، لا يتوفر أي مزود آخر: يتم فعليًا طرد المستخدم/ة دون هناك العديد من المزودين للاختيار من بينهم - يمكن للشخص ، (DNS) اتصال. في طبقات أخرى من الحزمة التكنولوجية، مثل نظام اسم المجا الذي تم تجميد اسم المجال الذي يملكه أن يأخذ موقعه على الانترنت في مكان آخر. لكن وجود البدائل وحده لا يكفي؛ يجب على المرء تقييم التكاليف وسهولة تبديل مقدمي الخدمة. نادرًا ما يوجد بديل رخيص أو سهل. وفي بعض المناطق، قد تكون الجهات الحكومية على صلة وثيقة بشركات البنية التحتية؛ على سبيل المثال، تمتلك حكومة كينيا 35٪ من ملكية شركة الاتصالات السلكية واللاسلكية سفاريكوم. وحتى عندما يكون التبديل سهلاً، فلن يساعد إذا اختار جميع مقدمي الخدمة مستوى معينًا من الحزمة التكنولوجية، أو تم الضغط عليهم لفرض رقابة على نفس المحتوى و/أو المتحدثين/ات و/ أو وجهات النظر. أخيرًا، قد تتفاقم المشكلة عندما يكون مقدمو الخدمات أصغر حجمًا، وبالتالي، من المحتمل أن يكونوا أكثر عرضة للضغط من الحكومات والجهات الفاعلة الخاصة.

6. متطلبات التدخل قد تأتي بنتائج عكسية.

قد يؤدي التدخل لاستهداف النقاش عبر الإنترنت في الواقع إلى تقويض الأهداف التي من المفترض أن تخدمها. على سبيل المثال، أدت الجهود المبذولة لمراقبة المحتوى "المتطرف" إلى منع أو محو عمل الصحفيين/ات والمدافعين/ات عن حقوق الإنسان لتوثيق الإرهاب والفظائع الأخرى. أدى الضغط لمنع الوصول إلى خدمات الإنترنت في بلدان معينة إلى تقويض الجهود المبذولة لمساعدة الناس على تجاوز الرقابة الحكومية والوصول إلى معلومات دقيقة.

7. قد تقوض التدخلات القائمة على المحتوى على مستوى البنية التحتية بروتوكولات الإنترنت الأساسية وتعرض الأمن للخطر.

على الشبكة أو حظر (DPI) قد تعيد بعض التدخلات القائمة على المحتوى من موفري البنية التحتية، مثل إدخال فحص الحزمة العميق DNS تشكيل بنية الإنترنت على حساب الخصوصية والأمان. على سبيل المثال، إذا بدأ مشغلو محللات ، DNS استعلامات نظام اسم المجال مقاومًا للعبث DNS في إعادة توجيه الاستعلامات لبعض المجالات بناءً على المحتوى وحده، فسيؤدي ذلك إلى تعقيد الجهود المبذولة لجعل الخبيث، لأن أجهزة الكمبيوتر لا يمكنها التمييز بين عمليات إعادة التوجيه "الجيدة" ومحاولات انتحال موقع الكتروني. إذا قررت المراجع المصدقة أنها ستلغي الشهادات الرقمية لبعض المواقع الالكترونية لأنها تعترض على محتواها، فسيتم اختراق "سلسلة الثقة" التي يعتمد عليها قدر كبير من أمان الإنترنت. بالإضافة إلى ذلك، من خلال انتهاك مبدأ التصميم الرئيسي للإنترنت المفتوح، قد تؤدي التدخلات على مستوى البنية التحتية إلى تسريع تجزئتها، حيث يقوم الأشخاص ببناء بنية تحتية جديدة لتجاوز مثل هذه التدخلات ويواجه موفرو البنية التحتية الحاليون قواعد متضاربة وحظرًا في بلد أو آخر بناءً على أي منهم يتبعون.

8. القواعد غير المتسقة أمر لا مفر منه.

يواجه مقدمو البنية التحتية، مثل جميع مزودي الخدمات الذين يعملون عبر ولايات قضائية متعددة، متطلبات متضاربة بناءً على قواعد وقيم البلدان التي يعملون فيها. يعد الامتثال لتلك القواعد المتضاربة أمرًا مكلفًا ومستحيلًا في بعض الأحيان. من خلال الانخراط في مراقبة المحتوى، فإنهم يتبنون مجموعات جديدة من الالتزامات التي قد تؤدي إلى سباق يضرب به المثل إلى القاع، على سبيل المثال، حظر أكبر قدر من المحتوى، عبر الخدمة، كما هو مطلوب لتلبية أكثر السلطات الرقابية.

الخلاصة

الإنترنت هو مصدر أساسي لمليارات الأشخاص حول العالم. يستخدم للتواصل والتنظيم والاحتجاج والعمل والتعلم والشراء والبيع والوصول إلى الخدمات الحكومية وغير ذلك. إذا كان للإنترنت أن يستمر في لعب هذا الدور، فنحن بحاجة إلى أن يكون قويا ومرنا وآمنا. نحن بحاجة ليظل مزودي البنية التحتية مركزين على مهمتهم الأساسية: دعم إنترنت قوي ومرن. هذه المهمة هي الأكثر أهمية، وأكثر حماية لحقوق الإنسان، من محاولة بناء عمليات تدخل قائمة على المحتوى من شأنها أن تسبب حتما ضررًا أكثر من نفعها.

توقيع

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