PROTECT THE STACK

Infrastructure Providers Should Not Be Content Police

Protégez la couche : Les fournisseurs d'infrastructure ne devraient pas être la police du contenu

Les fournisseurs de services d'infrastructure Internet sont sous pression pour jouer un plus grand rôle dans le contrôle du contenu et de la participation en ligne. Certains décident d'intervenir seuls. C'est une tendance dangereuse qui doit cesser maintenant.

Bien que l'appel à enrôler toute la "couche" dans la lutte pour mettre fin aux discours nuisibles puisse être compréhensible dans certains cas, il entraînera une foule de conséquences imprévues, en particulier pour les utilisateurs les moins puissants. Sous réserve de rares exceptions, les gouvernements ne devraient pas exiger de telles interventions et les entreprises d'infrastructure ne devraient pas intervenir volontairement.

Antécédents

Les utilisateurs et les décideurs connaissent très bien les plateformes comme Facebook, Twitter ou YouTube. Mais ces services ne sont pas Internet. En fait, la communication et le commerce en ligne dépendent également d'un large éventail de fournisseurs de services, y compris les FAI et les opérateurs de télécommunications, comme Comcast, Orange, MTN, Airtel, Movistar ou Vodafone ; les bureaux d'enregistrement de noms de domaine tels que Namecheap ou GoDaddy ; des services de support tels qu'Amazon Web Services (AWS), des autorités de certification (telles que Let's Encrypt), des processeurs de paiement tels que PayPal et M-Pesa, des e-mails, des services de messagerie, etc. Pris ensemble, ces fournisseurs sont parfois appelés la "couche technologique".

La plupart des utilisateurs utilisent Internet sans penser à tous ces services d'infrastructure sous-jacents. Mais ces services sont essentiels à l'expression, à la confidentialité et à la sécurité en ligne. Et lorsque ces fournisseurs, dont beaucoup n'ont que peu ou pas de contact avec les utilisateurs, interviennent sur la base du contenu, leurs choix peuvent avoir d'énormes impacts sur les droits de l'homme qui peuvent être difficiles, voire impossibles à réparer.

Les pièges et les risques spécifiques à l'expression et à la vie privée peuvent varier en fonction de la nature du service. Mais pour chaque fournisseur d'infrastructure, une combinaison des préoccupations suivantes s'appliquera. Pris ensemble, ils démontrent avec force pourquoi, à de rares exceptions près, les fournisseurs d'infrastructure devraient rester en dehors de la réglementation du contenu.

Une note sur « la couche »

La couche est un terme emprunté à l'informatique et au génie logiciel, utilisé pour décrire une combinaison d'outils, de processus, de langages de programmation et de mécanismes utilisés en combinaison pour créer une application ou un produit. Dans ce contexte, nous l'utilisons pour décrire Internet tel que nous le connaissons, les fournisseurs de services, les plateformes, les processus et divers autres acteurs qui rendent possible le Web moderne.

La couche technologique comprend des plateformes de contenu générées par les utilisateurs telles que Facebook et Twitter, ainsi que la gamme de fournisseurs d'infrastructures référencés ci-dessus. Les plateformes de médias sociaux se situent au sommet de la pile, tandis que les fournisseurs d'infrastructure de base tels que votre FAI se trouvent au bas, avec un large éventail d'intermédiaires, y compris les processeurs de paiement et les bureaux d'enregistrement, entre autres, assis entre les deux.

Les risques pour les droits humains

1. La plupart des services d'infrastructure ne peuvent pas adapter leurs pratiques d'intervention pour qu'elles soient nécessaires et proportionnées.

Les plateformes ont souvent une variété d'options de modération. En revanche, de nombreux services d'infrastructure ne peuvent pas cibler leur réponse avec la précision exigée par les normes relatives aux droits de l'homme. Twitter bloque des tweets spécifiques ; Amazon Web Services refuse le service à un site ou à un compte entier, ce qui signifie que ses interventions affectent inévitablement bien plus que le discours répréhensible qui a motivé l'action. Le détournement par le gouvernement des services de télécommunications pour perturber Internet pour tout un pays est particulièrement flagrant.

Des actions flagrantes se produisent également au niveau du domaine, où les bureaux d'enregistrement qui s'opposent à la parole sur un site Web ne ciblent pas uniquement cette parole, mais suspendent et/ou désenregistrent l'ensemble du site. Par exemple, ARTICLE 19 a documenté plusieurs cas d' « abus de DNS »: la suspension et le retrait de noms de domaine comme moyen d'étouffer la dissidence.

Nous pouvons ici tirer une leçon du contexte du droit d'auteur, où nous avons également vu des bureaux d'enregistrement de noms de domaine et des hébergeurs fermer des sites entiers en réponse à des avis d'infraction ciblant un seul document. Il peut être possible pour certains services de communiquer directement avec les clients lorsqu'ils sont préoccupés par un contenu spécifique et de demander qu'il soit retiré. Mais si cette demande est rejetée, le service n'a à sa disposition que l'instrument contondant de la suppression complète. Et certains services peuvent ne pas avoir de moyen viable de communiquer directement avec la source du contenu.

2. Un avis et un appel significatifs sont rarement possibles, en particulier pour les moins puissants.

Les normes relatives aux droits de l'homme et les principes de procédure régulière exigent que les fournisseurs de services informent les utilisateurs que leur discours et/ou leur compte ont été - ou seront - mis hors ligne, et offrent aux utilisateurs la possibilité de demander réparation. Au niveau de l'infrastructure, un tel avis et des possibilités de réparation peuvent être impossibles. Les services d'infrastructure sont souvent incapables de communiquer directement avec les internautes car les services n'ont généralement pas de relation directe avec l'orateur ou le public de l'expression en question. Et contrairement aux hébergeurs de contenu au niveau de la plate-forme, qui peuvent laisser une notice explicative à l'emplacement d'origine d'une publication supprimée (dans une pratique parfois appelée "désactivation"), les fournisseurs d'infrastructure n'ont généralement pas la capacité pratique d'informer les futurs utilisateurs de la manière dont le fournisseur a entravé l'accès au contenu.

Ainsi, par exemple, si un utilisateur découvre qu'un lien envoyé par un ami ne fonctionne pas, il ne peut pas facilement savoir s'il y a eu un problème avec le lien, si le propriétaire a volontairement fermé le site ou s'il a été bloqué. Les utilisateurs d'un service qui s'appuie sur un processeur de paiement peuvent également être surpris de voir le service disparaître car, à leur insu, le processeur a interrompu le paiement de ce service. En Argentine, par exemple, Uber a été interrompu du jour au lendemain grâce à une décision de justice exigeant qu'un processeur de paiement bloque les paiements au service.

Les utilisateurs sont essentiellement tenus aux termes et conditions de chaque service de la chaîne, du conférencier au public, même s'ils ne savent peut-être pas quels sont ces services ou comment les contacter. Compte tenu des conséquences potentielles des violations et de la difficulté de naviguer dans les processus d'appel de services auparavant invisibles (en supposant qu'un tel processus existe même), de nombreux utilisateurs éviteront simplement de partager des opinions controversées. De même, lorsqu'un fournisseur de services n'a aucune relation avec l'orateur ou le public, les retraits seront beaucoup plus faciles et moins chers pour l'entreprise qu'une analyse nuancée du discours d'un utilisateur donné.

3. Les interventions basées sur le contenu au niveau de l'infrastructure causent des dommages collatéraux qui nuiront de manière disproportionnée aux groupes les moins puissants.

Ceux qui ont du pouvoir et de l'influence exploitent inévitablement tous les systèmes de censure pour réprimer les voix et les idées impopulaires. En effet, le blocage des infrastructures est un outil favori des gouvernements autoritaires. Au cours d'une période de troubles sociaux soutenus en octobre 2019, les internautes équatoriens ont été confrontés à des blocages répétés du réseau. Le Nigeria a demandé aux FAI d'interdire Twitter pendant des mois. Grâce à une application trop large des sanctions américaines, AWS a bloqué les utilisateurs iraniens de ses services. Cloudflare a refusé le service à une instance de Mastodon qui hébergeait un collectif de travailleuses du sexe basé en Australie, citant la réglementation américaine. Et bien sûr, plusieurs pays ont complètement fermé Internet.

De plus, même des décideurs bien intentionnés sous-estiment régulièrement la parole des personnes marginalisées. Au niveau de la plateforme, les entreprises qui s'engagent dans la modération de contenu reflètent et renforcent systématiquement les préjugés contre les communautés marginalisées. Les exemples ne manquent pas : Facebook a décidé, au milieu de la montée du mouvement #MeToo, que l'affirmation « les hommes sont des déchets » constituait un discours haineux ; Twitter a décidé d'utiliser les dispositions relatives au harcèlement pour fermer le compte vérifié d'un éminent militant anti-torture égyptien ; diverses décisions de modération de contenu ont empêché les femmes de couleur de partager avec leurs amis et abonnés des histoires de harcèlement qu'elles subissent ; Twitter a décidé de marquer les tweets contenant le mot "queer" comme offensants, quel que soit le contexte.

Même les patients qui n'ont pas les moyens d'acheter des médicaments sur ordonnance sont touchés. Dans un effort pour contrôler l'utilisation du mot "opioïde" et des mots apparentés dans les hashtags, Instagram a fermé et interdit les comptes qui "semblaient" vendre des opioïdes. L'une des conséquences a été la fermeture du compte de PharmacyChecker, qui fournit des informations de vérification et de prix sur les pharmacies en ligne qui aident les patients et leurs soignants à acheter des médicaments par importation, mais ne vendent pas de médicaments.

Il n'y a aucune raison de penser que les entreprises d'infrastructure seront meilleures que les plateformes pour passer ces appels, et de nombreuses raisons de penser qu'elles seront pires.

4. Les acteurs étatiques et privés peuvent chercher à détourner toute voie d'intervention basée sur le contenu et à en étendre le contrôle.

Les voies d'intervention, une fois établies, peuvent fournir aux acteurs étatiques, parrainés par l'État et privés des outils supplémentaires pour contrôler le dialogue public. Une fois que les processus et les outils pour interférer avec l'expression sont développés ou étendus, les entreprises peuvent s'attendre à un flot de demandes pour les appliquer plus largement. Au niveau de la plateforme, les acteurs étatiques et parrainés par l'État ont armé des outils de signalement pour faire taire la dissidence. Et Cloudflare, qui fournit une variété de services, y compris des protections contre les attaques DDos, rapporte qu'après avoir retiré les services de sécurité d'un site de théorie du complot néo-nazi, il a vu une augmentation spectaculaire des demandes de régimes autoritaires qu'il fait de même avec respect des organisations de défense des droits de l'homme.

Dans le contexte du droit d'auteur, des acteurs privés exploitent régulièrement des processus de retrait faciles pour faire taire les critiques. Il n'y a aucune raison de s'attendre à ce que les choses soient différentes au niveau de l'infrastructure.

5. Le manque de concurrence et les coûts de changement font qu'il est difficile, voire impossible, de tenir certaines entreprises responsables des erreurs ou des excès.

Lorsqu'un FAI décide de fermer le compte d'un utilisateur individuel, dans la plupart des pays du monde, aucun autre fournisseur n'est disponible : l'utilisateur est en fait mis hors ligne. À d'autres couches de la pile, telles que le système de noms de domaine (DNS), il existe plusieurs fournisseurs parmi lesquels choisir - un locuteur dont le nom de domaine est gelé peut emmener son site Web ailleurs. Mais l'existence d'alternatives seules ne suffit pas ; il faut évaluer les coûts et la facilité de changer de fournisseur. Il existe rarement une alternative bon marché ou facile. Et dans certains endroits, les acteurs gouvernementaux peuvent être étroitement liés aux entreprises d'infrastructure ; par exemple, le gouvernement du Kenya détient 35 % de la société de télécommunications Safaricom. Et même lorsque le changement est facile, cela n'aidera pas si tous les fournisseurs à un certain niveau de la pile choisissent, ou subissent des pressions, de censurer le même contenu, les mêmes orateurs et/ou les mêmes points de vue. Enfin, le problème peut être aggravé lorsque les prestataires de services sont plus petits et, par conséquent, potentiellement plus vulnérables aux pressions des gouvernements et des acteurs privés.

6. Les exigences d'intervention peuvent être contre-productives.

Intervenir pour cibler le discours en ligne peut en fait saper les objectifs qu'il est censé servir. Par exemple, les efforts pour contrôler les contenus « extrémistes » ont conduit au blocage ou à l'effacement du travail des journalistes et des défenseurs des droits humains pour documenter le terrorisme et d'autres atrocités. La pression pour bloquer l'accès aux services Internet dans certains pays a sapé les efforts visant à aider les gens à contourner la censure gouvernementale et à accéder à des informations précises.

7. Les interventions basées sur le contenu au niveau de l'infrastructure peuvent saper les protocoles Internet fondamentaux et compromettre la sécurité.

Certaines interventions basées sur le contenu des fournisseurs d'infrastructure, telles que l'insertion d'une inspection approfondie des paquets (DPI) sur le réseau ou le blocage des requêtes DNS, peuvent remodeler l'architecture d'Internet au détriment de la confidentialité et de la sécurité. Par exemple, si les opérateurs de résolveurs DNS commençaient à rediriger les requêtes pour certains domaines en se basant uniquement sur le contenu, cela compliquerait considérablement les efforts visant à rendre le DNS résistant aux altérations malveillantes, car les ordinateurs ne peuvent pas distinguer les «bonnes» redirections des tentatives d'usurpation de site Web. Si les autorités de certification décident de révoquer les certificats numériques de certains sites Web parce qu'elles s'opposent à leur contenu, la « chaîne de confiance » dont dépend une grande partie de la sécurité sur Internet sera compromise. De plus, en violant un principe de conception clé de l'internet ouvert, les interventions au niveau de l'infrastructure peuvent accélérer sa fragmentation, car les gens construisent de nouvelles infrastructures pour contourner ces interventions et les fournisseurs d'infrastructures existants sont confrontés à des règles contradictoires et à des blocages dans un pays ou un autre en fonction de ils obéissent.

8. Les règles incohérentes sont inévitables.

Les fournisseurs d'infrastructures, comme tous les fournisseurs de services qui opèrent dans plusieurs juridictions, sont déjà confrontés à des exigences contradictoires basées sur les règles et les valeurs des pays dans lesquels ils opèrent. Se conformer à ces règles contradictoires est à la fois coûteux et parfois impossible. En s'engageant dans le contrôle du contenu, ils invitent de nouveaux ensembles d'obligations qui peuvent conduire à une course proverbiale vers le bas, par exemple, bloquer autant de contenu, à travers le service, qu'il est nécessaire pour satisfaire la juridiction la plus censurée.

Conclusion

Internet est une ressource essentielle pour des milliards de personnes dans le monde. Nous l'utilisons pour communiquer, organiser, protester, travailler, apprendre, acheter et vendre, accéder aux services gouvernementaux et plus encore. Si Internet doit continuer à jouer ce rôle, nous avons besoin qu'il soit solide, flexible et sécurisé. Nous avons besoin que les fournisseurs d'infrastructure restent concentrés sur leur mission principale : soutenir un Internet robuste et résilient. Cette mission est bien plus importante et plus protectrice des droits de l'homme que de tenter de mettre en place des processus d'intervention basés sur le contenu qui causeront inévitablement plus de mal que de bien.

Signé

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