

PRINCIPIOS DEMOCRÁTICOS PARA UNA INTERNET ABIERTA

Poniendo los Principios de Internet Abierta a trabajar por la
democracia



ÍNDICE GENERAL

Generalidades	2
Libertad de Expresión	3
Libertad de Reunión y Asociación	6
Accesibilidad	9
Privacidad y Protección de Datos	11
Protección Personal y Seguridad Safety	14
Inclusión	16
Igualdad en la Red	18
Estándares	20
Gobernanza	22

GENERALIDADES

Una Internet abierta – donde todos los ciudadanos puedan expresarse libremente, compartir y debatir ideas y participar en actividades económicas – es parte esencial de una democracia moderna y vibrante. Asegurar que Internet permanezca abierta y accesible es necesario para fortalecer el compromiso democrático, permitir la participación igualitaria en la economía de mercado y promover la responsabilidad social.

El cada vez mayor cambio del discurso político y social hacia las plataformas en línea ha llevado a un aumento correspondiente en el uso de Internet como una herramienta que puede silenciar la disidencia, promover la violencia y perpetuar las desigualdades preexistentes, incluido el acceso y el uso. La naturaleza nueva y en rápida evolución de Internet significa que muchos ciudadanos desconocen o están mal informados sobre cómo se aplican sus derechos fundamentales, como expresión, reunión y asociación, en un mundo digital.

Teniendo esto en cuenta, el Centro para la Empresa Privada Internacional (CIPE), el Instituto Democrático Nacional (NDI) y el Centro para la Asistencia Internacional de Medios (CIMA) han desarrollado los Principios Democráticos para una Internet Abierta. Estos nueve principios fueron informados por el trabajo de la Coalición Dinámica de los Derechos y Principios de Internet de las Naciones Unidas (IRPC por sus siglas en inglés), un grupo de trabajo de múltiples partes interesadas del Foro de Gobernanza de Internet (FGI), pionera en los esfuerzos para explicar cómo se manifiestan los derechos humanos internacionalmente reconocidos en el espacio digital. Lo que distingue a este documento es que examina los principios generales específicamente desde la perspectiva de cómo son un componente integral de una democracia robusta.

A medida que los ciudadanos y reformistas democráticos navegan en entornos políticos cambiantes, esperamos que esta guía ayude a los activistas que trabajan por la democracia en una era de Internet y los conecte en redes mundiales de pares para el intercambio de mejores prácticas. La guía también sirve como una herramienta de promoción que las organizaciones pueden utilizar para impulsar a los gobiernos, el sector privado y la sociedad civil a adherirse a los derechos humanos universales a través de los principios y estándares de una internet abierta.

1. LIBERTAD DE EXPRESIÓN

Todos deberían tener derecho a buscar, recibir y difundir información libremente en Internet sin censura o interferencias.

¿CÓMO SE VE ESTO EN UNA DEMOCRACIA?

Internet es un espacio para un debate público sólido en el que todas las personas, independiente de su religión, género, etnia, orientación sexual y clase socioeconómica pueden expresar libremente sus opiniones, incluidas opiniones disidentes sobre políticas, procedimientos y/o figuras públicas. Los usuarios de Internet deberían tener la posibilidad de debatir cualquier tema en línea sin interferencias indebidas, vigilancia ilegal o temor a represalias.

SEÑALES DE ADVERTENCIA DE UNA INTERNET ANTIDEMOCRÁTICA:

- Bloqueo o filtrado de contenido arbitrario, como el bloqueo de sitios web de medios de noticias específicos para que los ciudadanos no puedan acceder a la información relevante.
- Abuso de las leyes de difamación o propiedad intelectual para reprimir la expresión.
- Imposición de responsabilidad de intermediarios sin protecciones adecuadas de puerto seguro.
- Los organismos reguladores y el poder judicial solicitan que los intermediarios de Internet, como los proveedores de servicios de Internet (ISP), los proveedores de alojamiento web, los administradores de sitios web o las plataformas de redes sociales, eliminen el contenido sin justificación legal.
- Los actores políticos interrumpen el diálogo democrático al inundar los espacios en línea con desinformación, trolls, bots o lenguaje de acoso.
- La violencia en línea, ya sea perpetrada por individuos u organizaciones, hace que los ciudadanos políticamente activos se auto-censuren o se retiren completamente del debate público por temor a las repercusiones.

ESFUERZOS DE DEFENSA EXITOSOS PARA APOYAR ESTE PRINCIPIO:

En Filipinas, una ley de delitos informáticos introducida en 2012 propuso aumentar las sanciones por difamación y otorgar a las autoridades un poder sin control para rastrear información en línea. Los activistas por la libertad de Internet temían que varias disposiciones de la ley infrinjan la libertad de expresión al impedir que los filipinos publiquen contenido libremente en los sitios web y participen en foros y discusiones en línea sin temor a ser bloqueados

o enfrentar graves sanciones. En respuesta, organizaciones pro democracia de todo el espectro político se unieron para desafiar la constitucionalidad de la ley. A través de protestas, mesas redondas y actividades de desarrollo de capacidades, crearon conciencia y alentaron los esfuerzos de defensa en torno a los peligros que la ley implica para la libertad de expresión y la privacidad. La Foundation for Media Alternatives (FMA), una organización fundada luego de la caída de la dictadura de Marcos y la Alianza por la Libertad de Internet Filipina, se encontraban entre las organizaciones en el frente de lucha. PIFA fue incluso una de las 20 organizaciones que presentaron 15 peticiones al Tribunal Supremo sobre la constitucionalidad de la ley.

Los esfuerzos públicos en los tribunales y las acciones en las calles contribuyeron a la eliminación de tres disposiciones impugnadas de la ley, incluida una disposición que permitiría al gobierno bloquear o restringir el acceso a los datos informáticos. La Corte Suprema declaró estas disposiciones inconstitucionales y retrasó la aplicación de la ley. A pesar de la preocupación pública sobre las disposiciones vigentes, la campaña nacional contra la ley de delitos informáticos llevó a un punto de inflexión para los activistas filipinos; mostró el poder de las personas que se unen y luchan por la importancia de los derechos humanos en línea en Filipinas. Inicialmente fragmentada, la campaña condujo a un movimiento más amplio unificado bajo el objetivo de proteger los derechos humanos y la libertad de expresión en línea. Así, se tomó la introducción de una ley defectuosa y campañas públicas activas para iniciar un diálogo más amplio sobre la privacidad, la vigilancia y la seguridad digital. Activistas en el sudeste asiático se han inspirado en los esfuerzos de defensa filipinos, que han entendido como un ejemplo de cómo comunicar el equilibrio requerido entre las medidas contra el delito cibernético y los derechos fundamentales para una audiencia pública.

FUENTES SELECCIONADAS DE MARCOS INTERNACIONALES:

- United Nations Declaration of Human Rights, Article 19: "Declaración de Derechos Humanos de las Naciones Unidas, Artículo 19: "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión."¹
- Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos: "(1) Nadie podrá ser molestado a causa de sus opiniones; (2) Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección; (3) El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar

¹ <http://www.un.org/en/universal-declaration-human-rights/>

sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para: (a) Asegurar el respeto a los derechos o a la reputación de los demás, (b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas.”²

- La Resolución 32, 2016 del Consejo de Derechos Humanos de las Naciones Unidas: “Los mismos derechos que las personas tienen fuera de línea también deben protegerse en línea, en particular la libertad de expresión, que se aplica independientemente de las fronteras y de cualquier medio que elija.”

² <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>

2. LIBERTAD DE REUNIÓN Y ASOCIACIÓN

Todos deberían poder asociarse libremente con y a través de Internet para fines sociales, políticos, culturales u otros.

¿CÓMO SE VE ESTO EN UNA DEMOCRACIA?

Internet es una plataforma importante para la organización política donde los ciudadanos pueden colaborar para promover objetivos democráticos. Los ciudadanos pueden asociarse pacíficamente con otros en Internet. Internet ofrece un espacio abierto para que las personas puedan ejercer sus derechos democráticos y abogar por los derechos de los demás.

SEÑALES DE ADVERTENCIA DE UNA INTERNET ANTIDEMOCRÁTICA:

- Se impide a los ciudadanos acceder a sitios web y aplicaciones de mensajería que facilitan la movilización política.
- Los gobiernos presionan a los sitios web y las plataformas de medios sociales a eliminar la publicidad de un evento porque tiene el efecto de limitar la capacidad de los ciudadanos para programar una reunión pública u organizar una protesta.
- Agentes de seguridad se infiltran en las comunidades en línea para monitorear grupos.

ESFUERZOS DE DEFENSA EXITOSOS PARA APOYAR ESTE PRINCIPIO:

Los medios sociales son una importante herramienta de organización para periodistas y grupos de defensa en Uganda. Facebook, WhatsApp, y otras aplicaciones de mensajería se han utilizado para compartir³ conocimientos políticos, conectar líderes con partidarios y organizar eventos, incluso compartir información sobre abusos del gobierno. Durante las protestas nacionales "Caminando al trabajo"⁴ en 2011, organizadas para protestar por el costo de la vida después de las elecciones presidenciales, Facebook y Twitter brindaron un flujo constante de actualizaciones de manifestantes, espectadores y periodistas.

Sin embargo, el uso de las redes sociales puede tener consecuencias peligrosas para grupos marginados, como la comunidad LGBT. Se sabe que el gobierno de Uganda recopila información de usuarios y procesa a individuos basándose en información compartida en las redes sociales. Uganda es uno de los 76 países donde actualmente se criminaliza la homosexualidad, y los activistas LGBT

³ <https://books.google.com/books?id=2dmeBQAAQBAJ&pg=PA367>

⁴ https://en.wikipedia.org/wiki/Walk_to_work_protest

temen que sus conversaciones en línea sean monitoreadas y utilizadas en su contra. Al publicar información tomada de las fotos y el contenido publicado en Facebook, un tabloide local expuso la identidad de numerosos miembros de la comunidad LGBT en 2011 y nuevamente en 2014. Se cree que las historias de los tabloides en 2011 contribuyeron al asesinato de David Kato⁵, un destacado activista de los derechos de los homosexuales.

Además, el gobierno ha restringido repetidamente el acceso para que los grupos de defensa utilicen Internet para compartir información política. En 2016, el regulador de medios del país restringió el uso⁶ de WhatsApp, Facebook y Twitter para evitar la organización de protestas antes de las elecciones presidenciales de febrero, como lo había hecho el gobierno antes en 2011. En ambos casos, la comisión electoral impuso⁷ el cierre de las redes sociales.

Los grupos de la sociedad civil han respondido de dos maneras. Primero, han buscado profundizar su capacidad de seguridad digital. Para protegerse contra las amenazas a los periodistas, las organizaciones LGBT y otros grupos han aprendido cómo usar Facebook y las aplicaciones de redes sociales de forma más segura e implementar otras prácticas que aumentan su privacidad. En el período previo a la elección de 2016, esto incluía el uso de redes privadas virtuales (VPN) para compartir información. Los grupos de la sociedad civil difunden información sobre cómo usarlos a través de transmisiones de radio. El hecho de que el hashtag #UgandaDecides se mostrara en Twitter muestra cómo pudieron difundir sus conocimientos a través de redes locales y conectarse con los medios internacionales. En segundo lugar, los grupos de la sociedad civil formaron coaliciones con organizaciones internacionales para llamar la atención sobre los abusos que se cometen en Uganda. En 2016, Access Now apoyó a una coalición de grupos para exigir que el gobierno detenga el cierre de Internet como parte de la campaña #KeepitOn.

FUENTES SELECCIONADAS DE MARCOS INTERNACIONALES:

- El Artículo 20 de la Declaración de Derechos Humanos de las Naciones Unidas establece que “Toda persona tiene derecho a la libertad de reunión y de asociación pacíficas”
- Derechos Humanos del Consejo de Europa para los Usuarios de Internet, Asamblea, Asociación y Participación. ⁸“Usted tiene la libertad de elegir cualquier sitio web, aplicación u otro servicio para formar, unirse, moverse y participar en grupos sociales y asambleas, sean estas formalmente reconocidas o no por las autoridades públicas”
- Informe del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación. En el informe, el Relator Especial exhorta a los

⁵ <https://www.theguardian.com/world/2016/jan/26/uganda-lgbt-groups-david-kato-murder-5-years-on>

⁶ <http://www.bbc.com/news/world-africa-35601220>

⁷ <https://freedomhouse.org/report/freedom-net/2016/uganda>

⁸ <http://www.coe.int/en/web/internet-users-rights/assembly-association-and-participation>

Estados a "reconocer que los derechos a la libertad de reunión pacífica y de asociación pueden ejercerse a través de las nuevas tecnologías, incluso a través de Internet."

3. ACCESIBILIDAD

Todos deberían poder acceder y usar una Internet abierta y segura.

¿CÓMO SE VE ESTO EN UNA DEMOCRACIA?

Todos los miembros de la sociedad deberían tener la posibilidad de aprender, acceder y usar Internet. Para garantizar la igualdad de oportunidades para la participación, los principales actores de Internet, públicos y privados, identifican y abordan las desigualdades existentes en el acceso, en particular entre las mujeres y otras poblaciones marginadas.

SEÑALES DE ADVERTENCIA DE UNA INTERNET ANTIDEMOCRÁTICA:

- Los planes nacionales de banda ancha omiten o demoran sin razón el acceso a las comunidades rurales, lo que les deja con un ancho de banda bajo y/o alternativas de alto costo para el acceso en línea.
- Los altos costos prohíben el acceso a las comunidades más pobres.
- Falta de inversiones en infraestructura para banda ancha y acceso móvil en todo el país.
- El marco regulatorio para la competencia en el mercado, es a veces inexistente, etc.
- Un apagón de internet exigido por el gobierno en respuesta a las protestas políticas compromete la capacidad de ganancia y los ingresos de los empresarios locales que usan internet para hacer negocios.

ESFUERZOS DE DEFENSA EXITOSOS PARA APOYAR ESTE PRINCIPIO:

En Nigeria, los planes nacionales de banda ancha han pasado por alto a las comunidades rurales, dejándolos con un ancho de banda bajo y opciones de alto costo para el acceso a internet. Esto significa que las tarifas de banda ancha y datos móviles no son asequibles para muchos en Nigeria, especialmente para los pobres. Las suscripciones de banda ancha de línea fija cuestan un promedio del 39 por ciento del ingreso promedio, y los paquetes de banda ancha móvil cuestan el 13 por ciento. Dado que aproximadamente el 80 por ciento de los nigerianos ganan por debajo de la línea de pobreza (\$ 2 por día o menos), el acceso a Internet está fuera del alcance y es inaccesible para la mayoría de los ciudadanos en Nigeria.

La Alianza por una Internet asequible, una coalición global que trabaja en la asequibilidad de Internet, trabaja con los líderes de la sociedad civil nigeriana para crear conciencia sobre este tema a través de grupos de trabajo temáticos. El grupo de trabajo de defensa del consumidor y transparencia de precios, por ejemplo, trabaja en estrecha colaboración con una coalición de ONG

nigerianas⁹ que han liderado campañas para crear conciencia sobre las políticas de fijación de precios e impuestos que se han propuesto en Nigeria. Una política propuesta incluye la imposición de un impuesto del nueve por ciento sobre los servicios de voz, datos y SMS a los consumidores. Esta política haría que Internet sea dramáticamente más cara para los consumidores nigerianos. Los grupos manifiestan su preocupación por las consecuencias de la política propuesta en un entorno donde los agricultores se ven obligados a trepar a los árboles para obtener una conexión a Internet estable.

Los líderes de la sociedad civil que forman parte de la coalición han trabajado para construir un diálogo saludable entre los reguladores, la sociedad civil y el gobierno. Una estrategia clave, según los activistas, ha sido alentar a los grupos a encontrar formas constructivas de trabajar con el gobierno y aprovechar los intereses de cada uno de estos grupos para proteger y reducir los costos para los consumidores nigerianos. Buscan establecer relaciones con el regulador e informarles sobre las formas de comunicarse mejor y hacer participar a los grupos de consumidores, como por ejemplo, compartir su contenido a través de las redes sociales en lugar de comunicados de prensa. Otro aprendizaje importante ha sido identificar defensores dentro del gobierno para trabajar en estos temas.

FUENTES SELECCIONADAS DE MARCOS INTERNACIONALES:

- Derechos Humanos del Consejo de Europa para los Usuarios de Internet, Asamblea, Asociación y Participación.: "Su acceso debe ser asequible y no discriminatorio. Debe tener el mayor acceso posible al contenido de Internet, las aplicaciones y los servicios utilizando los dispositivos de su elección."¹⁰

⁹ <http://a4ai.org/a4ai-nigeria-multi-stakeholder-coalition/a4ai-nigeria-coalition-members/>

¹⁰ <http://www.coe.int/en/web/internet-users-rights/assembly-association-and-participation>

4. PRIVACIDAD Y PROTECCIÓN DE DATOS

Todos deberían tener derecho a la privacidad en línea. Las instituciones y entidades que poseen datos personales tienen la obligación de recopilar, retener, procesar, disponer y divulgar los mismos de manera responsable.

¿CÓMO SE VE ESTO EN UNA DEMOCRACIA?

Las medidas de seguridad y las restricciones en línea implementadas por los gobiernos u otras entidades deben ser consistentes con el derecho y las normas internacionales de derechos humanos. La privacidad y la protección de datos también incluyen la protección contra el pirateo no ético, la interceptación de datos y el robo de identidad. Los intermediarios de Internet garantizan la adopción de políticas y prácticas que protegen contra las solicitudes ilegales de datos personales por parte de entidades estatales o no estatales.

SEÑALES DE ADVERTENCIA DE UNA INTERNET ANTIDEMOCRÁTICA:

- Una autoridad gubernamental que exige que todas las computadoras vendidas en el país estén equipadas con software de filtrado o vigilancia.
- Organizaciones que recopilan datos personales de los consumidores no garantizan la confidencialidad y privacidad de dichos datos.
- Se requiere que los ciudadanos registren los nombres de usuario de sus cuentas de redes sociales con el gobierno para que puedan así rastrear y castigar fácilmente a aquellos que hacen declaraciones contra el gobierno.
- Los gobiernos penalizan el cifrado evitando que los ciudadanos se comuniquen entre sí de manera segura; que los periodistas que se comuniquen con las fuentes, y otros.
- El gobierno realiza un rastreo de todas las actividades y transacciones de individuos que utilizan metadatos analíticos de la tarjeta de identidad de un ciudadano.
- Seguridad y fuerzas policiales requieren acceso al uso individual de Internet al tomar el teléfono de una persona.

ESFUERZOS DE DEFENSA EXITOSOS PARA APOYAR ESTE PRINCIPIO:

En Birmania, las brechas en la ley han dejado vulnerables a los ciudadanos cuando se trata de privacidad y protección de datos. Las restricciones a la privacidad han disminuido desde la transición del país del gobierno militar, pero la falta de leyes de protección de datos y la falta general de conciencia sobre la privacidad y la protección de datos presentan desafíos importantes para proteger una Internet abierta. Las aplicaciones de mensajería como Viber y Facebook Messenger, por ejemplo, son la herramienta de facto para la

comunicación para activistas y se utilizan para organizar eventos y actividades políticas. Más baratas que las llamadas de voz, mucho más accesibles que las líneas fijas y más fáciles de usar que el correo electrónico, estas herramientas son la principal forma de comunicación de las personas en Birmania. Los activistas han recibido severas sanciones por compartir contenido que pueden verse como una amenaza para la seguridad del estado¹¹. Estas aplicaciones a menudo no son seguras, lo que hace posible que las autoridades del estado de Birmania o los agentes del estado puedan interceptar sus conversaciones. Durante una represión contra las protestas estudiantiles en marzo de 2015, los teléfonos móviles fueron tomados por la policía¹². En ese momento, era preocupante para los activistas, que la información de estos teléfonos fuera utilizada en su contra.

Al observar la necesidad de proteger a los activistas y educarlos sobre la protección de datos, los activistas en 2016 formaron una coalición, Digital Rights MM. La coalición, liderada por Phandeeay, Centro de Negocios Responsables de Myanmar, ICT para el Desarrollo de Myanmar y Free Expression Myanmar, ha liderado una conversación nacional sobre el tema. Basándose en la experiencia de la región y las organizaciones internacionales¹³, 22 organizaciones locales con base en Birmania han tenido éxito en señalar las brechas en lo que respecta a la privacidad y la libertad de expresión en la ley nacional de telecomunicaciones¹⁴, una ley integral que supervisa el desarrollo del sector de las telecomunicaciones en Birmania. También participaron en reuniones con el gobierno y lanzaron una campaña pública #ourvoicourhluuttaw¹⁵ presionando para enmendar 23 artículos, incluyendo uno sobre la interceptación legal de datos.

FUENTES SELECCIONADAS DE MARCOS INTERNACIONALES:

- Asamblea General de las Naciones Unidas, Resolución 69/166, Derecho a la Privacidad en la era Digital 2014
- Estándares para una Internet Libre, Abierta e Inclusiva, Despacho de Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, 2017
 - » *Párrafo 231*: "Las medidas para restringir el cifrado reducen la capacidad de las personas para protegerse de las invasiones ilegales a su privacidad."
 - » *Párrafo 228*: "Los Estados tienen la obligación de respetar el discurso anónimo como un ejercicio de privacidad y libertad de expresión y solo pueden exigir excepcionalmente la autenticación o prueba de

¹¹ <https://www.fastcompany.com/40438242/jailed-for-a-facebook-poem-the-fight-against-myanmars-draconian-defamation-law>

¹² https://pen.org/sites/default/files/unfinished_freedom_lowres.pdf

¹³ <https://www.forbes.com/sites/chynes/2016/12/21/digital-rights-must-become-a-top-priority-in-myanmars-connectivity-revolution/#4fde153b2267>

¹⁴ <https://www.article19.org/resources.php/resource/38665/en/myanmar-telecommunications-law>

¹⁵ <https://www.facebook.com/MMTelecomLaw/photos/a.821155664669495.1073741830.821091201342608/1347827635335626/?type=3&theater>

- identidad de la persona que lo expresa, aplicando un estándar de proporcionalidad.”
- » *Párrafo 227:* “Los espacios anónimos que están libres de observación y donde las identidades y actividades no están documentadas, deben ser garantizados.”
 - » *Párrafo 212:* “La vigilancia de Internet en cualquiera de sus formas o matices constituye una interferencia en la vida privada de las personas y, cuando se realiza ilegalmente, también puede afectar los derechos al debido proceso y un juicio justo, la libertad de expresión y el acceso a la información. Se reconoce tanto a nivel regional como universal que la vigilancia, la interceptación y la recopilación de datos personales ilegales o arbitrarias no solo afectan el derecho a la privacidad y la libertad de expresión, sino que también pueden ir en contra de los preceptos de una sociedad democrática.”
 - » *Párrafo 204:* “Para proteger la privacidad en Internet, se debe garantizar la confidencialidad de los datos personales en línea.”

5. PROTECCIÓN PERSONAL Y SEGURIDAD

La protección personal y seguridad deben ser respetadas, protegidas y cumplidas en línea.

¿CÓMO SE VE ESTO EN UNA DEMOCRACIA?

Se han establecido protecciones legales que abordan amenazas de violencia física, sexual y psicológica o acoso en línea. Además, existen protecciones contra la desinformación en línea o campañas de arrastre que incitan a la violencia, la discriminación u hostilidad contra individuos o grupos.

SEÑALES DE ADVERTENCIA DE UNA INTERNET ANTIDEMOCRÁTICA:

- Informes crecientes de mujeres políticamente activas sobre acoso, piratería y chantaje en línea generados en espacios en línea y que tienen un efecto de puerta de entrada a la confrontación personal y física.

ESFUERZOS DE DEFENSA EXITOSOS PARA APOYAR ESTE PRINCIPIO:

En Pakistán, las mujeres enfrentan amenazas de acoso físico, sexual y psicológico en línea. Fugas de fotos explícitas y amenazas de chantaje son cada vez más comunes. De 2014 a 2015, más de 3,000 delitos cibernéticos fueron reportados a la Agencia Federal de Investigación y de esos casos, casi la mitad fueron dirigidos a mujeres en las redes sociales.¹⁶ Los observadores estiman que muchos más casos no son reportados. De hecho, en los talleres realizados por la Fundación de Derechos Digitales, muchas estudiantes universitarias informaron que no sabían que el acoso cibernético era un delito.

Las plataformas en línea son un espacio importante para el compromiso político, la expresión y la movilización en Pakistán. Por lo tanto, el acoso en línea afecta directamente la participación política de las mujeres, incluidas las periodistas y las mujeres políticas. En 2016, la Fundación de Derechos Digitales estableció una Línea de Ayuda contra el Acoso Cibernético¹⁷ a la que las mujeres pueden acudir en busca de ayuda cuando son acosadas en Internet. Uno de los principales objetivos de la línea de ayuda es ayudar a reducir el déficit de confianza entre los sobrevivientes y los organismos encargados de hacer cumplir la ley. Un análisis de más de 400 casos¹⁸ mostró que las barreras más comunes

¹⁶ <https://digitalrightsfoundation.pk/drpcwstraining/>

¹⁹ <https://digitalrightsfoundation.pk/cyber-harassment-helpline-completes-its-four-months-of-operations/>

¹⁸ http://digitalrightsfoundation.pk/wp-content/uploads/2017/04/4-Month-Report.Final_.pdf

para la participación igualitaria son el uso no consentido de la información, la suplantación de identidad, el pirateo de cuentas, el envío de correos electrónicos en negro y la recepción de mensajes no solicitados; los grupos más específicos incluyen mujeres, niños, defensores de derechos humanos y comunidades minoritarias. La Fundación de Derechos Digitales también ha liderado los esfuerzos para fortalecer las protecciones legales para las mujeres y responder a las sobrevivientes mediante recomendaciones a las agencias policiales y al gobierno. Pakistán tiene un Centro Nacional de Respuesta para la Ciber-delincuencia, pero ha enfrentado desafíos en el servicio para las mujeres fuera de las principales ciudades.

FUENTES SELECCIONADAS DE MARCOS INTERNACIONALES:

- Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, párrafo 81: “Los Estados tienen la obligación de proteger a los individuos contra la interferencia de terceros que socavan el disfrute del derecho a la libertad de opinión y expresión.”

6. INCLUSIÓN

Se debe promover la diversidad cultural y lingüística en Internet, y se debe alentar la innovación técnica y de políticas para facilitar la pluralidad de expresión.

¿CÓMO SE VE ESTO EN UNA DEMOCRACIA?

Internet está diseñado y mantenido de una manera que promueve la inclusión de todas las personas, como las mujeres, personas con discapacidad y otros grupos marginados. El contenido de Internet se crea con el objetivo de promover la diversidad y la participación democrática. Esto incluye la diversidad lingüística y adhiere a los estándares de accesibilidad, para que todas las personas puedan comunicarse, compartir información o crear contenido en línea en el idioma de su elección.

SEÑALES DE ADVERTENCIA DE UNA INTERNET ANTIDEMOCRÁTICA:

- Los sitios web oficiales no se adhieren a las mejores prácticas ni a los requisitos legales para los estándares de accesibilidad, lo que impide que las personas con discapacidades interactúen o utilicen un sitio.
- Los gobiernos que publican información en línea habitualmente excluyen las traducciones de los miembros de la población que no hablan el idioma primario.
- El espacio en línea se cierra a la participación de mujeres y personas marginadas.

ESFUERZOS DE DEFENSA EXITOSOS PARA APOYAR ESTE PRINCIPIO:

En la India, la población de personas con discapacidades se estima en 150 millones de personas, y las tasas registradas de personas con discapacidad visual se encuentran entre las más altas del mundo. Grupos de activismo en India, como el Centro para Internet y la Sociedad (CIS), han trabajado para garantizar que estas personas puedan participar plenamente en línea mediante la promoción de políticas que prioricen la accesibilidad. Estas incluyen la Política Nacional sobre Accesibilidad Universal a los Electrónicos, la Ley de Derechos de las Personas con Discapacidad y las Pautas para el Gobierno de la India (GIGW), que requieren que la información gubernamental se comparta en formatos accesibles. Sin embargo, los grupos de defensa han demostrado con éxito que las políticas por sí solas no son suficientes y han tomado medidas para garantizar que las personas con discapacidades tengan acceso a información y recursos críticos en línea.

Los teléfonos móviles, en particular, son un portal vital para acceder a los servicios gubernamentales, pero las aplicaciones móviles siguen siendo en gran

parte inaccesibles para muchas personas con discapacidades, especialmente aquellas con discapacidades visuales. Por ejemplo, CIS observó en 2015 que MyGov, la plataforma móvil de participación ciudadana del Gobierno de la India y la aplicación del Primer Ministro eran altamente inaccesibles: las pantallas no pueden ser navegadas por usuarios con discapacidades visuales y tampoco pueden leerse con un lector de pantalla. Sobre esta base, CIS y otras organizaciones de defensa trabajaron en la elaboración de pautas de accesibilidad para aplicaciones móviles recomendadas como estándar para el Gobierno de la India. Los grupos de defensa, como el Centro Nacional para la Promoción del Empleo para Personas Discapacitadas (NCPEDP), también han estado apelando al sector privado para garantizar que los productos diseñados para atender estas necesidades sean asequibles y estén disponibles para las personas con discapacidades. Hacen un llamamiento a las empresas y responsables políticos de la India defendiendo el atractivo universal de la tecnología de asistencia para garantizar que las comunidades con discapacidades no sean dejadas de lado.

La defensa sostenida, los nuevos mandatos legales aplicados a los sectores público y privado y el aumento de la investigación en este dominio han ayudado a avanzar en el tema de la accesibilidad de las aplicaciones móviles. El Centro Nacional de Informática del país ha establecido un comité para revisar el GIGW y ponerlo al día con los estándares internacionales.

FUENTES SELECCIONADAS DE MARCOS INTERNACIONALES:

- Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, párrafo 87: “Cuando la infraestructura para el acceso a internet está presente, el Relator Especial alienta a los Estados a apoyar iniciativas para garantizar que se pueda acceder a la información en línea de una manera significativa por todos los sectores de la población, incluidas las personas con discapacidad y las personas pertenecientes a minorías lingüísticas”.
- Estándares para una Internet libre, abierta e inclusiva, Despacho del Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, 2017¹⁹ “Los estados deben tomar medidas diseñadas para reducir los obstáculos lingüísticos a fin de que la alfabetización sea viable y garantizar el acceso de todas las personas en igualdad de condiciones. También deben “promover contenidos de origen local e indígena en Internet.”

¹⁹ http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf

7. IGUALDAD EN LA RED

Todos deben tener acceso universal y abierto al contenido de Internet, libre de priorización discriminatoria, filtrado o control del tráfico por motivos comerciales, políticos u otros.

CÓMO SE VE ESTO EN UNA DEMOCRACIA?

Todos los ciudadanos tienen acceso igualitario al contenido públicamente disponible en Internet. Los sitios y servicios a los que los ciudadanos pueden acceder no son discriminados por su contenido político. No se permite el cierre o la limitación del acceso a Internet por ningún motivo, incluido el orden público o los motivos de seguridad nacional.

SEÑALES DE ADVERTENCIA DE UNA INTERNET ANTIDEMOCRÁTICA:

- Acelerar el contenido específico a cambio de consideraciones comerciales.
- Un apagón de internet que corta el acceso a un país, región, ciudad o vecindario determinado.
- La limitación del servicio de Internet durante las elecciones u otro evento político (por ejemplo, protestas) para que las imágenes o los videos no puedan ser circulados por los ciudadanos.
- Un ciudadano en un país no puede acceder a sitios web que están ampliamente disponibles en otros países debido a la censura y regulación del gobierno local.

ESFUERZOS DE DEFENSA EXITOSOS PARA APOYAR ESTE PRINCIPIO:

A principios de 2017, el cierre de Internet en Camerún negó el acceso en línea a una parte importante de la población del país²⁰. El cierre se produjo en la región anglófona del país, un área históricamente marginada por la mayoría francófona. En el período previo al apagón de internet, el gobierno de Camerún advirtió públicamente a los usuarios de internet que habría sanciones penales por cualquier acción para difundir noticias falsas en las redes sociales en la región anglófona. A pesar de la afirmación del gobierno de que esta acción evitaría la difusión de información falsa, la mayoría de los observadores sostuvieron que el gobierno pretendía frenar las protestas recientes limitando las conexiones a las aplicaciones de mensajería de las redes sociales y otras plataformas de comunicación en línea. Los activistas creen que el gobierno era muy consciente del papel fundamental que jugaba Internet en la organización de las protestas.

Grupos de activistas que no se vieron afectados por el cierre lanzaron una

²⁰ <http://www.bbc.com/news/world-africa-39665244>

campaña global de medios sociales, #bringbackourinternet, para crear conciencia sobre el cierre. Apuntaron a liderar los esfuerzos para aplicar presión local, panafricana e internacional sobre el gobierno. También comprometieron directamente a Camtel, la compañía nacional de telecomunicaciones del país. Finalmente, las nuevas empresas crearon un "campamento de refugiados en Internet"²¹ donde los miembros trajeron módems de Internet portátiles para que otros los usaran en lugar de conducir hasta la siguiente ciudad más grande, Douala, para usar Internet. A través de estos esfuerzos, la tecnología camerunesa y las comunidades activistas crearon conciencia global sobre el cierre, aplicando presión sobre el gobierno.

FUENTES SELECCIONADAS DE MARCOS INTERNACIONALES:

- Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, párrafo 79: "El Relator Especial insta a todos los Estados a garantizar que se mantenga el acceso a Internet en todo momento, incluso en momentos de inestabilidad política."²²

²¹ <https://qz.com/942879/an-internet-shutdown-in-cameroon-has-forced-startups-to-create-an-internet-refugee-camp-in-bonako-village/>

²² http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/17/27

8. ESTÁNDARES

La arquitectura de Internet, los sistemas de comunicación y los formatos de documentos y datos se basarán en estándares abiertos que garanticen la interoperabilidad completa, la inclusión y la igualdad de oportunidades para todos.

¿CÓMO SE VE ESTO EN UNA DEMOCRACIA?

Los estándares/formatos de Internet deben estar abiertos con pocas o ninguna barrera de acceso para garantizar que los usuarios, los hosts de contenido y los proveedores de servicios puedan intercambiar información libremente. Las normas técnicas no se utilizan como una forma de lograr la censura o la vigilancia.

SEÑALES DE ADVERTENCIA DE UNA INTERNET ANTIDEMOCRÁTICA:

- Se desarrolla un estándar técnico con la expresa intención de posibilitar el seguimiento o la vigilancia de usuarios individuales de Internet..
- Un gobierno se niega a adoptar estándares internacionales de internet limitando efectivamente el acceso de los ciudadanos a internet global.

ESFUERZOS DE DEFENSA EXITOSOS PARA APOYAR ESTE PRINCIPIO:

Comunicarse de forma segura y en línea es un desafío para los activistas de la democracia y los periodistas de todo el mundo. En los últimos diez años, los grupos de defensa mundial Centro para la Democracia y la Tecnología (CDT) y la Fundación Frontera Electrónica (EFF) han pedido a los propietarios de sitios web que apoyen el protocolo HTTPS o el Protocolo de transferencia de hipertexto con una S adicional para "seguro".

El uso de un sitio HTTPS ayuda a garantizar que los usuarios se conecten a los sitios a los que pretenden y que el contenido transferido entre el servidor del sitio web y el navegador del usuario sea menos susceptible a la vigilancia o interferencia. La capa adicional de seguridad hace que sea menos probable que los agentes gubernamentales, proveedores de servicios de Internet o piratas informáticos vigilen a los usuarios en línea. Sin HTTPS, un agente podría reemplazar las noticias o las entradas de Wikipedia con contenido alternativo, rastrear los hábitos de los lectores e incluso interceptar contraseñas.

Desde que se lanzó el protocolo HTTPS original en 1995, se ha convertido en un estándar de la industria para ofrecer cifrado y autenticación de contenido en Internet. En 2010, Google modificó su motor de búsqueda para que los

navegadores enviaran consultas de búsqueda a través de HTTPS,²³ y más tarde Wikipedia y Facebook también adoptaron HTTPS, por defecto.²⁴ Las organizaciones de medios como la BBC, Washington Post y The New York Times también han migrado a HTTPS. Hoy en día, el volumen promedio de tráfico cifrado supera el tráfico no cifrado.²⁵

A pesar de una mayor conciencia, hay más por hacer, dice la Fundación Libertad de Prensa, señalando que varios sitios de noticias internacionales importantes aún no han migrado sus sitios a HTTPS, incluyendo Al Jazeera, El Mundo (España), Francia 24 (Francia), Agencia de Noticias Xinhua (China) y The Hindu (India). A través de campañas de promoción global, CDT y EFF también han educado a los actores de la industria sobre los beneficios de HTTPS. Las herramientas de migración como Let's Encrypt, un servicio desarrollado por Internet Security Research Group, y el complemento del navegador EFF, HTTPS://everywhere, satisfacen las necesidades de los propietarios y usuarios de sitios más pequeños. Es importante destacar que estos grupos consideran que las estrategias de promoción segmentadas para los grupos de partes interesadas, incluidos los mensajes personalizados, son una estrategia importante para fomentar el conocimiento y la acción.

FUENTES SELECCIONADAS DE MARCOS INTERNACIONALES:

- Standards for a Free, Open and Inclusive Internet, Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 2017 - Paragraph 231: "Measures to restrict encryption reduce people's ability to protect themselves from illegal invasions of their privacy. The measures include... the imposition of centralized key registries or the creation of back doors to enable collection of communication even from encrypted devices."²⁶
- OECD Council Recommendation on Principles for Internet Policy Making. December 2013. "The internet allows people to give voice to their democratic aspirations and that any policy-making associated with it must promote openness and be grounded in respect for human rights and the rule of law"²⁷

²³ <https://web.archive.org/web/20100526165218/http://www.h-online.com:80/security/news/item/Google-secures-search-with-SSL-encryption-1006020.html>

²⁴ <https://www.facebook.com/notes/facebook-engineering/secure-browsing-by-default/10151590414803920/>

²⁵ <https://www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer/>

²⁶ http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf

²⁷ <http://www.oecd.org/sti/ieconomy/49258588.pdf>

9. GOBERNANZA

Los derechos humanos y la justicia social deben formar los fundamentos legales y normativos sobre los cuales opera y se gobierna Internet. Esto sucederá de manera transparente y multilateral, basado en los principios de apertura, participación inclusiva y responsabilidad.

¿CÓMO SE VE ESTO EN UNA DEMOCRACIA?

Las partes interesadas involucradas en la gobernanza de Internet representan un sector de organizaciones intersectoriales, como gobiernos, grupos de la sociedad civil, representantes del sector privado, instituciones académicas y medios de comunicación a fin de ser verdaderamente democráticos y pluralistas. La diversidad es esencial para asegurar que la gobernanza de internet sea inclusiva y representativa.

SEÑALES DE ADVERTENCIA DE UNA INTERNET ANTIDEMOCRÁTICA:

- Los órganos de gobierno de Internet incluyen sólo representantes gubernamentales y designados por el gobierno.
- Las conferencias y foros de gobernanza de Internet, ya sea directa o indirectamente, excluyen la participación de representantes de Sur Global.
- Solo compañías multinacionales de tecnología y telecomunicaciones están presentes, excluyendo a otras grandes porciones del sector privado, como empresarios o asociaciones de pequeñas empresas.

ESFUERZOS DE DEFENSA EXITOSOS PARA APOYAR ESTE PRINCIPIO:

En Nepal, el capítulo nacional de la Internet Society ha liderado los esfuerzos para crear una estructura de gobierno nacional de múltiples partes interesadas que incluya al gobierno, la sociedad civil y el sector privado mediante la organización de un Foro Nacional de Gobernanza de Internet. Al hacerlo, han procurado garantizar que las decisiones sobre la política de Internet incluyan la participación de todos los interesados afectados.

En 2009, Shreedeeep Rayamajhi y un grupo de activistas lanzaron el capítulo de Internet Society en Nepal. Después de asistir a los Foros de Gobernanza de Internet (IGF), una conferencia sobre políticas de múltiples partes interesadas organizada bajo los auspicios de las Naciones Unidas, los activistas decidieron planificar su propio IGF en Nepal. Esto tuvo lugar en el contexto en el que creció el abuso de los derechos de los ciudadanos en línea y aumentó la conciencia sobre la falta de leyes y regulaciones específicas para protegerlos. Hubo un sentimiento creciente entre los grupos de la sociedad civil de que era necesario desarrollar una nueva plataforma para discutir estos temas.

A través de la reunión de IGF Nepal y el trabajo del capítulo de la Internet Society de Nepal, estos activistas pueden proporcionar plataformas a las personas, especialmente a los jóvenes, para discutir su visión y estrategias para fomentar una Internet más abierta y segura en Nepal y compartir estas ideas con los hacedores de políticas mundiales. Es importante destacar que lo ven como el comienzo de un esfuerzo mayor para desarrollar un mecanismo que involucre a la comunidad nacional e internacional de formulación de políticas, que aún tiene un nivel de comprensión en desarrollo en torno a cómo se entienden y se implementan los problemas de gobernanza de Internet en el Sur Global.

FUENTES SELECCIONADAS DE MARCOS INTERNACIONALES:

- Declaración de Principios de la WSIS. 12 de diciembre de 2003. Artículo 20. “Los gobiernos, el sector privado, la sociedad civil y las Naciones Unidas y otras organizaciones internacionales tienen un papel y una responsabilidad importantes en el desarrollo de la Sociedad de la Información y, según corresponda, en los procesos de toma de decisiones. Construir una Sociedad de la Información centrada en las personas es un esfuerzo conjunto que requiere la cooperación y la asociación entre todas las partes interesadas.”²⁸
- Recomendación del Consejo de la OCDE sobre los Principios para la formulación de políticas de Internet. 13 de diciembre de 2011.²⁹

²⁸ <http://www.itu.int/net/osis/docs/geneva/official/dop.html>

²⁹ <http://www.oecd.org/sti/ieconomy/49258588.pdf>

[HTTPS://OPENINTERNET.GLOBAL](https://openinternet.global)



**National Endowment
for Democracy**

Supporting freedom around the world