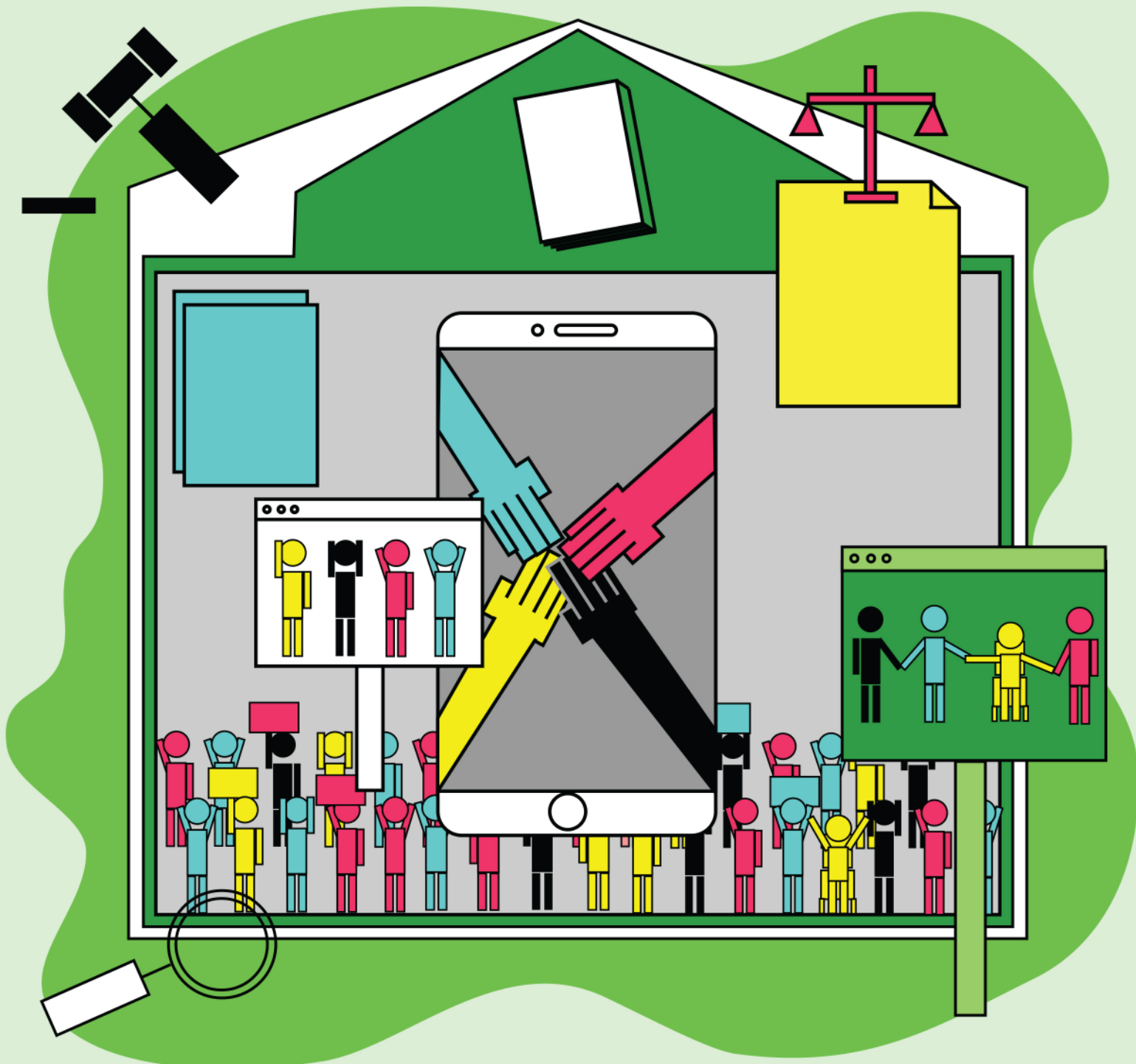


Defensa de la libertad de reunión pacífica y asociación en la era digital:

bajas de contenido, apagones de Internet y vigilancia





Defensa de la libertad de reunión pacífica y asociación en la era digital: bajas de contenido, apagones de Internet y vigilancia

Publicado en inglés en julio de 2020. Edición en español, octubre 2020

Esta es una publicación de Access Now. Fue escrita por Laura O'Brien y Peter Micek. Los autores desean agradecer a los miembros del equipo de Access Now que colaboraron con el informe, incluidos Javier Pallero, Alexia Skok, Berhan Taye, Carolyn Tackett, Daniel Leufer, Donna Wentworth, Eliška Pírková, Elizabeth Metts, Eric Null, Estelle Massé, Fanny Hidvégi, Isedua Oribhabor, Juliana Castro, Marwa Fatafta, Natalia Krapvia, Raman Jit Singh Chima, Sage Cheng y Verónica Arroyo, así como a nuestros pasantes de políticas públicas y asuntos legales Alanna Fichtel, Carolina Gonçalves Berenger y Emilia Porubcin.

Es importante tener en cuenta que, si bien este artículo se basa en ejemplos de distintas regiones del mundo, los casos mencionados no son exhaustivos y no representan las experiencias de todos aquellos que intentan hacer uso de sus derechos a la libertad de reunión pacífica y asociación en todo el mundo. Reconocemos que se requieren más investigaciones y datos para considerar todas las estructuras de opresión involucradas, incluidas, entre otras, aquellas basadas en la raza, el género,¹ el origen étnico, la orientación sexual, las discapacidades, las clases sociales, el idioma, la religión, la edad, la ciudadanía y el estado familiar.²

¹ Con especial atención a las situaciones de las personas transgénero, con identidades de género no binarias y con identidades de género no convencionales.

² Ver, p. ej., esfuerzos como Initiative for a Representative First Amendment (Iniciativa para lograr una primera Enmienda Representativa), en <https://www.ifrfa.org>, Equality Labs, en <https://www.equalitylabs.org> y la Liga de Justicia Algorítmica, en <https://www.ajl.org>.

ÍNDICE

ÍNDICE	2
I. RESUMEN EJECUTIVO	3
II. INTRODUCCIÓN	6
DERECHO A LA LIBERTAD DE REUNIÓN PACÍFICA	9
DERECHO A LA LIBERTAD DE ASOCIACIÓN	12
DERECHOS A LA LIBERTAD DE REUNIÓN PACÍFICA Y ASOCIACIÓN EN LÍNEA	13
RESTRICCIONES ACEPTABLES CONFORME A LA LEY INTERNACIONAL DE DERECHOS HUMANOS	14
III. ACCESO, CONECTIVIDAD Y APAGONES DE INTERNET	15
CASOS PRÁCTICOS	20
Ecuador	21
Etiopía	22
India	23
Irak	24
Sudán	24
Togo	25
IV. VIGILANCIA Y DERECHO A LA PRIVACIDAD	26
CASOS PRÁCTICOS	32
Azerbaiyán	32
Brasil	33
Francia	34
Hong Kong	34
India	35
Rusia	36
Estados	37
Unidos	37
V. LA INFLUENCIA DEL SECTOR PRIVADO EN EL ESPACIO CÍVICO EN LÍNEA	38
CAMPAÑA #SAVEDOTORG	39
INFORMES DE TRANSPARENCIA	40

REGULACIÓN DEL DISCURSO	41
CASOS PRÁCTICOS	44
Activision Blizzard	44
<i>Hong Kong</i>	44
Whole Foods (Amazon)	44
<i>Estados Unidos</i>	44
Twitter	45
<i>Egipto</i>	45
VI. RECOMENDACIONES PARA LAS POLÍTICAS PÚBLICAS	46
RECOMENDACIONES PARA LOS ESTADOS	46
RECOMENDACIONES PARA EL SECTOR PRIVADO	48
RECOMENDACIONES PARA LAS INSTITUCIONES INTERNACIONALES	49
VII. CONCLUSIÓN	51

I. RESUMEN EJECUTIVO

Este año, 2020, ha revitalizado las discusiones nacionales e internacionales respecto de los derechos a la libertad de reunión pacífica y asociación. Algunos ejemplos de estas discusiones incluyen las secuelas de la muerte de George Floyd. Tras este hecho clave, multitudes globales se manifestaron y obligaron al mundo a mirarse al espejo y terminar con las estructuras sistémicas de injusticia racial. Otro ejemplo son los distintos movimientos liderados por jóvenes de Hong Kong a Sudán que opusieron resistencia frente a la represión.

Debido a las medidas de distanciamiento social implementadas para combatir el COVID-19, distintas asociaciones y grupos de reunión tuvieron que aplicar su creatividad para rediseñar sus estrategias, equiparse y empoderarse a fin de tener presencia tanto en el entorno físico como el digital durante la pandemia.³ Desde protestas en automóviles y bicicletas⁴ hasta aplausos, bailes y vítores desde ventanas y balcones para alentar a los trabajadores esenciales,⁵ las asociaciones y las reuniones físicas han adoptado formas únicas para lograr participaciones cívicas significativas. Del mismo modo, el COVID-19 demostró la importancia de las tecnologías digitales, específicamente, de Internet y las tecnologías de información y comunicación (TIC), para el ejercicio de la libertad de reunión pacífica y asociación en línea.⁶ En plena pandemia del COVID-19, la activista medioambiental Greta Thunberg, por ejemplo, motivó a los activistas jóvenes (que crecieron en línea) para que utilizaran las herramientas digitales que tanto conocen a fin de participar en una "manifestación digital" en lugar de realizar reuniones públicas físicas y, así, sostener la presión pública hacia los gobiernos en cuanto a la lucha contra el cambio climático.⁷ En general, la pandemia del COVID-19 volvió a enfatizar el hecho de que las asociaciones y las reuniones físicas ya no son el *único* medio de conexión disponible. En cambio, podemos reunirnos y conectarnos en línea (y atravesar las fronteras físicas) para expresar

³ Anthony Faiola, "Coronavirus chills protests from Chile to Hong Kong to Iraq, forcing activists to innovate", *The Washington Post*, 4 de abril de 2020, https://www.washingtonpost.com/world/the_americas/coronavirus-protest-chile-hong-kong-iraq-lebanon-india-venezuela/2020/04/03/c7f5e012-6d50-11ea-a156-0048b62cdb51_story.html

⁴ Samantha Melamed, "Protesting in the time of social distancing: Philly demands action by car, bike, text, and tweet", *The Philadelphia Inquirer*, 30 de marzo de 2020, <https://www.inquirer.com/health/coronavirus/protest-philadelphia-jails-social-distancing-coronavirus-covid-19-20200330.html>

⁵ Amanda Hess, "In Praise of Quarantine Clapping", *The New York Times*, 9 de abril de 2020, <https://www.nytimes.com/2020/04/09/arts/virus-quarantine-clapping.html>

⁶ Laurie Goering, "As coronavirus drives climate protests off streets, activists go online", *Reuters*, 20 de marzo de 2020, <https://www.reuters.com/article/us-health-coronavirus-climate-change/as-coronavirus-drives-climate-protests-off-streets-activists-go-online-idUSKBN2170MM>

⁷ Zack Colman, "Climate activists shift gears in an age of 'social distancing'", *POLITICO*, 19 de marzo de 2020, <https://www.politico.com/news/2020/03/19/climate-activists-social-distancing-coronavirus-137216>; Zoey Shipley, "Using Social Media as the Platform for Protesting in an Age of Social Distancing", *Our Daily Planet*, 22 de marzo de 2020, <https://www.ourdailyplanet.com/story/using-social-media-as-the-platform-for-protesting-in-an-age-of-social-distancing/>

nuestras opiniones, generar acciones, mostrar solidaridad y acceder a información importante y vital en estos tiempos sin precedentes.

Internet y las TIC ayudan a que se respeten los derechos humanos.⁸ En 2011, el Relator Especial de la ONU sobre libertad de expresión destacó que "Internet es una de las herramientas más poderosas del siglo XXI para incrementar la transparencia respecto de la conducta de los poderosos, mejorar el acceso a la información y facilitar la participación activa de los ciudadanos en el desarrollo de sociedades democráticas".⁹ Pensemos, por ejemplo, en las revoluciones de la Primavera Árabe en Oriente Medio y Norte de África, entre 2010 y 2012. Durante este período, diversos activistas inspiraron al mundo al crear vínculos entre las acciones en los entornos físico y digital y redefinieron el espacio cívico en línea como un entorno en el que los individuos y grupos pueden expresar sus preocupaciones, compartir información y organizar acciones colectivas.¹⁰ Por consiguiente, los estados deben brindar acceso universal, asequible, abierto, seguro y estable a Internet y las TIC a fin de permitir a las personas hacer un uso pleno de sus derechos humanos, como los derechos a la reunión pacífica y la asociación.

No obstante, el cierre del espacio cívico en línea ha afectado los derechos a la libertad de reunión pacífica y asociación tanto en el entorno digital como el físico. Las plataformas y herramientas antes descentralizadas y abiertas se volvieron restringidas, lo que significa que tanto los individuos como las comunidades ahora se ven afectados por factores como la privatización (p. ej., fines de lucro, tendencias monopólicas y políticas discriminatorias sin rectificación o revisión), la censura, el acoso, la vigilancia y la persecución, que impiden el uso de las TIC como herramienta de protesta y asociación en línea. Por ejemplo, en el último año, fuimos testigos del predominio de la vigilancia hacia los activistas de *Black Lives Matter* en Estados Unidos, el apagón de Internet que acompañó las estrictas medidas en contra de manifestantes pacíficos en Sudán y la propuesta de venta del dominio .ORG.

Las leyes nacionales e internacionales reconocen que las circunstancias extraordinarias requieren medidas extraordinarias. Esto significa que algunos derechos fundamentales, como los derechos a la libertad de reunión pacífica y asociación, pueden ser restringidos (p. ej., en pos del orden público, la seguridad pública, intereses de seguridad nacional o la protección de principios morales o la salud pública, lo cual se intensifica durante la pandemia del COVID-19) siempre que

⁸ Consejo de Derechos Humanos de las Naciones Unidas, *Informe del Relator Especial sobre la promoción y protección de los derechos a la libertad de opinión y expresión*, Frank La Rue, doc. de la ONU A/HRC/17/27 (16 de mayo de 2011). <https://undocs.org/en/A/HRC/17/27>, párr. 22-23.

⁹ *Ibid.*, párr. 2; Consejo de Derechos Humanos de las Naciones Unidas, *Informe del Relator Especial sobre el derecho a la libertad de reunión y asociación pacíficas*, Maina Kiai, doc. de la ONU A/HRC/20/27 (21 de mayo de 2012). <https://undocs.org/A/HRC/20/27>, párr. 84 (k). Ver también: Consejo de Derechos Humanos de las Naciones Unidas, *Informe del Relator Especial sobre la protección y promoción del derecho a la libertad de opinión y expresión*, David Kaye, doc. de la ONU A/HRC/32/38 (11 de mayo de 2016) <https://undocs.org/A/HRC/32/38>, párr. 8.

¹⁰ Access Now. *Five years later: the internet shutdown that rocked Egypt*, 2016. <https://www.accessnow.org/five-years-later-the-internet-shutdown-that-rocked-egypt/>

se apliquen principios democráticos básicos y una serie de salvaguardas, y la interferencia sea lícita, proporcionada, limitada en tiempo y alcance, y no arbitraria.¹¹ No obstante, datos recopilados por Access Now y la campaña #KeepItOn (una coalición de más de 220 organizaciones de 99 países de todo el mundo dedicadas a combatir los apagones de Internet) revelan que "en 2019, la causa más común de los apagones de Internet fueron protestas".¹² Este hecho indica que, cuando un estado "dice que debe interrumpir el acceso para restaurar la 'seguridad pública', en realidad, podría significar que (el estado) prevé las protestas y desea interrumpir la capacidad de las personas de organizarse y expresar sus opiniones, ya sea en el entorno digital o el físico".¹³ Además, las autoridades policiales y otros departamentos estatales han recibido grandes poderes para la implementación de medidas de emergencia durante la pandemia del COVID-19, que, desafortunadamente, algunos aplican para restringir el derecho al ejercicio lícito y legítimo de la reunión y la asociación. Actualmente, algunos estados persiguen a individuos y periodistas con leyes de "noticias falsas" o normativas relacionadas con la epidemia durante la pandemia. Y los manifestantes reciben restricciones aún más severas. El envío de mensajes a través de la Web y los servicios de redes sociales se encuentran sujetos a solicitudes de censura y monitoreo de parte de algunas autoridades estatales bajo el pretexto de combatir la desinformación con respecto al COVID-19 o la publicación de "noticias falsas".

Inevitablemente, la pandemia del COVID-19 dejará secuelas. Y las medidas que adopten los estados ahora determinarán su alcance. Las respuestas que brinden deben promover la salud pública, evitar la discriminación, garantizar el acceso a información confiable y oportuna, defender el acceso ilimitado a una Internet abierta, asequible, estable, segura y universal, asegurar el cumplimiento de los derechos a la libertad de expresión y opinión, y de reunión pacífica y asociación, y proteger la privacidad y los datos personales. Access Now se encuentra comprometida a proteger los derechos humanos y colaborar con las respuestas de los estados frente a la pandemia del COVID-19 y las consecuencias posteriores.

En este contexto global (la expansión de los apagones de Internet en todo el mundo, la prevalencia de la vigilancia ilícita, el aumento de la privatización y el impacto de la pandemia del COVID-19), decidimos examinar el estado de los derechos a la libertad de reunión pacífica y asociación desde la perspectiva de los derechos digitales. ¿Cuáles son nuestros antecedentes, particularmente, desde la Primavera Árabe? ¿Cómo estamos actualmente, considerando el impulso de las protestas de Black Lives Matter tanto dentro como fuera de los EE.UU.? Y, por último, ¿hacia dónde nos lleva el impacto del COVID-19?

¹¹ Pacto Internacional de Derechos Civiles y Políticos (ICCPR), 19 de diciembre de 1966, 999 U.N.T.S. 171 y 1057 U.N.T.S. 407 (implementado el 23 de marzo de 1976).

<https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf>, artículos 21-22.

¹² Access Now. *Targeted, Cut Off, and Left in the Dark: The #KeepItOn report on internet shutdowns in 2019, 2020.* <https://www.accessnow.org/keepiton-2019-report>, pág. 13.

¹³ *Ibíd.*

En este artículo, examinamos tres problemas actuales: (1) los apagones de Internet y las interrupciones del acceso y la conectividad, (2) la vigilancia ilícita y el derecho a la privacidad y (3) la influencia del sector privado en el espacio cívico en línea. Los matices de estos problemas, en particular respecto de los rápidos cambios que presenta el contexto global actual, no se analizarán en este artículo. Por lo tanto, los autores desean hacer dos advertencias. Primero, debido al contexto global actual, este artículo se centra en el derecho a la libertad de reunión pacífica (considerando especialmente las protestas colectivas protegidas por las leyes internacionales de derechos humanos) y destaca la necesidad de un análisis más profundo para analizar a fondo el derecho a la libertad de asociación. Segundo, en este artículo, se hace referencia a asuntos actuales, y algunos datos pueden requerir actualizaciones o nuevas investigaciones. Aquí, brindamos un resumen de cada tema mencionado junto con estudios de caso y lineamientos específicos para los estados, el sector privado y las instituciones internacionales respecto de cada uno de ellos. En definitiva, este artículo, que cuenta con el respaldo de casos prácticos de distintas regiones del mundo, tiene el objetivo de brindar un resumen del estado de los derechos a la libertad de reunión pacífica y asociación en la era digital, así como una serie de recomendaciones para las distintas partes interesadas.

II. INTRODUCCIÓN

Los derechos a la libertad de reunión pacífica y asociación se consagran en el Artículo 20 de la Declaración Universal de los Derechos Humanos y se ratifican en el Pacto Internacional de Derechos Civiles y Políticos (ICCPR) de la ONU, en los artículos 21 y 22 respectivamente.¹⁴ El Comité de Derechos Humanos de la ONU, un organismo de expertos independientes que monitorean la implementación del ICCPR e interpretan el significado del tratado, se encuentra actualmente en el proceso de desarrollar (por primera vez) la Observación General N.º 37 sobre el Artículo 21, acerca del derecho a la reunión pacífica.¹⁵ Este instrumento legal oportuno ayudará a interpretar el Artículo 21. Y lo que es más importante, la Observación General actualizará la interpretación del Artículo 21 tras su lanzamiento original en 1966. Esta actualización es útil y necesaria, ya que la naturaleza de las reuniones ha cambiado sustancialmente desde la adopción del ICCPR, en particular, en cuanto al uso de tecnologías digitales en todo el mundo. Por lo tanto, la Observación General tendrá un rol fundamental en el asesoramiento de terceros y otras partes interesadas en cuanto al derecho de reunión pacífica en espacios digitales. Además, la Observación General debe destacar los riesgos potenciales (como el aumento de los apagones de Internet, la limitación del acceso a Internet, la prevalencia de la vigilancia ilícita y la privatización injustificada de los espacios de reunión), que restringen indebidamente el derecho a la reunión pacífica. En este artículo, se analizan estos riesgos en el marco legal de los derechos humanos internacionales a partir de ejemplos regionales y domésticos para respaldar nuestra posición, y se proporcionan recomendaciones con el fin de guiar a las organizaciones internacionales, como la ONU.

Al igual que todos los derechos humanos, los derechos a la libertad de reunión pacífica y asociación son universales, indivisibles, interdependientes e interrelacionados.¹⁶ Si bien el derecho a la libertad de reunión pacífica y el derecho a la asociación suelen analizarse en conjunto, es importante reconocer que son dos derechos diferentes y que suelen estar sujetos a distintas legislaciones domésticas.¹⁷ Por ejemplo, la Observación General se enfoca específicamente en el Artículo 21 (libertad de reunión pacífica). Sin embargo, la asociación es

¹⁴ Resolución de la Asamblea General 217 (III) A, Declaración Universal de Derechos Humanos, (10 de diciembre de 1948). [https://undocs.org/A/RES/217\(III\)](https://undocs.org/A/RES/217(III)); ICCPR, *supra*, nota 9.

¹⁵ Comité de Derechos Humanos de la ONU, *Segunda lectura del borrador de la Observación General N.º 37 sobre el Artículo 21 (Derecho a la reunión pacífica) del Pacto Internacional de Derechos Civiles y Políticos*. <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx>

¹⁶ Conferencia Mundial de Derechos Humanos en Viena, *Declaración y Programa de Acción de Viena*, (25 de junio de 1993). <https://www.ohchr.org/en/professionalinterest/pages/vienna.aspx>

¹⁷ Maina Kiai, *supra*, nota 7, párr. 4.

importante, en particular, en el contexto laboral y en la formación de comunidades de identidad y acciones políticas en línea.

Las libertades de reunión pacífica y asociación son derechos humanos fundamentales, no solo en los estados democráticos, sino también en los autoritarios. Tal como lo describe el Relator Especial de la ONU sobre la libertad de reunión y asociación, estas reuniones y asociaciones pueden funcionar como un "barómetro para medir la situación en cuanto a los derechos humanos (y su prevalencia) en un país determinado y un indicador útil sobre qué tan abiertos o cerrados son los distintos países y sus instituciones nacionales".¹⁸ Las interferencias en las reuniones y asociaciones indican de manera anticipada que el estado no satisface las necesidades o los intereses del público.¹⁹ Las reuniones y las asociaciones, así como las respuestas que obtienen, destacan la necesidad de rendición de cuentas del estado y de otros agentes poderosos, como las corporaciones, que tienen un alto nivel de influencia en la sociedad y afectan los derechos fundamentales, así como quiénes son responsables de su cumplimiento en el marco de los derechos humanos internacionales.²⁰

Este barómetro puede generar acciones tanto a nivel local como internacional. Por ejemplo, después de una solicitud del Grupo de Estados Africanos, que representa a 54 estados miembro del continente africano, el Consejo de Derechos Humanos de la ONU organizó un debate urgente sobre las actuales violaciones de derechos humanos basadas en la etnia, el racismo sistematizado, la brutalidad policial en contra de las personas con ascendencia africana y la violencia contra las protestas pacíficas.²¹ Los estados y más de 600 organizaciones de la sociedad civil de todo el mundo instaron a la ONU para que adoptara una resolución en respuesta al asesinato policial de George Floyd e innumerables afroamericanos. El 19 de junio de 2020 (también conocido como *Juneteenth*, el día en que se

¹⁸ Resolución de la Asamblea General 72/135, *Derecho a la libertad de reunión y asociación pacíficas*, documento de la de la ONU A/72/135 (14 de julio de 2017). <https://undocs.org/A/72/135>, párr. 17.

¹⁹ Comité de Derechos Humanos de la ONU. *Discusión General de medio día de preparación para la Observación General del Artículo 21 (Derecho a la Reunión Pacífica) del Pacto Internacional de Derechos Civiles y Políticos*, Palais Wilson, 20 de marzo de 2019 - Artículo 19, aporte escrito. <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GC37.aspx>, párr. 10.

²⁰ ACNUDH, *Principios Rectores sobre las Empresas y los Derechos Humanos*, HR/PUB/11/04 (16 de junio de 2011). https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

²¹ ACLU, *Carta de Coalición - Solicitud de indagación independiente de la ONU sobre la situación de gravedad creciente de violencia policial y represión de protestas en Estados Unidos*, 2020. <https://www.aclu.org/letter/coalition-letter-request-un-independent-inquiry-escalating-situation-police-violence-and> Esta iniciativa se encuentra acompañada de otros esfuerzos similares de diversas organizaciones de la sociedad civil y expertos internacionales para generar respaldo. Consejo de Derechos Humanos de la ONU. *Statement on the Protests against Systemic Racism in the United States*, 2020.

<https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25927&LangID=E>; y Deutsche Welle, *UN agrees to urgent debate on racism and police violence*, 2020.

<https://www.dw.com/en/un-agrees-to-urgent-debate-on-racism-and-police-violence/a-53807879>

celebra la emancipación de la esclavitud en EE.UU.) la resolución se adoptó por consenso.²² Si bien este hecho fue un evento histórico en muchos aspectos, la resolución final no estuvo a la altura del deseo original de las cientos de organizaciones de la sociedad civil que instaron este debate urgente.²³ No obstante, tal como lo destaca Gay MacDougall, ex Experto Independiente de la ONU en problemas de minorías, "este es un paso importante en esta lucha continua".²⁴

Históricamente, las reuniones y las asociaciones han desempeñado un rol fundamental en la deconstrucción de las distintas formas sistémicas de racismo, la decolonización, la autodeterminación, el avance de la lucha por la igualdad de género y los derechos de la comunidad LGBTQ, entre otros. Por ejemplo, los miembros de la comunidad LGBTQ lograron conquistar derechos hablando en las calles (incluso en los disturbios de Stonewall de 1969, cuando un grupo de individuos transexuales afroamericanos se opusieron al abuso policial en Greenwich Village, lo que dio origen a la tradición del Orgullo).²⁵

Tal como lo mencionamos anteriormente, si bien los derechos a la libertad de reunión pacífica y asociación suelen utilizarse indistintamente, es importante recordar que son dos derechos diferentes.²⁶ Por lo tanto, en esta sección, examinaremos brevemente estos derechos por separado.

DERECHO A LA LIBERTAD DE REUNIÓN PACÍFICA

Las reuniones, comúnmente llamadas "protestas", adoptan muchas formas. Se definen como "un encuentro intencional y temporal en un espacio público o privado con un fin específico".²⁷ Según los organismos internacionales, la libertad de reunión comprende una amplia variedad de encuentros, que pueden ser estáticos o en movimiento, y pueden

²² La resolución final insta al Alto Comisado a preparar un informe exhaustivo sobre el racismo sistémico y supervisar las prácticas similares a las que condujeron al asesinato de George Floyd, la violencia contra los manifestantes y otros incidentes relacionados en todo el mundo. UN News. *Human Rights Council calls on top UN rights official to take action on racist violence*, 2020. <https://news.un.org/en/story/2020/06/1066722>

²³ Human Rights At Home Blog, *The UN Makes Unprecedented Response to George Floyd's Murder*, 2020. https://lawprofessors.typepad.com/human_rights/2020/06/the-un-makes-unprecedented-response-to-george-floyds-murder.html

²⁴ *Ibíd.*

²⁵ Access Now. *Standing together in Pride*, 2020. <https://www.accessnow.org/standing-together-in-pride/>

²⁶ Maina Kiai, *supra*, nota 7, párr. 4.

²⁷ *Ibíd.*, párr. 24.

ubicarse en propiedades públicas o privadas, incluso en calles y rutas.²⁸ De hecho, la Corte Suprema de California sostuvo en un caso puntual que un centro comercial puede considerarse como un foro público. Por lo tanto, este caso establece que los discursos constitucionales y las peticiones de derechos deben protegerse incluso en un centro comercial privado.²⁹ Adicionalmente, en un caso presentado ante la Corte Suprema de Nueva Jersey, la corte reconoció que el centro comercial había desplazado el área central de compras y que, por lo tanto, no podía negar el derecho a utilizar su espacio como un foro público.³⁰

Las leyes internacionales de derechos humanos promueven el derecho a la reunión "pacífica", un adjetivo bastante particular.³¹ En consecuencia, los estados pueden adoptar una interpretación parcial del término "pacífico" a fin de limitar el alcance del derecho.³² Si

²⁸ Organización para la Seguridad y la Cooperación en Europa. *Benchmarks for Laws related to Freedom of Assembly and List of International Standards*. <https://www.osce.org/files/f/documents/5/d/37907.pdf>, párr 6; ver *Rassemblement Jurassien & Unité Jurassienne v Switzerland*, Application N.º 8191/78 (1979) ECtHR. <http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-74721&filename=001-74721.pdf>; ver *Christians against Racism and Fascism v United Kingdom*, Aplicación N.º 8840/78 (1980) ECtHR. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-74287%22%5D%7D>; ver *Anderson and Nine Others v United Kingdom*, Aplicación N.º 33689/96, 25 EHRR CD 172 (1997). <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-3988%22%5D%7D>; ver *Djavit An v. Turkey*, Aplicación N.º 20652/92 (2003) ECtHR. <http://hudoc.echr.coe.int/eng?i=001-60953>; ver *Kudrevičius and others v. Lithuania*, Aplicación N.º 37553/05 (2015) ECtHR. <https://hudoc.echr.coe.int/eng#%7B%22docname%22:%5B%22Kudrevi%C4%8Dius%20and%20others%20v.%20Lithuania%22%22%22%7D%7B%22itemid%22:%5B%22001-158200%22%5D%7D>. Importante: La Convención Europea de Derechos Humanos destaca que "la práctica mediante la cual las autoridades permiten que una reunión se lleve a cabo, pero solo en una ubicación que no brinda visibilidad frente al público objetivo y que, por lo tanto, no le permitirá tener un impacto significativo es incompatible con los requisitos del Artículo 11 de la Convención"; ver *Lashmankin v Russia*, Aplicación n.º 57818/09 (2017) ECtHR. <https://hudoc.echr.coe.int/rus?i=001-170857>, en § 426.

²⁹ *Pruneyard Shopping Ctr v Robins*, 447 U.S. 74 (1980). <https://supreme.justia.com/cases/federal/us/447/74/#tab-opinion-1953647> Es importante destacar que este caso, así como los subsiguientes, dejaron en claro que esta decisión no se aplicó a todos los centros comerciales. Si bien esta decisión fue apelada, la Corte Suprema de los Estados Unidos sostuvo que "un Estado... puede adoptar restricciones razonables respecto de la propiedad privada siempre que estas no la perjudiquen sin una compensación justa ni infrinjan otras disposiciones constitucionales federales". En este caso específico, la Corte afirmó que la petición no resultaba "perjudicial" porque la actividad no implicó un "impedimento razonable del valor o el uso de la propiedad como un centro comercial". A su vez, la Corte Suprema de EE.UU. afirmó que, en esta situación, obligar al propietario a dar lugar a otros oradores no infringe sus derechos constitucionales.

³⁰ *New Jersey Coalition Against War in the Middle East v. J.M.B. Realty Corp*, A-124/125-93 (NJ 1994). La Corte aplicó los factores de balance establecidos en *State v Schmid*. Para obtener más información a nivel internacional, ver, p. ej., Consejo de Derechos Humanos de la ONU, *Informe conjunto del Relator Especial sobre los derechos a la libertad de reunión pacífica y asociación y del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias respecto de la administración correcta de las reuniones*, doc. de la ONU A/HRC/31/66 (4 de febrero de 2016) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/018/13/PDF/G1601813.pdf?OpenElement>, párr. 84. A nivel regional, ver *Appleby v. the United Kingdom*, Application No. 44306/982003) ECtHR. <https://hudoc.echr.coe.int/eng#%7B%22appno%22:%5B%2244306/98%22%22%7D%7B%22documentcollectionid%22:%5B%22GRANDCHAMBER%22%22%7D%7B%22itemid%22:%5B%22001-61080%22%5D%7D>

³¹ En el contexto regional de África, no se incluye el adjetivo "pacífico".

³² Se aplica un adjetivo similar en los marcos legales regionales y domésticos, salvo en la Carta Africana de Derechos Humanos y de los Pueblos, que, en el Artículo 11, garantiza el "derecho a la reunión libre", sin hacer referencia a la calidad de "pacífico".

bien el término "pacífico" se ha aplicado principalmente a los encuentros físicos, el espectro entre los entornos físico y en línea es cada vez más fluido. Todas las partes interesadas involucradas en manifestaciones (ya sea la prensa, la policía o los manifestantes) pueden utilizar tecnologías digitales. Y, con frecuencia, intentan responder ante el uso del otro o controlarlo.

Las cortes regionales y los estándares internacionales existentes brindan interpretaciones importantes de lo que significa que una reunión sea "pacífica". Para "evitar el riesgo de una interpretación restrictiva" del derecho a la libertad de reunión pacífica, la Corte Europea de Derechos Humanos se abstiene de "formular la noción de reunión o enumerar exhaustivamente los criterios que la definen".³³ Asimismo, en *The Right to Protest: Principles on the protection of human rights in protests (The Right to Protest Principles)* (El derecho a la protesta: Principios sobre la protección de los derechos humanos en protestas (Principios del derecho a la protesta)), un conjunto de principios establecidos por la organización de sociedad civil ARTÍCULO 19 establece una equivalencia entre "pacífico" y "no violento" a fin de compensar la interpretación parcial de los estados que podría restringir este derecho.³⁴ En su presentación escrita para el debate general de medio día del Comité de Derechos Humanos de la ONU, en preparación para la Observación General sobre el Artículo 21 (Derecho a la Reunión Pacífica), ARTÍCULO 19 sostiene que, al determinar si una reunión es "pacífica", el análisis correspondiente se debe llevar a cabo en cada caso específico y teniendo en cuenta el contexto, en particular (1) la intención de los organizadores y los participantes y (2) las probabilidades de que se produzca un nivel significativo de violencia y daño a la propiedad. En este análisis, se debe aplicar una escala con límites altos que proporcione la mayor protección posible al derecho a la libertad de reunión pacífica sin perder de vista que la conducta en cuestión puede estar sujeta a limitaciones según el Artículo 21.³⁵

Este análisis binario es especialmente relevante en el contexto digital. Por ejemplo, consideremos las tácticas en línea que pueden generar interrupciones, confusiones o daños potenciales. Un espectro cada vez mayor de actividades, como el *Zoombombing* (un término creado a partir de la plataforma de videollamadas en línea), puede infringir los términos de

³³ *Navalnyy v Russia*, Aplicación N.º 29580/12 y otros cuatro, [GC] (2018) ECtHR.
<https://hudoc.echr.coe.int/eng#%7B%22docname%22:%5B%22Navalnyy%20v%20Russia%22%5D%2C%22documentcollectionid%22:%5B%22GRANDCHAMBER%22%2C%22CHAMBER%22%5D%2C%22itemid%22:%5B%22001-187605%22%5D%7D>, párr. 98.

³⁴ Article 19. *The Right to Protest: Principles on the protection of human rights in protests*, 2016.
https://www.article19.org/data/files/medialibrary/38581/Right_to_protest_principles_final.pdf Para obtener más información, consulte el principio 1.2 de los Principios del Derecho a la Protesta, que establece una cuatro consideraciones que se deben tener en cuenta para interpretar los términos "pacífico" o "no violento" a fin de proteger los derechos humanos en la mayor medida posible para la realización de reuniones pacíficas.

³⁵ Comité de Derechos Humanos de la ONU, *supra*, nota 19, párr. 16.

uso de la plataforma privada o la ley penal.³⁶ No obstante, en algunas circunstancias, ¿podrían estas interrupciones considerarse formas legítimas de desacuerdo explícito? Según el contexto y la naturaleza de la interrupción, el Zoombombing podría asemejarse más a un *flash mob* o una expresión repentina en un evento de campaña política o un evento privado, a fin de expresar desacuerdo e interrumpir las dinámicas inherentes presentes en ciertas discusiones. En general, parece claro que la desobediencia civil seguirá formando parte de la era digital, y las tácticas evolucionarán constantemente a medida que avanzan las tecnologías digitales. La intención del organizador (ya sea expresar discrepancia, lo cual estaría dentro del alcance del derecho, o simplemente interrumpir, provocar o impedir ciertas acciones) es una consideración clave. Asimismo, el significado de "daño significativo" o la probabilidad de que nos encontremos frente a uno también se deben tener en cuenta. ¿El Zoombombing o las demás perturbaciones digitales similares causan daños "significativos"? Si es así, ¿a quién afectan, en qué medida y por cuánto tiempo? Para conocer los detalles específicos de estas preguntas, es necesario llevar a cabo un análisis más profundo.

Es importante destacar que, tal como lo remarca ARTÍCULO 19, incluso si quienes participan "en una reunión incurrir en actos de violencia o daños a la propiedad, esto no debe ser un motivo suficiente para categorizar (automáticamente) el encuentro como "no pacífico" y negar a los participantes su derecho a la reunión pacífica".³⁷ De hecho, en 1980, la Comisión Europea de Derechos Humanos opinó que:

La posibilidad de que se produzcan contramanifestaciones violentas o de que se unan extremistas con intenciones violentas que sean ajenos a la asociación organizadora no deben, en sí mismas, restringir el derecho (a la reunión pacífica). Incluso si una manifestación pública cuenta con un riesgo real de generar disturbios a cargo de agentes ajenos al control de los organizadores, este motivo no es suficiente para excluir dicha procesión del alcance del Artículo 11 (1).³⁸

La intención de llevar adelante una reunión pacífica es clave a la hora de determinar si el encuentro recae dentro del alcance del derecho, a diferencia de la probabilidad de violencia debida a las reacciones de otros grupos, o bien otros factores.³⁹ *The Right to Protest Principles* luego afirma que "los estados deben reconocer que siempre que una protesta terminó de

³⁶ Para obtener más información, ver Lawfare. *Prosecuting Zoom-Bombing*, 2020. <https://www.lawfareblog.com/prosecuting-zoom-bombing>

³⁷ Comité de Derechos Humanos de la ONU, *supra*, nota 19, párr. 18.

³⁸ *Christians against Racism and Fascism v United Kingdom*, *supra*, nota 28, pág. 148; *Anderson and Nine Others vs United Kingdom*, *supra*, nota 28.

³⁹ Ver Maina Kiai, *supra*, nota 7, párr. 25.

forma violenta, esto se debió al fracaso del estado a la hora de posibilitar una manifestación pacífica, evitar la violencia y colaborar para resolver el conflicto con las partes que podían generar violencia o tenían probabilidades de hacerlo".⁴⁰ Esta responsabilidad del estado también se aplica en línea, dado que los ciberataques a la sociedad civil limitan el espacio cívico y perjudican la movilización democrática. Las interrupciones pueden utilizarse para las protestas legítimas, pero también (y probablemente con más frecuencia) se usan para coartar derechos humanos y el funcionamiento de la democracia.

DERECHO A LA LIBERTAD DE ASOCIACIÓN

Según el Relator Especial de la ONU sobre la libertad de asociación y reunión, "'asociación' hace referencia a, entre otras cosas, organizaciones de la sociedad civil, clubes, cooperativas, ONG, asociaciones religiosas, partidos políticos, uniones comerciales, fundaciones o incluso asociaciones en línea, por lo que Internet ha sido fundamental, por ejemplo, para 'facilitar la participación activa de los ciudadanos en el desarrollo de sociedades democráticas'".⁴¹ Particularmente, las asociaciones pueden ser *ad hoc*, dedicarse a una causa o problema específicos y pueden existir durante distintos períodos de tiempo. El derecho a la libertad de asociación protege de igual manera a las asociaciones registradas y no registradas.⁴²

DERECHOS A LA LIBERTAD DE REUNIÓN PACÍFICA Y ASOCIACIÓN EN LÍNEA

El Consejo de Derechos Humanos de la ONU declaró que los mismos derechos que las personas tienen en el entorno físico deben protegerse en el entorno digital.⁴³ El Comité de Derechos Humanos de la ONU instó a los estados a "garantizar que los mismos derechos que los individuos tienen en el entorno físico... se protejan en el entorno en línea conforme a las leyes de derechos humanos".⁴⁴ Internet, en particular las redes sociales, y otras TIC facilitaron el goce de los derechos a la libertad de reunión y asociación pacíficas tanto en línea como en el entorno físico. Según la Asociación para el Progreso de las Comunicaciones (APC), las

⁴⁰ Article 19. *The Right to Protest: Principles on the protection of human rights in protests*, 2016.

https://www.article19.org/data/files/medialibrary/38581/Right_to_protest_principles_final.pdf, 1.2 (d).

⁴¹ Maina Kiai, *supra*, nota 7, párr. 52.

⁴² *Ibid.*, párr. 56.

⁴³ Comité de Derechos Humanos de la ONU, Consejo de Derechos Humanos de la ONU, Res. 38/L.10, *The promotion, protection and enjoyment of human rights on the Internet*, ONU, de la ONU A/HRC/38/L.10/Rev.1 (4 de julio de 2018).

<https://undocs.org/en/A/HRC/38/L.10/REV.1>; Consejo de Derechos Humanos de la ONU, Res. 24/5, *The rights to freedom of peaceful assembly and association*, doc. de la ONU A/HRC/RES/24/5 (8 de octubre de 2013).

<http://freeassembly.net/wp-content/uploads/2013/08/A-HRC-RES-24-5-ENG.pdf>, párr. 2.

⁴⁴ Comité de Derechos Humanos de la ONU, Res. 73/173, *Promotion and protection of human rights and fundamental freedoms, including the rights to peaceful assembly and freedom of association*, ONU, de la ONU A/HRC/Res/73/173 (8 de enero de 2019) <https://undocs.org/en/A/RES/73/173> párr. 4. Para obtener información de un ejemplo regional destacado que afirme estos derechos en el contexto en línea, ver la Declaración Africana sobre los Derechos y Libertades en Internet del Grupo de la Declaración Africana. *African Declaration on Internet Rights and Freedoms*, 2015.

<https://africaninternetrights.org/articles/>

asociaciones en línea "hacen referencia al acto de formar grupos en línea, incluso grupos informales, ya sea con o sin moderadores o líderes".⁴⁵ Asimismo, el concepto de "reunión pacífica en línea" hace referencia a "un encuentro intencional y temporal en un espacio público o privado y con un fin específico que incluye actos de coordinación, organización, planificación o reunión en plataformas disponibles en línea, como servicios de mensajería instantánea, recursos de voz sobre protocolo de Internet, aplicaciones de chat, grupos de correos electrónicos y listas de difusión, entre otros".⁴⁶

Se utilizan varias técnicas y herramientas en línea para colaborar con los derechos a la libertad de reunión y asociación pacíficas en el entorno digital.⁴⁷ En 2019, el Relator Especial de la ONU sobre la libertad de reunión y asociación, Clément Voule, presentó un informe oportuno sobre el ejercicio de los derechos a la libertad de reunión pacífica y asociación en la era digital ante el Consejo de Derechos Humanos de la ONU.⁴⁸ En este informe, Voule hace referencia a la intersección entre las tecnologías digitales, y la reunión pacífica y la asociación, y destaca algunos ejemplos de distintas partes del mundo que "demuestran el poder que tiene la tecnología digital para las personas que desean reunirse a fin de promover la democracia, la paz y el desarrollo".⁴⁹ Por ejemplo, es frecuente el uso de *hashtags* para compartir información, movilizar a las personas y reunir respaldo a nivel mundial.⁵⁰ Las tecnologías de encriptación de extremo a extremo, los pseudónimos y otros recursos de seguridad digital brindan a las personas la posibilidad de operar en un espacio digital seguro a fin de conectarse y movilizarse sin interferencias no deseadas.⁵¹ Por último, las plataformas de peticiones y financiamiento colectivo que circulan a través de las redes sociales permiten a las personas llegar a nuevos públicos, fomentar la participación y diseminar información a nivel global.⁵² Consideremos, por ejemplo, los esfuerzos de los jóvenes de todo el mundo para utilizar plataformas de medios sociales, como TikTok, a fin de movilizar a otras personas en contra de la injusticia. Recientemente, los seguidores de la escena de la música popular de Corea del Sur, conocida como *K-pop*, participaron en iniciativas activistas en línea para brindar su respaldo al movimiento Black Lives Matter. Además de utilizar las redes sociales

⁴⁵ Venkiteswaran, G., Asociación para el Progreso de las Comunicaciones (APC). *Freedom of assembly and association online in India, Malaysia and Pakistan: Trends, challenges and recommendations*, 2016. https://www.apc.org/sites/default/files/FOAA_online_IndiaMalaysiaPakistan.pdf, pág. 13.

⁴⁶ *Ibíd.*, pág. 13.

⁴⁷ Comité de Derechos Humanos de la ONU, Consejo de Derechos Humanos de la ONU, Res. 21/16, *The rights to freedom of peaceful assembly and of association*, doc. de la ONU A/HRC/RES/21/16 (11 de octubre de 2012). <https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/174/63/PDF/G1217463.pdf?OpenElement>

⁴⁸ Consejo de Derechos Humanos de la ONU, *Informe del Relator Especial sobre el derecho a la libertad de reunión y asociación pacíficas*, Clément Voule, doc. de la ONU A/HRC/41/41 (17 de mayo de 2019). <https://undocs.org/A/HRC/41/41>

⁴⁹ *Ibíd.*, párr. 2.

⁵⁰ *Ibíd.*, párr. 22-23, 43.

⁵¹ *Ibíd.*, párr. 24.

⁵² *Ibíd.*, párr. 25.

para solicitar donaciones (con lo cual reunieron alrededor de un millón de dólares para organizaciones asociadas con Black Lives Matter), los fanáticos del K-pop tomaron medidas para "desbaratar las operaciones policiales" diseñadas para identificar a los manifestantes de Black Lives Matter. Para ello, "pidieron a los demás seguidores que envíen sus filmaciones de *fancam* a un departamento de policía de EE.UU." y que se apropien de los hashtags racistas.⁵³ El activismo de estos grupos recibió cada vez más atención tras las noticias recientes sobre la baja concurrencia al evento político del presidente de los EE.UU., Donald Trump, a mediados de junio. Los usuarios de TikTok y los seguidores del K-pop revelaron que "se movilizaron para pedir entradas a fin de inflar las expectativas de concurrencia".⁵⁴ Según Marshall McLuhan, un famoso filósofo canadiense, "el medio es el mensaje". Esto significa que el acceso a Internet y las distintas tecnologías digitales es clave a la hora de rediseñar el propósito de las herramientas digitales y utilizarlas para organizarse y realizar protestas de formas únicas y creativas. En general, estas iniciativas de movilización en línea destacan el impulso que han generado estos tipos de asociaciones y activismo al aprovechar las herramientas digitales para promover el ejercicio de la libertad de reunión y asociación pacíficas en la era digital.

RESTRICCIONES ACEPTABLES CONFORME A LA LEY INTERNACIONAL DE DERECHOS HUMANOS

Los derechos a la libertad de reunión y asociación pacíficas no son absolutos, y los estándares internacionales permiten ciertas restricciones en circunstancias limitadas y específicas.⁵⁵ El Artículo 21 y el Artículo 22(2) del ICCPR respectivamente establecen que "no se deben aplicar restricciones en el ejercicio de este derecho salvo aquellas previstas por la ley y que sean necesarias en una sociedad democrática, en interés de la seguridad nacional, de la seguridad pública o del orden público, o para proteger la salud o la moral públicas o los derechos y libertades de los demás".⁵⁶ Las restricciones no deben contradecir los propósitos del derecho y deben ser proporcionadas y "necesarias en una sociedad democrática".⁵⁷ El Artículo 22 (2), acerca del derecho a la asociación, agrega una advertencia adicional: "El presente artículo no impedirá la imposición de restricciones legales al ejercicio de tal derecho

⁵³ The Guardian. *Digitally-savvy and passionate, K-pop fans' Trump activism should come as no surprise*, 2020. <https://www.theguardian.com/commentisfree/2020/jun/22/digitally-savvy-and-passionate-k-pop-fans-trump-activism-should-come-as-no-surprise>

⁵⁴ *Ibíd.*

⁵⁵ Asociación Americana para la Comisión Internacional de Juristas. *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, 1984. <https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf>

⁵⁶ ICCPR, *supra*, nota 9., Artículos 21 y 22; Consejo de Derechos Humanos de la ONU, Res. 15/21, *The rights to freedom of peaceful assembly and of association*, doc. de la ONU A/HRC/RES/15/21 (6 de octubre de 2010). <https://undocs.org/en/A/HRC/RES/15/21>

⁵⁷ Maina Kiai, *supra*, nota 7, párr. 16.

cuando se trate de miembros de las fuerzas armadas y de la policía".⁵⁸ El Relator Especial de la ONU sobre la libertad de reunión y asociación, Clément Voule, destaca que, en el contexto digital, "la libertad de acceso y uso de tecnologías digitales para el ejercicio de los derechos de reunión pacífica y asociación debe ser la regla, y las limitaciones deben ser la excepción".⁵⁹

Al escribir este artículo, 173 países ya ratificaron el ICCPR, afirmando así los derechos a la libertad de reunión pacífica y asociación. No obstante, algunos de los estados parte del ICCPR aplican restricciones excesivas sobre dichos derechos, tanto en el entorno físico como el digital, entre ellos, Estados Unidos, Egipto, Túnez, Sudán, Irán, Siria, China, Cuba, Etiopía y Vietnam.⁶⁰ En la siguiente sección, se examinan estudios de caso específicos de estos y otros contextos domésticos a fin de respaldar las recomendaciones para los estados, las empresas y las organizaciones internacionales.

⁵⁸ ICCPR, *supra*, nota 9, Artículo 22;

⁵⁹ Clément Voule, *supra*, nota 48, párr. 12.

⁶⁰ OHCHR. *Status of Ratification Interactive Dashboard*. <https://indicators.ohchr.org/>

Es importante destacar que algunos de estos los países que se mencionan, como Estados Unidos, Egipto, Sudán, Siria, China, Etiopía y Vietnam, no han tomado medidas para firmar o ratificar el Protocolo Opcional del ICCPR.

III. ACCESO, CONECTIVIDAD Y APAGONES DE INTERNET

Las interrupciones del acceso a Internet y los servicios de comunicación por parte de los estados durante manifestaciones públicas son cada vez más frecuentes. Un apagón de Internet se produce cuando alguien (generalmente, un estado) interrumpe intencionalmente el acceso a Internet o ciertas aplicaciones móviles para controlar lo que las personas hacen o dicen. Los apagones de Internet también suelen llamarse "bloqueos de Internet" o "*kill switches*".⁶¹

Los apagones de Internet son una herramienta flagrante que usan los estados para reprimir protestas y discrepancias. Según datos recopilados por Access Now y la coalición #KeepItOn, "en 2019, la causa más común de los apagones de Internet fueron las protestas".⁶² Este hecho indica que, cuando un estado "dice que debe interrumpir el acceso para restaurar la 'seguridad pública', en realidad, podría significar que (el estado) prevé las protestas y desea interrumpir la capacidad de las personas de organizarse y expresar sus opiniones, ya sea en el entorno digital o el físico".⁶³ Los apagones de Internet restringen el acceso a información vital y perjudican el derecho fundamental a la libertad de expresión. Además, estas medidas bloquean la comunicación entre los manifestantes y les impiden compartir filmaciones de las manifestaciones. Por ejemplo, en 2017, Access Now y WITNESS enviaron una carta a varios proveedores importantes de servicios de comunicación en la que destacaban las preocupaciones sobre el desborde y la congestión excesiva de las redes durante las protestas del fin de semana de inauguración del presidente Trump, ya que podrían evitar que los manifestantes y periodistas registren los sucesos.⁶⁴ A su vez, esto podría impedir que los manifestantes accedan a servicios médicos y de emergencia, así como a información vital, y que puedan comunicarse con sus amigos y familiares ubicados en otras partes del país y en el exterior.

El flujo libre de información es fundamental en los momentos de agitación social, pero los apagones de Internet impiden que los periodistas informen la situación desde el lugar donde

⁶¹ Una definición más técnica de "apagones de Internet" elaborada por expertos explica que "un apagón de Internet es una interrupción intencional de Internet o a las comunicaciones electrónicas a fin de impedir su acceso o su uso, para una población específica o en una ubicación determinada, frecuentemente, con el fin de ejercer control sobre el flujo de información". Access Now, *supra*, nota 10, FN 1.

⁶² *Ibíd.*, pág. 13.

⁶³ *Ibíd.*

⁶⁴ The Hill. *Cellphone providers brace for heavy inauguration use*, 2017. <https://thehill.com/policy/technology/315187-cellphone-providers-brace-for-heavy-inauguration-use>; Access Now. *Re: Ensure internet connectivity for events and demonstrations during weekend of presidential inauguration*, 2016. https://www.accessnow.org/cms/assets/uploads/2017/01/Mobile_Internet_AccessNow_Witness12-21.pdf

sucedan. A veces, estas medidas no permiten que los medios se comuniquen con sus fuentes y compartan información realista sobre la violencia y las infracciones de los derechos humanos por parte de las fuerzas de seguridad. Pensemos, por ejemplo, en las manifestaciones de #IAmTheSudanRevolution. En junio de 2019, en la semana siguiente al apagón de Internet de Sudán, 100 personas fueron asesinadas, 700 resultaron heridas y se produjeron al menos 70 abusos sexuales.⁶⁵ El apagón hizo que fuera extremadamente difícil para los periodistas mostrar la alta cantidad de violaciones de derechos humanos que se cometieron durante esa semana a medida que ocurrían.

Muchas agencias de medios locales e internacionales no pudieron comunicarse con sus fuentes ni sus informantes, enviar sus historias ni verificar la gran cantidad de videos que se publicaban en línea. Lógicamente, los métodos de comunicación alternativos disponibles, como los SMS y las llamadas a teléfonos celulares, eran inseguros y ponían en peligro a los periodistas, activistas, defensores de derechos humanos y proveedores de servicios de emergencia.⁶⁶

A grandes rasgos, los apagones de Internet perjudican la educación y tienen consecuencias económicas y de salud en tiempos de protesta. De hecho, estas medidas exacerbaban especialmente estos efectos en el contexto de la crisis de salud mundial sin precedentes que vivimos hoy, en el que el acceso a la información sanitaria es clave para salvar vidas.⁶⁷

Las restricciones que imponen los estados sobre los derechos a la libertad de reunión pacífica y asociación, en especial los apagones de Internet, no cumplen con los estándares internacionales de derechos humanos.⁶⁸ De hecho, en 2015, una serie de importantes expertos internacionales y de la ONU en materia de derechos humanos afirmaron que los apagones de Internet no deben permitirse en ningún contexto conforme a la ley internacional de derechos humanos, incluso en momentos de conflicto.⁶⁹ Numerosas cortes, incluida la ECtHR, han dispuesto que las restricciones innecesarias o las órdenes de bloqueo que impidan el acceso a dominios o servicios web completos no pueden considerarse como restricciones proporcionadas sobre los derechos fundamentales protegidos a nivel

⁶⁵ Access Now. *#IAmTheSudanRevolution: There's a direct link between internet shutdowns and human rights violations in Sudan!*, 2019.

<https://www.accessnow.org/iamthesudanrevolution-theres-a-direct-link-between-internet-shutdowns-and-human-rights-violations-in-sudan/>

⁶⁶ *Ibíd.*

⁶⁷ Access Now. *#KeepItOn: Internet shutdowns put lives at risk during COVID-19*, 2020.

<https://www.accessnow.org/keepiton-internet-shutdowns-put-lives-at-risk-during-covid-19/>

⁶⁸ Frank La Rue, *supra*, nota 6, párr. 79.

⁶⁹ Access Now. *Internet kill switches are a violation of human rights law, declare major UN% and rights experts*, 2015.

<https://www.accessnow.org/internet-kill-switches-are-a-violation-of-human-rights-law-declare-major-un/>

internacional conforme a la ley de derechos humanos.⁷⁰ Estas decisiones críticas jurisprudenciales ratifican que los estados ya no pueden justificar las órdenes de corte de servicios móviles o de Internet a las empresas de telecomunicaciones frente a situaciones de agitación social o protesta, y tienen un gran impacto en los derechos de los manifestantes de todo el mundo.

Un hecho relacionado, aunque diferente de los apagones de Internet, es el problema de la conectividad de Internet. La conectividad garantiza que los individuos puedan comunicarse entre sí y acceder a la información que necesitan para hacer un uso pleno de sus derechos humanos, incluidos sus derechos a la libertad de reunión pacífica y asociación. No obstante, la realidad es que, a medida que los estados desconectan intencionalmente a los ciudadanos de Internet para reprimir el disenso y las reuniones pacíficas, también descuidan las inversiones en infraestructura (a veces involuntariamente y otras veces deliberadamente) que permiten a las personas conectarse a Internet. Al igual que otras infraestructuras fundamentales, como la atención médica, las calles, etc., las infraestructuras que permiten la conexión a Internet no llegan a las áreas marginadas.

La conectividad es esencial para la participación económica, social, cultural política y cívica en la era digital. Dado que más de 3.600 millones de personas de todo el mundo no tienen acceso a Internet, el mayor grupo de partes interesadas en estas iniciativas permanece desconectado, tiene altas probabilidades de seguir marginado, no participa de las consultas y corre un alto riesgo de quedar atrás.⁷¹ Este problema es particularmente grave si consideramos la cantidad desproporcionada de individuos y grupos marginados que no tienen conectividad. Estas personas no pueden utilizar las tecnologías digitales para acceder a información y comunicarse con otros para organizar protestas y otros tipos de reuniones en los espacios físico y digital a fin de visibilizar la responsabilidad de los estados y otros agentes poderosos en las injusticias y las desigualdades sistémicas. Distintas investigaciones científicas han revelado "un sesgo político persistente y sólido en la asignación de cobertura de Internet para los grupos étnicos en todo el mundo".⁷² Además de la etnia, también es necesario considerar otros indicadores que afectan el acceso de los individuos a Internet,

⁷⁰ Access Now. #KeepItOn: Keeping the internet open and secure in Hong Kong, 2019.

<https://www.accessnow.org/keeping-internet-open-in-hong-kong/>

⁷¹ Access Now. *The Human Rights Principles for Connectivity and Development*, 2016.

<https://www.accessnow.org/cms/assets/uploads/2016/10/The-Human-Rights-Principles-for-Connectivity-and-Development.pdf>; Unión Internacional de Telecomunicaciones. *New ITU data reveal growing Internet uptake but a widening digital gender divide*, 2019. <https://www.itu.int/en/mediacentre/Pages/2019-PR19.aspx>

⁷² Nils B. Weidmann, Suso Benitez-Baleato, Philipp Hunziker, Eduard Glatz, Xenofontas Dimitropoulos. *Digital discrimination: Political bias in Internet service provision across ethnic groups*, *Science* 353, n.º 6304 (9 de septiembre de 2016): 1151-1155. <https://science.sciencemag.org/content/353/6304/1151>

incluida la raza. Por ejemplo, según Pew Research Center, en EE.UU., "el 92% de los caucásicos a nivel nacional utilizó Internet en 2019, mientras que, en los afroamericanos, este porcentaje es del 85% y, en los hispanos, del 86%".⁷³ Por lo tanto, examinar las experiencias individuales de los distintos grupos con diferencias en el acceso al espacio digital implica desafiar "la frecuente suposición de que las desigualdades de distribución de tecnología digital en todo el mundo pueden mitigarse con fuerzas e incentivos económicos", como compensaciones y regulaciones estratégicas (o la ausencia de este tipo de regulaciones) para las empresas de telecomunicaciones.⁷⁴

Este análisis es especialmente importante en el debate sobre el acceso a Internet y las consecuencias sociales, económicas y de salud de la pandemia del COVID-19, así como su período posterior. Incluso con apagones breves o parciales, el impacto en la economía y los derechos humanos puede ser devastador. Mientras más dure el apagón, peores serán las secuelas a nivel general, con efectos indirectos que azotarán la economía y el desarrollo. Por ejemplo, según las estimaciones, el corte de Internet que se produjo durante las protestas de Zimbabwe en 2019 le costó al país cerca de USD 5.7 millones por día.⁷⁵ En muchos estados, estos costos solo empeorarán durante la pandemia del COVID-19 y después de esta.

Internet es una herramienta esencial para el respeto de los derechos humanos en la era digital. Algunos sugieren incluso que el acceso a Internet es un derecho humano.⁷⁶ No obstante, la pandemia del COVID-19 no ha hecho más que amplificar la diferencia entre quienes tienen acceso a una conexión a Internet universal estable, asequible, abierta y segura, y quienes no cuentan con este recurso. Los Objetivos de Desarrollo Sostenible (SDG) son una serie de metas ambiciosas para eliminar la pobreza extrema y combatir el cambio climático en todo el mundo antes de 2030. Según el Instituto Danés para los Derechos Humanos, "más del 90% de los objetivos de SDG están relacionados con los estándares laborales y los derechos humanos internacionales".⁷⁷ La agenda para el 2030 está basada en los derechos humanos, lo que significa que su protección es fundamental para cumplir los

⁷³ Pew Research Center. Internet/Broadband Fact Sheet, 2019.
<https://www.pewresearch.org/internet/fact-sheet/internet-broadband/>;

National Telecommunications and Information Administration. *The State of the Urban/Rural Digital Divide*, 2016.
<https://www.ntia.gov/blog/2016/state-urbanrural-digital-divide>

⁷⁴ Nils B. Weidmann, Suso Benitez-Baleato, Philipp Hunziker, Eduard Glatz, Xenofontas Dimitropoulos, *supra*, nota 72.; Access Now. *We can't reach the U.N. goals for sustainable development without the internet*, 2017.
<https://www.accessnow.org/cant-reach-u-n-goals-sustainable-development-without-internet/>

⁷⁵ Exx Africa Business Risk Intelligence. *Special Report: The cost of internet shutdowns in Africa*, 2019.
https://exxafrica.com/wp-content/uploads/2019/01/SPECIAL-REPORT_-THE-COST-OF-INTERNET-SHUTDOWNS-IN-AFRICA.pdf

⁷⁶ OpenGlobalRights. *COVID-19 exposes why access to the internet is a human right*, 2020.
<https://www.openglobalrights.org/covid-19-exposes-why-access-to-internet-is-human-right/>

⁷⁷ The Danish Institute for Human Rights. *The sustainable development goals (SDGs)*.
<https://www.humanrights.dk/learning-hub/sustainable-development-goals-sdgs>

SDG. Consideramos que extender el acceso seguro y abierto a Internet es esencial para el ejercicio de los derechos humanos en la era digital y, por lo tanto, para cumplir los SDG. Estos objetivos, en particular el SDG 9.C, instan a los países menos desarrollados (LDC) a proporcionar una conexión a Internet universal antes de 2020. Desde nuestra perspectiva, esto implica extender la alfabetización digital y el acceso a la Web global y abierta, no solo brindar una conectividad censurada, vigilada, limitada o basada en aplicaciones. El objetivo es extremadamente ambicioso y, ya en la segunda mitad de 2020 y en medio de una pandemia global, la necesidad de movilizar la voluntad política para acelerar los objetivos de SDG es más imperiosa que nunca, dado que el mundo está lejos de cumplir esta meta.

Respetar los derechos humanos en línea es particularmente importante para garantizar los derechos humanos de las mujeres. Tal como lo destaca la Oficina del Alto Comisionado para los Derechos Humanos (OHCHR) en su informe sobre la división digital basada en el género, "las activistas mujeres, incluidas las defensoras de los derechos humanos de las mujeres, emplean cada vez más las TIC para mostrar y generar respaldo, comunicarse, movilizarse, protegerse, acceder a información y ganar visibilidad".⁷⁸ La OHCHR destaca específicamente que "dado que muchas defensoras de los derechos humanos de las mujeres todavía encuentran dificultades para acceder a los espacios en línea, la necesidad de compartir dispositivos, utilizar cibercafés o teléfonos móviles básicos⁷⁹ puede limitar sus derechos a la libertad de opinión y expresión e incrementar aún más su inseguridad digital".⁸⁰ Los estados tienen la obligación de facilitar el ejercicio de los derechos humanos, incluso en el entorno digital.⁸¹ Las divisiones digitales representan un desafío importante, especialmente, en algunas regiones del mundo. No obstante, los países de Norteamérica y Latinoamérica deben ser reconocidos por sus esfuerzos recientes para abordar las divisiones basadas en el género. Doreen Bogdan-Martin, directora del Sector de Desarrollo de las

⁷⁸ Consejo de Derechos Humanos de la ONU, *Promotion, protection and enjoyment of human rights on the Internet: ways to bridge the gender digital divide from a human rights perspective - Informe del Alto Comisionado para los Derechos Humanos de las Naciones Unidas*, ONU, de la ONU A/HRC/35/9 (5 de mayo de 2017). <https://undocs.org/A/HRC/35/9>, párr. 23.

⁷⁹ Normalmente llamados "feature phones" en inglés.

⁸⁰ Comité de Derechos Humanos de la ONU, de la ONU, *supra*, nota 78, párr. 23; APC. *What are the digital security concerns and threats facing women human rights defenders?*, 2012.

<https://www.apc.org/en/news/what-are-digital-security-concerns-and-threats-facing-women-human-rights-defenders;>

Asociación para los Derechos de las Mujeres y el Desarrollo, *Our right to safety: women human rights defenders' holistic approach to protection*, 2014,

https://www.awid.org/sites/default/files/atoms/files/Our%20Right%20To%20Safety_FINAL.pdf, pág. 19.

Point of View. *Free To Be Mobile*. https://sgt-57ed.kxcdn.com/wp-content/uploads/2019/03/FTBM_Web_final.pdf, una organización sin fines de lucro basada en India que tiene el propósito de empoderar a las mujeres, las niñas y las personas *queer* y trans para que habiten libremente los dominios digitales, lanzó un informe llamado "Free To Be Mobile" (Libertad en los dispositivos móviles), el cual presenta 10 historias de violencia en línea con el uso de dispositivos móviles.

⁸¹ Comité de Derechos Humanos de la ONU, Consejo de Derechos Humanos de la ONU, Res. 38/7, *The promotion, protection and enjoyment of human rights on the Internet*, doc. de la ONU A/HRC/Res/38/7 (17 de julio de 2018).

<https://undocs.org/A/HRC/RES/38/7>, párr. 5.

Telecomunicaciones de la Unión Internacional de Telecomunicaciones, afirma que "más hombres que mujeres usan Internet en todas las regiones del mundo, salvo en América, y felicitó a los creadores de políticas de los países de Norteamérica y Latinoamérica por su éxito en la promoción de la igualdad digital".⁸²

CASOS PRÁCTICOS

Extender el acceso seguro y abierto a Internet es esencial para el ejercicio de los derechos humanos en la era digital y, por lo tanto, para cumplir los SDG. No obstante, para muchas poblaciones del mundo, este servicio aún no está disponible (con frecuencia debido a fallas de diseño) o el acceso se encuentra sujeto a restricciones, censura o vigilancia. En las reuniones, especialmente, es fundamental proteger la integridad de los canales de comunicación, incluido Internet, para que los heridos puedan acceder a los servicios médicos y de emergencia que requieran, los periodistas puedan reportar sus historias y comunicarse con sus fuentes y las personas puedan contactarse con sus familiares, amigos y seres queridos.⁸³ A continuación, analizaremos algunos ejemplos domésticos a fin de comprender el impacto de los apagones de Internet y las interrupciones de la conectividad.

Ecuador

#decreto883 #Ecuador #ParoNacionalEC

En octubre de 2019, el presidente de Ecuador publicó el decreto 883, que aplicaba cambios sustanciales a la economía ecuatoriana a fin de satisfacer los requisitos para recibir un préstamo del Fondo Monetario Internacional. Para ello, el gobierno eliminó los subsidios sobre el precio del combustible, lo cual afectó drásticamente el suministro de productos y el precio del transporte y generó faltantes de combustible y especulación de precios, entre otros efectos. En consecuencia, muchos grupos indígenas del país viajaron a la capital y lideraron protestas contra estas medidas⁸⁴, tal como lo habían hecho años antes para luchar en favor de otras causas.⁸⁵ Mientras viajaban, experimentaron interrupciones en su conexión a Internet y en la

⁸² Unión Internacional de Telecomunicaciones. *Measuring digital development: facts & figures 2019*, 2019. <https://news.itu.int/measuring-digital-development-facts-figures-2019/>

⁸³ Access Now. *#KeepItOn coalition warns internet shutdowns would further hurt Hong Kong*, 2019. <https://www.accessnow.org/internet-shutdowns-will-harm-hong-kong/>

⁸⁴ BBC. *Crisis en Ecuador: continúan las protestas mientras el gobierno y el movimiento indígena se preparan para dialogar este domingo*, 2019. <https://www.bbc.com/mundo/noticias-america-latina-50009459>

⁸⁵ El Espectador. *Movimiento indígena en Ecuador: ¿Por qué continúan las protestas?*, 2019. <https://www.youtube.com/watch?v=6H7EU66Cj3A>

señal telefónica. Debido a las protestas, el gobierno declaró un estado de emergencia, suspendió derechos y estableció medidas de confinamiento. Ante esta situación, los usuarios del proveedor estatal de servicios de Internet y telefonía móvil (Corporación Nacional de Telecomunicaciones) informaron el 6 y 7 de octubre que no podían enviar contenido multimedia a través de Facebook ni WhatsApp, ya que no podían acceder a los servidores de imágenes, audio y video.⁸⁶ Algunos días más tarde, el 12 de octubre, los informes señalaron problemas en la red de Claro que comenzaron en el momento en que se inició el confinamiento.⁸⁷

Etiopía

#OromoProtests

El 29 de junio de 2020, el destacado músico y activista social oromo Haacaaluu Hundeessaa fue asesinado por un atacante desconocido. En respuesta al incidente, se realizaron numerosas protestas en Addis Ababa y otras ciudades de la región de Oromía. Las protestas demandaron justicia para Hundeessaa y, tras aumentar su dimensión, terminaron en enfrentamientos policiales e intervenciones militares.⁸⁸ Al escribir este artículo, se registran al menos 239 personas muertas y 3500 arrestos a raíz de las protestas en contra del gobierno.⁸⁹ En respuesta a esto, el gobierno ordenó un apagón de Internet de alcance nacional con el fin de reprimir los disturbios.⁹⁰ El apagón de Internet presente impide a los periodistas, activistas y otros actores relevantes monitorear e informar las crisis del país de manera adecuada. En el diálogo interactivo final con el Consejo de Derechos Humanos de la ONU, David Kaye, Relator Especial de la ONU, instó al gobierno de Etiopía a "cancelar el apagón de Internet, que refuerza la

⁸⁶ Access Now. *Disrupciones de internet en Ecuador: cómo ocurrieron y cómo eludirlas*, 2019.

<https://www.accessnow.org/disrupciones-de-internet-en-ecuador-como-ocurrieron-y-como-eludirlas/>

⁸⁷ APC, Taller de comunicación mujer, Digital Defenders Partnership, and LaLibre.net. *Derechos digitales en el contexto de las protestas y movilización social en Ecuador en octubre de 2019. Aporte para la Visita de Observación al Ecuador por parte del Relator Especial para la Libertad de Expresión, Edison Lanza y del Comisionado Luis Ernesto Vargas de la Comisión Interamericana de Derechos Humanos (CIDH)*.

https://www.apc.org/sites/default/files/Ecuador_Informe_bloqueos_e_interrupciones_red_octubre2019_CIDH_1.pdf

⁸⁸ Access Now. *#KeptOn: The Ethiopian government must end the arbitrary use of internet shutdowns to quell protests*, 2020.

<https://www.accessnow.org/keepiton-ethiopian-government-must-end-arbitrary-internet-shutdowns/>

⁸⁹ The Washington Post. *Ethiopia's week of unrest sees 239 dead, 3,500 arrested*, 2020.

https://www.washingtonpost.com/world/africa/ethiopias-week-of-unrest-sees-239-dead-3500-arrested/2020/07/08/8eb30952-c100-11ea-8908-68a2b9eae9e0_story.html

⁹⁰ Access Now. *Back in the dark: Ethiopia shuts down internet once again*, 2020.

<https://www.accessnow.org/back-in-the-dark-ethiopia-shuts-down-internet-once-again/>

marginalización y limita el acceso del público a la información en un momento crítico para la salud, la protesta y el debate públicos".⁹¹

India

#CAAProtests #KeepUsOnline #LetTheNetWork

En diciembre de 2019, el gobierno de India suspendió los servicios de datos móviles, banda ancha y llamadas de voz en varios distritos de la capital nacional Delhi, así como en otros estados de India y todo el estado de Assam. Estos apagones inherentemente desproporcionados que afectan los derechos humanos se produjeron cuando las personas tomaron las calles de Delhi para protestar contra la Ley de Enmienda de Ciudadanía (legislación controversial por su supuesta discriminación religiosa que introdujo el parlamento indio por orden del Gobierno de la India) y la propuesta del Registro de Población Nacional.⁹² El gobierno afirma que "la decisión de suspender el acceso a Internet se tomó con el objetivo de evitar el mal uso de las plataformas de medios sociales que pretenda alterar la paz y la tranquilidad y, así, mantener la ley y el orden".⁹³ Los medios indios remarcaron que la orden de comunicación del gobierno que procuraba mantener "la ley y el orden" "no califica como peligro inminente para la tranquilidad pública que sostiene la corte (doméstica) si se restringen derechos fundamentales".⁹⁴ El apagón del estado de Assam fue anulado por la corte suprema estatal.⁹⁵ Investigaciones de la Asociación de Operadores de Celulares de India revelaron que "las operadoras de telefonía móvil de India

⁹¹ Freedex. David Kaye (United Nations Special Rapporteur on Freedom of Expression) - Final reports to Human Rights Council, 2020. <https://freedex.org/2020/07/09/final-reports-to-human-rights-council/>

⁹² Quartz India. Over 4,000 hours of internet shutdowns cost India more than \$1.3 billion in 2019, 2020. <https://qz.com/india/1781178/internet-shutdowns-over-caa-article-370-cost-india-1-3-billion/>; Access Now. *With shutdowns in major cities to silence protests, India tries to black out democracy*, 2019.

<https://www.accessnow.org/with-shutdowns-in-major-cities-to-silence-protests-india-tries-to-black-out-democracy/>; Reuters. *India widens internet shutdown to parts of Delhi to curb protests*, 2019. <https://www.reuters.com/article/us-india-citizenship-mobile-services/india-widens-internet-shutdown-to-parts-of-delhi-to-curb-protests-idUSKBN1YN0MX?il=0>

⁹³ Hindustan Times. *Internet shutdown in many parts including Mangaluru following CAA protests*, 2019. <https://www.hindustantimes.com/india-news/internet-shutdown-continues-in-several-parts-including-mangaluru-ghaziabad-following-anti-citizenship-protests/story-hnPSSj9oGh2AtZw8TQoxaM.html>

⁹⁴ Scroll.in. *Internet shutdowns now reach India's capital - but was the Delhi Police order legal?*, 2019. <https://scroll.in/article/947336/internet-shutdowns-now-reach-indias-capital-but-was-the-delhi-police-order-legal>

⁹⁵ Deccan Herald. *CAA stir: Mobile internet back in Assam after 9 days*, 2019. <https://www.deccanherald.com/national/east-and-northeast/caa-stir-mobile-internet-back-in-assam-after-9-days-787128.html>; Huffpost. *Internet Shutdown: Why Gauhati HC's Order To Restore Mobile Internet In Assam Is Significant*, 2019. https://www.huffingtonpost.in/entry/internet-shutdown-why-gauhati-hcs-order-to-restore-mobile-internet-in-assam-is-significant_in_5dfbd493e4b01834791dbd47

perdían alrededor de 24.5 millones de rupias (USD 350,000) de ingresos por cada hora en que se veían obligadas a suspender los servicios de Internet por órdenes gubernamentales para el control de las protestas".^{96 97} También se estima que, entre 2012 y 2017, las 16.315 horas de la interrupción de Internet en India le costaron cerca de USD 3.040 millones a la economía del país.

Irak

#IraqProtests #INSM_IQ

Tras el comienzo de las protestas masivas en contra del gobierno de Irak en 2019, miles de personas se manifestaron en contra del aumento del desempleo, las interrupciones en los servicios públicos, como cortes de energía prolongados, y la corrupción del gobierno.⁹⁸ Las fuerzas de seguridad que actuaron en respuesta dejaron más de 100 manifestantes muertos y más de 800 heridos, según medios internacionales.⁹⁹ La ola de protestas comenzó en la plaza Tahrir de Bagdad y se extendió a todo el país, con al menos 7 focos en otras provincias. Tras solo unas horas de las protestas iniciales, las autoridades iraquíes bloquearon Facebook, Twitter, WhatsApp, Instagram y otras aplicaciones de mensajería y redes sociales varias veces. A medida que la situación escaló, las autoridades de Irak implementaron un apagón de Internet casi total. También cerraron las oficinas gubernamentales, aplicaron medidas de confinamiento en varias ciudades, desplegaron cientos de unidades de seguridad armadas, arrestaron a cientos de personas y participaron en conflictos durante un período de tiempo extendido, lo que terminó con la vida de varios manifestantes según los informes.¹⁰⁰

⁹⁶ Access Now, *supra*, nota 92; India Today. *Telecoms burnt in CAA, Article 370 fire; lose Rs 24.5 million per hour of internet shutdown*, 2019. <https://www.indiatoday.in/business/story/telecoms-burnt-in-caa-art-370-fire-lose-rs-24-5-million-in-revenue-per-hour-of-internet-shutdown-1632107-2019-12-28>

⁹⁷ Indian Council for Research on International Economic Relations (ICRIER). *The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India*, 2018. https://icrier.org/pdf/Anatomy_of_an_Internet_Blackout_ppt.pdf

⁹⁸ BBC News. *Iraq protests: What's behind the anger?*, 2019. <https://www.bbc.com/news/world-middle-east-49960677>

⁹⁹ CNN. *Death toll rises to 93 in Iraq amid ongoing protests*, 2019. <https://edition.cnn.com/2019/10/03/middleeast/iraq-economic-protests-intl/>

¹⁰⁰ The Guardian. *Internet blackout in Iraq as death toll from violent protests rises*, 2019. <https://www.theguardian.com/world/2019/oct/03/internet-down-across-iraq-third-day-protests>

Sudán

#IAmtheSudanRevolution

Si bien los estados afirman que los apagones de Internet ayudan a mantener la seguridad pública,¹⁰¹ en realidad, facilitan la violación de derechos humanos encubierta. En junio de 2019, el acceso a Internet se interrumpió durante una semana en Sudán. Esa no fue la primera vez que se producía un corte de Internet en el país, pero en esta ocasión fue diferente: evidentemente, el apagón se aplicó para impedir que los manifestantes mostraran, mediante transmisiones en vivo, la matanza y los saqueos organizados y sistemáticos en manos del Consejo Militar Transitorio (TMC). Justo antes de que se interrumpiera el acceso a Internet, el TMC, que había llevado a cabo negociaciones con los grupos opositores para establecer un gobierno civil transitorio, se retiró de dichas negociaciones y envió a la milicia de Yanyauid a atacar violentamente a los manifestantes pacíficos, según indican informes.¹⁰²

Togo

#TogoDebout, #TogoEnMarche

En septiembre de 2017, Togo se unió en protestas para demandar reformas al presidente Faure Gnassingbe, cuyo régimen se llevó la vida de cientos de personas cuando asumió el poder en 2005, tras el reinado de cuatro décadas de su padre. Si bien Gnassingbe realizó el primer apagón de Internet durante las elecciones de 2015, bajo su liderazgo, el gobierno de Togo siguió implementando este tipo de medidas a fin de impedir que los manifestantes organicen marchas.¹⁰³ El 25 de junio de 2020, la Corte Comunitaria de Justicia de la Comunidad Económica de los Estados de África Occidental (ECOWAS) dispuso que el apagón de Internet de septiembre de 2017 ordenado por el gobierno de Togo durante las protestas fue ilegal y una ofensa al derecho de libertad de expresión de los manifestantes. La corte ordenó al gobierno de Togo pagar dos millones de francos CFA a los demandantes a modo de compensación y tomar todas las medidas

¹⁰¹ Africa News. *Ethiopia will cut internet as and when, 'it's neither water nor air' - PM Abiy*, 2019.

[https://www.africanews.com/2019/08/02/ethiopia-will-cut-internet-as-and-when-it-s-neither-water-nor-air-pm-abiy//](https://www.africanews.com/2019/08/02/ethiopia-will-cut-internet-as-and-when-it-s-neither-water-nor-air-pm-abiy/)

¹⁰² The Guardian. *Sudanese doctors say dozens of people raped during sit-in attack*, 2019.

<https://www.theguardian.com/world/2019/jun/11/sudan-troops-protesters-attack-sit-in-rape-khartoum-doctors-report>

¹⁰³ Access Now. *Dispatches from an internet shutdown--Togo*, 2017.

<https://www.accessnow.org/dispatches-internet-shutdown-togo/>

necesarias a fin de garantizar la implementación de salvaguardas para el derecho a la libertad de expresión de los habitantes de Togo.¹⁰⁴

¹⁰⁴ Access Now. *ECOWAS Court upholds digital rights, rules 2017 internet shutdowns in Togo illegal*, 2020. <https://www.accessnow.org/internet-shutdowns-in-togo-illegal/>. Ver también Access Now, *ECOWAS Togo court decision: Internet access is a right that requires protection of the law*, 2020. <https://www.accessnow.org/ecowas-togo-court-decision/>

IV. VIGILANCIA Y DERECHO A LA PRIVACIDAD

La privacidad genera una zona de libertad que es necesaria para promover la organización comunitaria y facilita el ejercicio de los derechos a la libertad de reunión pacífica y asociación. Y lo que es más importante, la privacidad es clave para fortalecer la confianza de las comunidades y los individuos vulnerables y marginados cuando acceden al entorno en línea, especialmente, cuando lo hacen para ejercer su derecho a la protesta. Tal como lo hemos visto en distintas partes del mundo, las tecnologías de vigilancia tienen el potencial de violar la privacidad y otros derechos humanos de millones de individuos y comunidades. Estos derechos son más vulnerables cuando no hay mecanismos de control adecuados para la adquisición y el uso de las tecnologías de vigilancia, ni medidas correctivas para los abusos.¹⁰⁵

Tal como lo explica el Relator Especial de la ONU sobre libertad de expresión, David Kaye, "el discurso anónimo ha sido necesario para los activistas y manifestantes, pero los estados han intentado permanentemente prohibir o interceptar este tipo de comunicaciones en tiempos de protesta".¹⁰⁶ Ya sea mediante tecnologías de reconocimiento facial (FRT) o la interceptación de dispositivos móviles, los derechos a la privacidad y el anonimato de los manifestantes son cada vez más vulnerados durante las protestas. Por ejemplo, "(las FRT) en espacios públicos pueden usarse fácilmente para violar los derechos de privacidad fundamentales de las personas de formas difíciles de remediar".¹⁰⁷ A diferencia de otros datos personales sensibles, como las contraseñas o las claves de seguridad, una persona no puede cambiar su rostro si se hace un mal uso de la información captada o esta resulta comprometida. Si no se aplican salvaguardas adecuadas, las herramientas de vigilancia pública se pueden utilizar para hacer un seguimiento de los movimientos de las personas de un modo que inhiba sus derechos de manifestarse en contextos laborales, asociarse libremente, expresarse y disfrutar del espacio público en eventos deportivos y culturales, entre otros.

No obstante, los manifestantes han desarrollado estrategias creativas para evadir las FRT. Por ejemplo, los participantes de las protestas de Hong Kong han utilizado máscaras, incluso

¹⁰⁵ Access Now. *Argentina province in talks with Huawei over acquiring facial recognition surveillance technology*, 2018. <https://www.accessnow.org/mendoza-surveillance-tech/>

¹⁰⁶ Comité de Derechos Humanos de la ONU, de la ONU. *Informe del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y expresión*, David Kaye, doc. de la ONU A/HRC/29/32 (22 de mayo de 2015). <https://undocs.org/A/HRC/29/32>, párr. 53.

¹⁰⁷ Access Now, *supra*, nota 105.

con el rostro de Guy Fawkes, en caso de que se utilizaran fotos o FRT para identificarlos.¹⁰⁸ Aun así, las tendencias más recientes indican que es relativamente fácil para los sistemas digitales adaptarse a la mayoría de los métodos que utilizan los individuos para eludir la vigilancia. De hecho, debido al uso generalizado de mascarillas faciales para evitar el contagio del COVID-19, "los desarrolladores de reconocimiento facial se adaptan día a día creando bases de datos de imágenes de rostros enmascarados que permiten desarrollar y entrenar algoritmos de identificación y reconocimiento facial, y mejorar las soluciones existentes".¹⁰⁹ Incluso cuando se usan mascarillas, es posible que los sistemas digitales usen otros indicadores, como la forma de caminar, para identificar a los individuos. En consecuencia, los manifestantes utilizan estas técnicas creativas, en parte, porque desconocen qué métodos utilizan las autoridades para identificarlos mediante tecnologías de vigilancia y reconocimiento facial.¹¹⁰

Las herramientas de comunicación son esenciales para hacer un uso seguro y eficiente del derecho a protestar. Esto significa que los servicios de comunicación digital, incluidas las nuevas tecnologías, deben permanecer abiertas y seguras para que todos hagan uso de sus derechos a la libertad de expresión y de reunión pacífica y asociación. La mayor parte de la información personal identificable que se encuentra disponible en línea también puede utilizarse para identificar y rastrear a ciertos individuos, así como detectar e impedir las convocatorias a reuniones, lo cual podría tener un impacto negativo significativo en la libertad de reunión pacífica y asociación. Por lo tanto, aplicar una estrategia sólida de encriptación de extremo a extremo es fundamental para defenderse del acceso ilícito a los datos y proteger a los usuarios, en especial, las comunidades marginadas con mayor riesgo de ser sujetas a vigilancia sin orden judicial.¹¹¹

¹⁰⁸ The Guardian. *Hong Kong's digital battle: tech that helped protestors now used against them*, 2019.
<https://www.theguardian.com/world/2019/jun/14/hong-kongs-digital-battle-technology-that-helped-protesters-now-used-against-them>

¹⁰⁹ GCN. *Facial recognition adapts to a mask-wearing public*, 2020.
<https://gcn.com/articles/2020/06/03/facial-recognition-masks.aspx>

¹¹⁰ BuzzFeed News. *Hong Kong Protesters are Worried About Facial Recognition Technology. But There Are Many Other Ways They're Being Watched*, 2019.
<https://www.buzzfeednews.com/article/rosalindadams/hong-kong-protests-paranoia-facial-recognition-lasers>; The New York Times. *His Face is Unmistakable. It Is the Face of Protest*, 2019.
<https://www.nytimes.com/2019/11/05/opinion/guy-fawkes-day-v-for-vendetta.html>

¹¹¹ Access Now. *195 companies, organizations, and individuals from 42 countries ask world leaders to support strong encryption*, 2016.
<https://www.accessnow.org/195-companies-organizations-and-individuals-from-42-countries-ask-world-leaders-to-support-strong-encryption/>; Access Now. *Access Now joins open letter on Facebook's end-to-end encryption plans*, 2019.
<https://www.accessnow.org/open-letter-facebooks-end-to-end-encryption-plans/>
Access Now. *Lawful Access to Encrypted Data Act would cripple digital security*, 2020.
<https://www.accessnow.org/lawful-access-to-encrypted-data-act-would-cripple-digital-security/>

No obstante, las comunicaciones en línea son fáciles de interceptar para los terceros de corporaciones, estados y otros agentes no estatales. Las tecnologías de vigilancia permiten interceptar comunicaciones de forma masiva. Por ejemplo, los receptores de identidad de suscriptor móvil, también conocidos como "receptores IMSI", son dispositivos invasivos de vigilancia de teléfonos celulares que "imitan las torres de telefonía celular" y envían señales para engañar a los teléfonos móviles a fin de que transmitan su ubicación y datos de identificación".¹¹² Algunos receptores IMSI también pueden interceptar mensajes de texto y grabar conversaciones telefónicas. En el contexto de las reuniones y las asociaciones, el monitoreo de los medios sociales puede implementarse como una medida de vigilancia general (sin adherir a los principios de necesidad o proporcionalidad que establece la ley internacional de derechos humanos) a fin de reprimir el disenso, prever las protestas y justificar medidas arbitrarias como detenciones, penalizaciones, etc. Los estados deben asegurarse de que las leyes, regulaciones, actividades y autoridades relacionadas con la vigilancia satisfagan las leyes y los estándares internacionales de derechos humanos. En 2013, tras una consulta con varias partes interesadas de distintas partes del mundo, una coalición de ONG, que incluye a Access Now, desarrolló los Principios de Necesidad y Proporcionalidad para la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.¹¹³ Los Principios de Necesidad y Proporcionalidad funcionan como un marco de trabajo para que distintas partes interesadas evalúen si las leyes y prácticas de vigilancia existentes o propuestas son coherentes con los derechos humanos. Sin embargo, las medidas que implementan los estados para abordar las actividades ilegales suelen ser generalizadas e innecesarias, y terminan desincentivando la expresión, la reunión y la asociación. Algunos ejemplos de estas medidas incluyen las propuestas de órdenes de retención de datos generales con fines de seguimiento de mensajes privados o la solicitud de identificaciones emitidas por el estado para utilizar redes sociales.¹¹⁴

Adicionalmente, los terceros pueden recopilar y almacenar datos sobre las asociaciones y aquellos que se reúnen tanto en el entorno físico como el digital. Las plataformas de medios sociales pueden vender o compartir esta información con otros terceros, incluidas las autoridades policiales. Para consultar un ejemplo reciente, consulte los informes sobre la *startup* de inteligencia artificial Dataminr, que cuenta con acceso en tiempo real a todas las publicaciones de Twitter. Esta "catarata" de contenido incluye los tuits y los datos de

¹¹² ACLU. *Stingray Tracking Devices*.

<https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices>;
Access Now. *Brazil's Olympic surveillance legacy*, 2016. <https://www.accessnow.org/brazils-olympic-surveillance-legacy/>

¹¹³ Electronic Frontier Foundation. *Necessary & Proportionate: On the Application of Human Rights to Communications Surveillance*, 2014. <https://necessaryandproportionate.org/principles/>

¹¹⁴ Coalizão Diretos na Rede. *Nota da Coalizão Direitos na Rede sobre Aprovação do PL 2630/20 no Senado*, 2020. <http://plfakeweb.direitosnarede.org.br/nota-da-coalizao-sobre-aprovacao-do-pl-2630-20/>

ubicación de los organizadores y participantes de protestas, quienes utilizan Twitter para coordinar y publicar acciones. Recientemente, se descubrió que Dataminr vendió el acceso a datos sobre las protestas de Black Lives Matter tras el asesinato de George Floyd a agencias de seguridad, incluidos los datos de ubicación de los manifestantes pacíficos.¹¹⁵ Esta no es la primera vez en que la policía compra datos de almacenamiento privado sin una orden judicial, lo cual viola las normas y los derechos humanos internacionales.¹¹⁶

Además de los ataques de *phishing* basados en *malware*, hay muchos otros tipos de ataques diseñados para *hackear* las cuentas de redes sociales de los manifestantes (en especial, de los organizadores de las protestas). En estos ataques, se crean cuentas a nombre de los organizadores de las protestas para difundir información falsa o poner en peligro a quienes los siguen. Por ejemplo, el año pasado, nuestra Línea de Ayuda de Seguridad Digital recibió informes de ataques de ingeniería social en Vietnam. Tenían como objetivo distintos perfiles de Facebook pertenecientes a *bloggers* o periodistas que escribían sobre democracia y derechos humanos.¹¹⁷ Nuestra Línea de Ayuda de Seguridad Digital también ha recibido informes de casos de *doxing* (publicación maliciosa de la información personal de una persona, como su dirección o número de teléfono) a fin de promover la realización de daños físicos a los manifestantes o los organizadores de la protesta.¹¹⁸ Además, según las investigaciones realizadas por Citizen Lab, el *spyware* Pegasus de NSO Group se ha utilizado en 45 países, de los cuales, al menos, 6 cuentan con antecedentes de operaciones significativas de Pegasus vinculadas al abuso de este *spyware* para atacar a la sociedad civil, los defensores de los derechos humanos y aquellos que participan en protestas.¹¹⁹

Los programas de identificación digital también afectan los derechos de libertad de reunión pacífica y asociación de los individuos, ya que facilitan la vigilancia por parte del estado mediante la recopilación masiva de datos personales, incluidos los datos biométricos. Por ejemplo, en más de 140 países del mundo, las personas deben brindar información personal

¹¹⁵ The Intercept. *Police Surveilled George Floyd protests with help from Twitter-affiliated startup Dataminr*, 2020.
<https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/>

¹¹⁶ Ver The Daily Beast. *AT&T is spying on Americans for profit*, 2017.
<https://www.thedailybeast.com/atandt-is-spying-on-americans-for-profit>; y las revelaciones anteriores de la colaboración de Dataminr con actividades de inteligencia, en The Wall Street Journal. *Twitter Bars Intelligence Agencies From Using Analytics Service*, 2016.

<https://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682>

¹¹⁷ Access Now. *New Facebook phishing attack taking Vietnamese opposition voices online*, 2018.
<https://www.accessnow.org/vietnam-facebook-phishing-attack-take-opposition-voices-offline/>

¹¹⁸ Access Now. *New wave of online attacks in Nicaragua puts opposition voices at risk of physical violence*, 2018.
<https://www.accessnow.org/new-wave-of-online-attacks-in-nicaragua-puts-opposition-voices-at-risk-of-physical-violence/>

¹¹⁹ The Citizen Lab. *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, 2018.
<https://citizenlab.ca/2018/09/hide-and-see-track-nso-groups-pegasus-spyware-to-operations-in-45-countries/>

para adquirir una tarjeta SIM.¹²⁰ Este registro obligatorio permite a los estados identificar al dueño de cada tarjeta SIM y atribuir comunicaciones a personas específicas. Debido a la falta de anonimato, los manifestantes temen que las autoridades puedan rastrear la identidad de los individuos que usan sus dispositivos móviles para emitir mensajes en contra de las prácticas estatales, o bien para organizar protestas y manifestaciones o participar en ellas.¹²¹ Además de las FRT, el registro obligatorio de las tarjetas SIM puede tener un impacto negativo en la predisposición de los manifestantes para participar en activismo, lo cual paraliza en cierta medida el ejercicio de las libertades de expresión, reunión pacífica y asociación, ya que facilita el monitoreo de los manifestantes y las represalias en su contra. Por lo tanto, el uso de FRT o programas de identificación digital debe satisfacer estándares aún más altos de necesidad y proporcionalidad.¹²²

En medio de la pandemia del COVID-19, mientras las ciudades, regiones y países retoman sus actividades, las autoridades diseñan estrategias para prevenir nuevas olas de contaminación. Una de estas estrategias es el procesamiento de datos de salud de individuos para permitir la identificación de aquellos que pueden o no trasladarse y acceder a distintos espacios, como espacios públicos, mediante certificados de salud digitales.¹²³ Esto implica la administración y autenticación de certificados digitales o pases para permitir el movimiento de personas según su historial de salud. Independientemente de cuáles son los motivos detrás del desarrollo de los certificados de salud digitales, resulta preocupante la posibilidad de que los

¹²⁰ GSMA. *Access to Mobile Services and Proof-of-Identity: Global policy trends, dependencies and risks*, 2018. <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/Access-to-Mobile-Services-and-Proof-of-Identity.pdf>, pág. 39.

¹²¹ GSMA. *The Mandatory Registration of Prepaid SIM Card Users - A White Paper*, 2013. https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2013_WhitePaper_MandatoryRegistrationofPrepaidSIM-Users.pdf, pág. 13. EFF establece que la libertad de asociación puede sufrir un "efecto paralizante" cuando una asociación dedicada a proteger la libertad de expresión se ve obligada a revelar los nombres de sus miembros. *Acorn Investments, Inc. v. City of Seattle*, 887 F.2d 219, 225 (9th Cir. 1989); y que "el efecto 'paralizante' de las regulaciones gubernamentales semejantes a una prohibición directa del ejercicio de los derechos de la Primera Enmienda puede generar violaciones constitucionales". *Laird v. Tatum*, 408 EE.UU. 1, 11 (1972). El Noveno Circuito también estableció que los demandantes pueden establecer un caso de incumplimiento de los derechos de la Primera Enmienda a prima facie si muestran "otros factores que indiquen un 'efecto paralizante' en los derechos de asociación de los miembros". *Brock v. Local 375, Plumbers Int'l Union of Am., AFL-CIO*, 860 F.2d 346, 350 n.1. (9th Cir. 1988). EFF brindó ejemplos específicos en el resumen del programa gubernamental de recolección masiva, que disminuye la cantidad de llamadas y asociaciones entre organizaciones y sus constituyentes, a fin de probar el efecto paralizante que tuvo el programa gubernamental en la libertad de asociación. Ver *First Unitarian Church v NSA* en <https://www.eff.org/cases/first-unitarian-church-los-angeles-v-nsa>.

¹²² Ver ejemplo de Pete Fussey, Daragh Murray. *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. 'The Human Rights, Big Data and Technology Project', University of Essex, Human Rights Centre, 2019. <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf>

¹²³ OMS, "Pasaportes de inmunidad" en el contexto de la COVID-19, 2020. https://apps.who.int/iris/bitstream/handle/10665/331903/WHO-2019-nCoV-Sci_Brief-Immunity_passport-2020.1-spa.pdf

estados usen estos certificados para dificultar el ejercicio de los derechos de los individuos.¹²⁴ Los datos asociados a los certificados de salud digitales pueden usarse como pretexto para impedir que las personas accedan a espacios públicos y hagan uso de sus derechos a la libertad de reunión pacífica y asociación.

El uso de tecnologías de vigilancia por parte de las fuerzas policiales genera preocupaciones a los manifestantes. En los casos de brutalidad policíaca y declaraciones de impunidad, las autoridades han utilizado o consideran equipar a los policías con cámaras corporales a fin de desalentar la violencia policial, promover la transparencia y aumentar la confianza del público. No obstante, esta estrategia también puede desalentar las protestas y manifestaciones debido al miedo de ser identificado y monitoreado por las fuerzas policiales.¹²⁵

El control comunitario sobre la vigilancia policial aumenta día a día. Recientemente, el Consejo Municipal de Nueva York aprobó la Ley de Supervisión de Tecnologías de Vigilancia (POST),¹²⁶ una legislación que requiere que el Departamento de Policía de la Ciudad de Nueva York (NYPD) divulgue las tecnologías de vigilancia que adquiere y utiliza, así como los datos que recopila, y que desarrolle políticas respecto del uso y el impacto de dichos usos.¹²⁷ También establece un control civil sobre las tecnologías de vigilancia que utiliza el NYPD.¹²⁸ La Ley POST sigue una tendencia de esfuerzos legislativos y policiales para controlar el uso de las tecnologías de vigilancia respecto del marco de la ley.¹²⁹

La vigilancia y los riesgos de censura son más graves para quienes sufren marginalización por identidades intersecantes, ya sea de raza, etnia, orientación sexual, religión o de otro tipo. La Asociación para el Progreso de las Comunicaciones (APC) explica que "la vigilancia funcionó históricamente como una herramienta del patriarcado que se utilizaba para controlar y

¹²⁴ EFF. *Immunity Passports Are a Threat to Our Privacy and Information Security*, 2020.

<https://www.eff.org/deeplinks/2020/05/immunity-passports-are-threat-our-privacy-and-information-security>; ACLU.

Coronavirus 'Immunity Passports' are not the Answer, 2020.

<https://www.aclu.org/news/privacy-technology/coronavirus-immunity-passports-are-not-the-answer/>

¹²⁵ ACLU. *Body Cameras and the George Floyd Protests*

<https://www.aclu.org/news/privacy-technology/body-cameras-and-the-george-floyd-protests/>

¹²⁶ Venture Beat. *NYC passes POST Act, requiring police department to reveal surveillance technologies*, 2020.

<https://venturebeat.com/2020/06/18/new-york-city-council-passes-law-requiring-nypd-to-reveal-its-surveillance-technologies/>

∟

¹²⁷ New York City Council. *Creating Civilian Oversight of Police Surveillance*, 2020.

<https://council.nyc.gov/press/2020/06/16/1984/>; New York Times. *Council Forces N.Y.P.D. to Disclose Use of Drones and Other Spy Tech*, 2020. <https://www.nytimes.com/2020/06/18/nyregion/nypd-police-surveillance-technology-vote.html>

¹²⁸ Surveillance Technology Oversight Project (STOP), *Post Act*. <https://www.stopspying.org/post-act>

¹²⁹ ACLU, *Community Control over Police Surveillance*.

<https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance>

restringir el uso de las mujeres de su cuerpo, su discurso y su activismo".¹³⁰ Además, APC remarca que "participar en activismo *queer* o feminista en línea [o] navegar en redes sociales como miembro de una minoría sexual, especialmente si también se pertenece a un grupo racial discriminado, puede tener un gran costo, desde la divulgación involuntaria de la identidad hasta acoso, estigmatización social, violencia y persecución".¹³¹ Por ejemplo, los miembros de la comunidad LGBTQ tienen más probabilidades de recibir ataques mediante violencia y acoso cibernéticos, ser víctimas de censura en línea o ser sujetos de intimidación por divulgación y doxing o de implementaciones orientadas por parte de las autoridades.¹³² El Relator Especial de la ONU sobre libertad de expresión, David Kaye, explica: "Los feeds de noticias basados en IA pueden perpetuar y reforzar actitudes discriminatorias, mientras que los sistemas de IA de perfilamiento y publicidad han demostrado facilitar la discriminación racial, religiosa y de género".¹³³ Por ejemplo, el reconocimiento de género automático (AGR), como parte de las FRT, viola los derechos de las personas trans y de género no binario. Específicamente, "los sistemas de AGR... no logran clasificar a las personas trans o de género no binario como masculino o femenino (lo que significa que las excluyen), o bien les asignan una clasificación incorrecta que no se condice con el género elegido".¹³⁴ Estas instancias de discriminación son especialmente preocupantes cuando las FRT se utilizan para determinar el acceso a edificios o instalaciones, como baños o vestuarios, ya que revelan información y asignan géneros incorrectos a los individuos de forma predeterminada.

CASOS PRÁCTICOS

Si bien Internet creó un nuevo espacio para que los individuos se movilizan en todo el mundo, también se considera "la mayor máquina de espionaje del mundo".¹³⁵ Los terceros, como los estados, corporaciones y agentes ajenos al estado, pueden monitorear y recopilar información sobre las asociaciones y las reuniones de individuos de todo el mundo. Estas técnicas de espionaje no solo socavan los derechos de los individuos a la privacidad y las

¹³⁰ APC. *Feminist Principles of the Internet 2.0*, 2016. <https://www.apc.org/en/pubs/feminist-principles-internet-version-20>

¹³¹ APC. *Providing a gender lens in the digital age: APC Submission to the Office of the High Commissioner for Human Rights Working Group on Business and Human Rights*, 2018. <https://www.ohchr.org/Documents/Issues/Business/Gender/APC.pdf>, pág. 12.

¹³² Access Now, *supra*, nota 25.

¹³³ General Assembly, *Promotion and protection of the right to freedom of opinion and expression - Nota del Secretario General*, doc. de la de la ONU A/73/348 (29 de agosto de 2018). <https://undocs.org/pdf?symbol=en/A/73/348>, párr. 37.

¹³⁴ Access Now. *Facial recognition on trial: emotion and gender 'detection' under scrutiny in a court case in Brazil*, 2020. [https://www.accessnow.org/facial-recognition-on-trial-emotion-and-gender-detection-under-scrutiny-in-a-court-case-in-brasil/](https://www.accessnow.org/facial-recognition-on-trial-emotion-and-gender-detection-under-scrutiny-in-a-court-case-in-brazil/)

¹³⁵ The Hindu. *World's greatest spying machine*, 2011.

<https://www.thehindu.com/opinion/editorial/lsquoWorlds-greatest-spying-machine/article14672829.ece>

libertades expresión, reunión pacífica y asociación, sino que también dañan la confianza que los individuos y asociaciones tienen en el uso de las tecnologías digitales para hacer uso de sus derechos humanos. Los siguientes casos prácticos domésticos destacan algunos aspectos preocupantes de la vigilancia y el derecho a la privacidad.

Azerbaiyán

#etiraz

El gobierno de Azerbaiyán ha suprimido sistemáticamente el disenso y las actividades de protesta mediante violencia, detenciones, arrestos y acciones de intimidación a la sociedad civil.¹³⁶ En 2016, tras un caso inicial que llegó a nuestra Línea de Ayuda de Seguridad Digital, Amnistía Internacional, junto a otras organizaciones, reveló una campaña sistemática de *spear phishing* (a través de un agente de software malicioso personalizado) orientada a periodistas, activistas y defensores de derechos humanos de Azerbaiyán durante 13 meses. Las distintas tácticas empleadas imitaban perfiles de defensores conocidos de derechos humanos y comprometían sus cuentas en línea. En Azerbaiyán, los periodistas, activistas y defensores de derechos humanos con frecuencia sufren ataques de ciberacoso, como "comentarios abusivos y amenazas en redes sociales y comentarios de sitios web, y a través del uso de *trolls* como armas por parte del gobierno".¹³⁷ Investigaciones de Citizen Lab, entre otras, indican que "Azerbaiyán intentó adquirir software invasivo a la compañía italiana Hacking Team".¹³⁸

Brasil

#SemFakeNewsComDireitos

En junio de 2020, el Senado Federal de Brasil aprobó un proyecto de ley que requería la retención de datos de comunicaciones de servicios de mensajería privada a gran escala con la intención de posibilitar el rastreo de mensajes.¹³⁹ Esta peligrosa medida, si se aprueba en la cámara de

¹³⁶ Human Rights Watch. *Azerbaijan's Not-So-Subtle Campaign to Stifle Protest*, 2016.

<https://www.hrw.org/news/2019/10/22/azerbaijan-peaceful-rallies-dispersed-violently>; Human Rights Watch. *Azerbaijan: Peaceful Rallies Dispersed Violently*, 2019.

<https://www.hrw.org/news/2019/10/22/azerbaijan-peaceful-rallies-dispersed-violently>.

¹³⁷ Medium/Amnesty Global Insights. *False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan*, 2017.

<https://medium.com/amnesty-insights/false-friends-how-fake-accounts-and-crude-malware-targeted-dissidents-in-azerbaijan-9b6594cafe60>

¹³⁸ *Ibid.*; The Citizen Lab. *Mapping Hacking Team's 'Untraceable' Spyware*, 2014.

<https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/>

¹³⁹ Coalizão Direitos na Rede, *supra*, nota 114.

representantes, podría representar un riesgo para cualquier grupo de usuarios que se comunique con el fin de organizar acciones políticas pacíficas o formar parte de ellas. Además, los primeros borradores del proyecto de ley incluían una identificación obligatoria para todos los usuarios de redes sociales mediante el documento de identidad nacional y el número de teléfono.¹⁴⁰ Tras recibir una gran ola de críticas, el texto limita los requisitos de identificación a las cuentas que reciban reclamos de otros usuarios, los casos en que haya dudas sobre la autenticidad de una cuenta y las órdenes de la corte. El problema con esta nueva disposición es que cualquier usuario puede presentar un reclamo en la plataforma.¹⁴¹ Este método puede utilizarse para silenciar a los líderes de las manifestaciones, que tal vez quieran permanecer en el anonimato. En el momento de esta publicación, el proyecto de ley espera la segunda y última votación en la Cámara de Representantes de Brasil.¹⁴²

Francia

#technoloplice

En mayo de 2020, ciertos jueces de Francia prohibieron el uso de drones de vigilancia por parte de la policía para supervisar el cumplimiento de las restricciones relacionadas con la pandemia del COVID-19 debido a problemas de privacidad.¹⁴³ Los grupos defensores de las libertades civiles afirmaron que "se filmaba a las personas sin su consentimiento y sin límites de tiempo para el almacenamiento del material registrado".¹⁴⁴ Los jueces dispusieron que "ya no se permite el uso de drones con cámaras hasta tanto no se resuelvan estos asuntos, ya sea mediante una ley de protección de privacidad o con algún tipo de tecnología que impida el reconocimiento de las personas filmadas".¹⁴⁵

¹⁴⁰ Access Now. *Coalition letter: Brazilian disinformation bill threatens freedom of expression and privacy online*, 2020. <https://www.accessnow.org/coalition-letter-brazilian-disinformation-bill-threatens-freedom-of-expression-and-privacy-online/>

¹⁴¹ Coalizão Direitos na Rede, *supra*, nota 114.

¹⁴² Ver ej. Senado Federal. *Lei Brasileira de Responsabilidade e Transparência na Internet*, 2020.

<https://legis.senado.leg.br/sdleg-getter/documento?dm=8128670&ts=1594325280670&disposition=inline>

¹⁴³ Bloomberg. *French Covid-19 Drones Grounded After Privacy Complaint*, 2020.

<https://www.bloomberg.com/news/articles/2020-05-18/paris-police-drones-banned-from-spying-on-virus-violators>

¹⁴⁴ *Ibíd.*

¹⁴⁵ *Ibíd.*

Hong Kong

#FightForHongKong and #HongKongProtest

El 4 de octubre de 2019, mientras las protestas escalaban en toda la ciudad, la jefa ejecutiva de la Región Administrativa Especial de Hong Kong (HKSAR), Carrie Lam, invocó una resolución de la época colonial en la cual se otorgaban poderes extraordinarios para reprimir los disturbios sociales, incluida la prohibición del uso de máscaras. Las autoridades de Hong Kong hace tiempo tienen acceso a FRT y otras herramientas de vigilancia de amplio espectro para identificar y rastrear a las personas. Estas estrategias de las autoridades suponen un alto riesgo para la identidad y la seguridad de los ciudadanos de Hong Kong. Como respuesta, los manifestantes de Hong Kong han utilizado técnicas creativas para limitar su exposición a las medidas de vigilancia y censura del gobierno. Por ejemplo, han mantenido "un perfil bajo en las redes sociales, se comunican solo mediante aplicaciones de mensajería seguras, borran las conversaciones relacionadas con las protestas y usan tarjetas SIM no vinculadas a su información personal".¹⁴⁶ También "utilizan máscaras faciales en caso de que las fotos se usen para identificarlos y se niegan a dar su número de teléfono y detalles de contacto a los periodistas".¹⁴⁷ Estos manifestantes utilizan este tipo de técnicas creativas, en parte, porque desconocen qué métodos utilizan las autoridades para identificarlos mediante tecnologías de vigilancia y reconocimiento facial.¹⁴⁸ Si bien la alta resistencia y la posterior pandemia del COVID-19 eliminaron prácticamente cualquier probabilidad de que se aplicara esta ley en contra del uso de máscaras, el gobierno de Hong Kong y el gobierno central de China tomaron medidas agresivas en 2020 para dismantelar las protestas y el movimiento en favor de la democracia. La Ley de Seguridad Nacional de Hong Kong, que entró en vigencia el 1 de julio de 2020, otorgó a las autoridades amplios poderes para criminalizar el discurso en línea, amplió los poderes de la policía para realizar allanamientos, eliminó radicalmente la supervisión judicial del sistema de vigilancia y aplicó requisitos más estrictos para los proveedores de servicios de Internet.¹⁴⁹

¹⁴⁶ The Guardian, *supra*, nota 108.

¹⁴⁷ *Ibíd.*

¹⁴⁸ Access Now, *supra*, nota 110.

¹⁴⁹ Access Now. *New police powers in Hong Kong threaten human rights online*, 2020.

<https://www.accessnow.org/new-police-powers-in-hong-kong-threaten-human-rights-online/>

India

#CAAProtests #SaveOurPrivacy #NCRB

En diciembre de 2019, un grupo de activistas en India expresaron sus preocupaciones en cuanto a actos ilegales de vigilancia masiva por parte de las autoridades de Delhi durante protestas en contra de la Ley de Enmienda de Ciudadanía y la propuesta del Registro Nacional de Ciudadanos.¹⁵⁰ Muchos manifestantes reportan haber sido objetos de vigilancia masiva mediante drones y cámara de video. Supuestamente, la Policía de Delhi compró software de reconocimiento facial a Innefu Labs, una startup financiada por IndiaNivesh Venture Capital Fund.¹⁵¹ La Agencia Nacional de Registros de Crímenes y el Ministerio del Gobierno de India para los Asuntos Internos han impulsado la aplicación de un "sistema de reconocimiento facial automático" (AFRS) de alcance nacional a pesar de las preocupaciones recurrentes sobre su alcance excesivo y la falta de claridad respecto de sus salvaguardas y supervisión legal.¹⁵² Los abogados locales, que expresan inquietudes en cuanto al uso creciente de tecnologías de vigilancia y la localización de datos obligatoria por parte de las autoridades de India, sugieren que "el uso de tecnologías de reconocimiento facial para perfilar a los ciudadanos podría ser ilegal, ya que no responde a los criterios de privacidad establecidos por la Corte Suprema".¹⁵³ Existe un proyecto de ley de privacidad y protección de datos demorado y pendiente ante un comité parlamentario. Los problemas en su contenido actual respecto de la regulación de la vigilancia y la recopilación de datos a cargo del gobierno generaron críticas por parte del autor asesor original (un juez retirado de la Corte Suprema) basadas en el incumplimiento de los estándares de privacidad y la aplicación de medidas de vigilancia gubernamental con efecto paralizante.¹⁵⁴ En India, la rápida expansión del uso de nuevas tecnologías para vigilar a los manifestantes y grupos de interés público,

¹⁵⁰ The Economic Times. *Activists rally against 'illegal' surveillance of CAA protests*, 2019.

<https://m.economictimes.com/news/politics-and-nation/activists-rally-against-illegal-surveillance-of-caa-protests/articleshow/73039535.cms>

¹⁵¹ *Ibíd.*

¹⁵² The Quint. *Govt Planning Facial Recognition System; Raises Privacy Concerns*, 2019.

<https://www.thequint.com/news/india/ncrb-automated-facial-recognition-system-ministry-of-home-affairs-data-protection-bill-privacy-pending>

¹⁵³ *Ibíd.*

¹⁵⁴ The Wire. *Interview | Dilution of Privacy Bill Makes Govt Surveillance a Cakewalk: Justice Srikrishna*, 2019.

<https://thewire.in/government/interview-justice-srikrishna-privacy>

entre otros, ha generado preocupaciones en cuanto a la vigilancia creciente en la democracia más grande del mundo.¹⁵⁵

Rusia

#Москва #Протест #Выборы

En julio de 2019, miles de personas salieron a las calles de la capital rusa a protestar en contra del rechazo de la participación de candidatos independientes en las elecciones de la Duma de la Ciudad de Moscú de 2019. Las autoridades respondieron con violencia y detuvieron a, al menos, 1373 personas.¹⁵⁶ En respuesta a ello, el 27 de septiembre de 2019, cerca de 20.000 personas se reunieron para demandar la liberación de los manifestantes arrestados en el evento político más grande de Rusia desde las protestas de 2011-2012.¹⁵⁷ Según los activistas, había cámaras de CCTV con sistemas de reconocimiento facial instaladas en la entrada del sitio de la protesta. El político de la oposición Vladimir Milov y la abogada Alena Popova se manifestaron en contra del uso de cámaras para reprimir las protestas en la corte de Moscú, alegando el derecho a la privacidad que establecen la constitución rusa y la Ley de Protección de Datos Personales, la cual prohíbe el procesamiento de datos biométricos sin consentimiento.¹⁵⁸ La corte rechazó el caso basándose en una decisión previa que calificó como lícito el uso de cámaras de reconocimiento facial durante otra protesta.¹⁵⁹ En julio de 2020, Popova y Milov llevaron el caso a la ECtHR.¹⁶⁰

¹⁵⁵ Foreign Affairs. *India's Growing Surveillance State: New Technologies Threaten Freedoms in the World's Largest Democracy*, 2020. <https://www.foreignaffairs.com/articles/india/2020-02-19/indias-growing-surveillance-state>

¹⁵⁶ Radio Free Europe/Radio Liberty. *Blood, Broken Legs, And Mass Detentions: 2019's Moscow Protests*, 2019. <https://www.rferl.org/a/moscow-protests-2019-photos-detentions-blood-broken-legs/30330552.html>

¹⁵⁷ BBC News. *Thousands demand protesters freed in Moscow rally*, 2019. <https://www.bbc.com/news/world-europe-49871901>

¹⁵⁸ Коммерсантъ. *Милов подал иск к московским властям и ГУВД из-за технологии распознавания лиц*, 2020. <https://www.kommersant.ru/doc/4227471>

¹⁵⁹ Роскомсвобода. *Иск о незаконном использовании технологии распознавания лиц в Москве отклонён судом*, 2020. <https://roskomsvoboda.org/55974/>

¹⁶⁰ Human Rights Watch. *Moscow's Use of Facial Recognition Technology Challenged*, 2020. <https://www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged>

Estados Unidos

#BlackLivesMatter and Standing Rock #NoDAPL

El 31 de mayo de 2020, tras las protestas de alcance nacional, el fiscal general William Barr describió el movimiento Antifa y a otros activistas antifascistas como "terroristas domésticos". Además, advirtió que la supuesta violencia por parte de Antifa y los demás movimientos se tratará como terrorismo doméstico. El 19 de junio de 2020, expertos independientes de la ONU expresaron grandes preocupaciones respecto de estas declaraciones argumentando que restringen los derechos a las libertades de expresión y reunión pacífica en el país.¹⁶¹ La reciente ronda de protestas de Black Lives Matter expuso el uso de herramientas de vigilancia para monitorear acciones políticas lícitas por parte de autoridades, que comprenden desde la policía local hasta el gobierno federal. Numerosos ejemplos muestran la readaptación de herramientas implementadas con otros propósitos: el Departamento de Seguridad Interna utiliza drones, aviones y helicópteros adquiridos con fines de protección de las fronteras y aduanas para monitorear las protestas de Black Lives Matter en más de 15 ciudades;¹⁶² y las filmaciones capturadas por los "semáforos inteligentes" de San Diego, instalados para supervisar el tráfico y las condiciones climáticas,¹⁶³ se usan para asistir la persecución de los manifestantes.¹⁶⁴

Asimismo, cuando las comunidades indígenas protestaban contra la instalación del Oleoducto para el Acceso a las Dakotas (Dakota Access Pipeline, DAPL), que representaba una amenaza para las tierras sagradas y el suministro de agua a la reserva Standing Rock, encontraron controles aéreos de helicópteros y otras formas de vigilancia directa. Cuando se corrió la voz de que la policía monitoreaba la función de registro de visitas de Facebook para identificar a los individuos que participaban en la protesta, más de un millón de personas de todo el mundo registraron visitas en el lugar para expresar su solidaridad y, potencialmente, defender a los manifestantes.¹⁶⁵

¹⁶¹ OHCHR. *UN experts decry US rhetoric on designation of terrorist groups*, 2020.

<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25980&LangID=E>

¹⁶² The New York Times. *U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance*, 2020.

<https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html>

¹⁶³ The City of San Diego. *San Diego to Deploy World's Largest City-Based 'Internet of Things' Platform Using Smart Streetlights*, 2017. <https://www.sandiego.gov/mayor/news/releases/san-diego-deploy-world%E2%80%99s-largest-city-based-%E2%80%99internet-things%E2%80%99-platform-using-smart>

¹⁶⁴ Mashable. *Police used 'smart streetlights' to surveil protesters, just as privacy groups warned*, 2020.

<https://mashable.com/article/police-surveil-black-lives-matter-protesters-smart-streetlights/>; Access Now. *Standing with #BlackLivesMatter -- for human rights, for justice, and for democracy*, 2020.

<https://www.accessnow.org/standing-with-black-lives-matter/>

¹⁶⁵ The Guardian. *A million people 'check in' at Standing Rock on Facebook to support Dakota pipeline protesters*, 2016.

<https://www.theguardian.com/us-news/2016/oct/31/north-dakota-access-pipeline-protest-mass-facebook-check-in>

V. LA INFLUENCIA DEL SECTOR PRIVADO EN EL ESPACIO CÍVICO EN LÍNEA

El sector privado cumple un rol fundamental en el respeto y el respaldo de los derechos a la libertad de reunión pacífica y asociación en la era digital. Desde empresas de telecomunicaciones hasta plataformas en línea, las compañías de tecnología controlan dónde las personas hacen uso de sus derechos. Las empresas privadas aprovechan los protocolos y la infraestructura desarrollados a través de décadas de inversiones del sector público y desarrollo académico. Pero incluso los servicios públicos y los sistemas educativos se vieron obligados a migrar al entorno en línea durante la pandemia del COVID-19, lo que provocó un aceleramiento de la "digitalización masiva", que muchas veces es privatización masiva. El sector de la tecnología se beneficia de estas nuevas bases de usuarios, pero también sacrifica los derechos a la libertad de reunión pacífica y asociación al priorizar sus ingresos, perpetrar tendencias monopólicas y fomentar políticas discriminatorias (sin rectificación ni revisión), entre otros factores que suelen acompañar la privatización.

Los estados ceden el acceso a los datos con demasiada facilidad debido a la falta de regulación, la corrupción o incluso las buenas intenciones. Los expertos en derechos humanos desaprueban "los esfuerzos por 'privatizar' las estrategias de control mediante la presión a los intermediarios para que tomen medidas", si los estados ceden las funciones tradicionalmente públicas a agentes privados.¹⁶⁶ Además, dado que poseen grandes cantidades de información, las empresas de tecnología reciben, con frecuencia, solicitudes y presión de los estados para acceder a los datos de los usuarios, eliminar o restringir cuentas o tomar una serie de medidas para satisfacer necesidades del estado. A su vez, estas empresas enfrentan obligaciones domésticas e internacionales que compiten por tener prioridad y que "ponen en riesgo el cumplimiento de los derechos humanos así como su posibilidad de operar en ciertas jurisdicciones".¹⁶⁷ Esto, muchas veces, conduce a la violación de los derechos de los usuarios, incluidos los derechos a la libertad de reunión pacífica y asociación, a fin de cumplir con las apremiantes demandas de los estados.

A estas prácticas corporativas sin rendición de cuentas se les suma la falta de divulgación de información adecuada por parte de las empresas sobre el impacto en los derechos humanos. Si bien, en algunas jurisdicciones, la divulgación de detalles sobre las solicitudes de los

¹⁶⁶ OAS, IACHR. *Joint Declaration on Freedom of Expression and 'Fake News,' Disinformation and Propaganda*, 2017. <http://www.oas.org/en/iachr/expression/showarticle.asp?artID=1056&IID=1>

¹⁶⁷ Clément Voule, *supra*, nota 48, párr. 58.

estados puede encontrarse restringida o prohibida a nivel legal, en muchos casos, las empresas aún pueden ofrecer un nivel básico de rendición de cuentas mediante "informes de transparencia".¹⁶⁸ El Relator Especial de la ONU sobre libertad de reunión pacífica y asociación, Clément Voule, explica que "distintas empresas de todo el mundo no divulgan información adecuada sobre la recopilación de datos y las solicitudes de los gobiernos", lo cual genera dudas respecto de la transparencia y la rendición de cuentas de las corporaciones.¹⁶⁹

CAMPAÑA #SAVEDOTORG

La falta de transparencia y rendición de cuentas por parte de las corporaciones es precisamente el motivo por el cual cientos de organizaciones de la sociedad civil de todo el mundo se unieron para salvar el dominio ".ORG" de manos privadas. En noviembre de 2019, la sociedad civil se manifestó tanto en línea como en el mundo real (principalmente en un encuentro espontáneo en el Foro de Gobernanza de Internet¹⁷⁰) a fin de recurrir a los líderes de Internet Society (ISOC) y la Corporación de Internet para la Asignación de Nombres y Números (ICANN) para impedir la venta del dominio superior .ORG a la firma de capital privado Ethos Capital. El dominio .ORG es el entorno en el que residen la sociedad civil y las ONG en el entorno digital. Es un "sitio de encuentro" fundamental para la sociedad civil y las ONG, ya que tanto el mundo físico como el virtual se han vuelto cada vez más inhóspitos y peligrosos para las organizaciones que afrontan situaciones constantes de vigilancia, censura en línea e incluso riesgos físicos y restricciones legales para sus operaciones y su personal. La propuesta de venta (que finalmente fue suprimida) representaba un peligro adicional para la seguridad y la estabilidad del espacio digital de numerosas ONG, sus socios y sus comunidades.¹⁷¹ Consejo de Derechos Humanos Relatores Especiales de la ONU David Kaye y Clément Voule avalaron las preocupaciones de la sociedad civil respecto de la propuesta de venta de .ORG en una carta conjunta dirigida a ICANN.¹⁷² Además, destacaron las implicancias de la propuesta en los derechos humanos, incluida la importancia de que "las organizaciones

¹⁶⁸ Access Now. *Transparency Reporting Index*. <https://www.accessnow.org/transparency-reporting-index/>

¹⁶⁹ Clément Voule, *supra*, nota 48, párr. 58.

¹⁷⁰ Access Now. *Access Now calls on Internet Society to halt the sale of .ORG*, 2019.

<https://www.accessnow.org/access-now-calls-on-icann-and-internet-society-to-halt-the-sale-of-org/>

¹⁷¹ Access Now. *Letter to ISOC and ICANN*, 2020. <https://www.accessnow.org/dot-org-civil-society-letter/>; BuzzFeed News. *A Private Equity Firm Is Trying to Buy the .Org Domain. Now, Greenpeace, the ACLU, and Color of Change Are Protesting*, 2020. <https://www.buzzfeednews.com/article/alexkantrowitz/a-private-equity-firm-is-trying-to-buy-the-org-domain-now>

¹⁷² David Kaye (Relator Especial de la ONU sobre libertad de expresión), Clément Voule (Relator Especial de la ONU sobre libertad de reunión y asociación). *Letter to ICANN - Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, 2019. <https://www.icann.org/en/system/files/correspondence/kaye-voule-to-marby-20dec19-en.pdf>

de la sociedad civil tengan un espacio en línea que no esté sujeto a las presiones de un entorno comercial, que podrían silenciarlas fácilmente".¹⁷³

El 30 de abril de 2020, la Junta Directiva de ICANN respondió a la ola de oposición rechazando el cambio del control del dominio .ORG.¹⁷⁴ Si bien la sociedad civil celebró la suspensión de la venta a Ethos Capital, aún hay preocupaciones respecto de "la forma unilateral en que la Junta Directiva de ISOC decidió la venta de .ORG de forma confidencial en cuestión de semanas".¹⁷⁵ En una carta reciente de seguimiento dirigida a ISOC y los líderes de Public Interest Registry, la sociedad civil emitió una declaración en la que reitera una solicitud de dos partes: (1) enmendar el acuerdo de registro de .ORG a fin de incluir protecciones vitales para los derechos humanos y el interés público y (2) tomar medidas concretas para restablecer la confianza en la propiedad existente de .ORG y evitar este tipo de amenazas en el futuro.¹⁷⁶

INFORMES DE TRANSPARENCIA

Generar informes de transparencia regularmente es una de las mejores medidas que pueden adoptar las empresas para comunicar a sus usuarios y el público las estrategias que adoptan a fin de respetar los derechos humanos. Los informes de transparencia cumplen tres funciones principales: (1) brindar una descripción general las operaciones de la empresa que afectan específicamente la privacidad y la libertad de expresión, (2) brindar detalles sobre la aplicación de reglas internas, como los términos de servicio y los lineamientos para la comunidad, y (3) divulgar estadísticas originales sobre las solicitudes de datos de usuarios y restricciones de cuentas y contenidos por parte de terceros y los estados.¹⁷⁷ Los informes de transparencia son esenciales por varios motivos. En primer lugar, proporcionan un mecanismo eficaz para que las empresas divulguen las amenazas a la privacidad de los usuarios y la libertad de expresión. En segundo lugar, funcionan como un recurso esencial para orientar las decisiones de los inversores y respaldar sus acciones en pro de los derechos humanos. Los informes de transparencia son un indicador clave en los "análisis de seguridad y riesgos para los estados, las empresas, las organizaciones y los individuos que buscan adoptar nuevas herramientas, servicios o plataformas".¹⁷⁸ De hecho, a medida que la

¹⁷³ *Ibíd.*

¹⁷⁴ ICANN. *Approved Board Resolutions | Special Meeting of the ICANN Board*, 2020. <https://www.icann.org/resources/board-material/resolutions-2020-04-30-en>

¹⁷⁵ Save Dot Org. *Letter to the Internet Society and Public Interest Registry leadership*, 2020. <https://savedotorg.org/>

¹⁷⁶ *Ibíd.* Public Interest Registry es la organización que se dedica a administrar y operar el dominio .ORG y es propiedad de ISOC.

¹⁷⁷ Access Now. *The what, why, and who of transparency reporting*, 2020.

<https://www.accessnow.org/the-what-why-and-who-of-transparency-reporting/>

¹⁷⁸ *Ibíd.*

pandemia del COVID-19 aceleró la migración de las operaciones y las comunidad global al entorno en línea, la ONU se vio obligada a evaluar sus propias asociaciones público-privadas tras fuertes críticas en torno a la falta de transparencia en el proceso de adquisición y el riesgo que suponen ciertos socios del sector privado para los derechos digitales.¹⁷⁹ Esto fue un importante llamado de alerta para la ONU, una organización internacional con un gran atraso en lo que respecta a garantizar la seguridad digital de las plataformas, pero que avanza para ponerse al día mediante iniciativas como la estrategia de datos del Secretario General de las Naciones Unidas.¹⁸⁰ Como resultado de una crisis global en la que prácticamente todos los aspectos de nuestra vida se desarrollan en línea, las empresas de tecnología han obtenido un gran crecimiento en sus bases de usuarios.¹⁸¹ La necesidad y el uso cada vez más generalizado de los servicios y plataformas en línea permiten a estas empresas tener una influencia desmedida sobre cómo vivimos nuestras vidas. Esta influencia es más notoria en el contexto de la pandemia, dado que las reuniones y asociaciones han redefinido y adaptado sus estrategias durante este período. Este poder trae aparejada la responsabilidad de respetar los derechos humanos.

REGULACIÓN DEL DISCURSO

Conforme a las normas internacionales y los Principios Rectores sobre las Empresas y los Derechos Humanos (UNGP) de la ONU, las empresas tienen la responsabilidad específica de respetar todos los derechos humanos, incluido el derecho a la no discriminación.¹⁸² Y lo que es más importante, estas entidades podrían afrontar obligaciones internacionales aún más estrictas con el tratado vinculante propuesto por la ONU acerca de los regímenes de diligencia debida para corporaciones transnacionales y derechos humanos obligatorios, que se encuentra en proceso.¹⁸³ En general, estas políticas y prácticas de las empresas de tecnología, incluido su poder de decidir qué voces se amplifican y cuáles se silencian, tienen un impacto directo en los derechos a la libertad de reunión pacífica y asociación. Por ejemplo, tal como lo explica la organizadora feminista Nadine Moawad, "cuando Google

¹⁷⁹ Access Now. *U.N. backs down on partnership with Tencent*, 2020.

<https://www.accessnow.org/un-backs-down-on-partnership-with-tencent/>

¹⁸⁰ Estrategia de datos del Secretario General de las Naciones Unidas.

<https://www.un.org/en/content/datastrategy/index.shtml>

¹⁸¹ Access Now, *supra*, nota 177; Apptopia. *Top iOS Apps: Free app store rank data for iTunes Connect*, 2020.

<https://apptopia.com/store-insights/top-charts/itunes-connect/top-overall/united-states>

¹⁸² Más adelante, la Resolución de Internet del Consejo de Derechos Humanos de las Naciones Unidas de 2018 "motiva a las empresas a trabajar para ofrecer soluciones técnicas que ayuden a proteger la confidencialidad de las comunicaciones digitales, las cuales pueden incluir medidas de encriptación y anonimato y solicitudes a los estados para que no interfieran en el uso de dichas soluciones técnicas, y que las restricciones correspondientes satisfagan las obligaciones del Estado conforme a las leyes internacionales de derechos humanos". Ver Consejo de Derechos Humanos de la ONU, *supra*, nota 43.

¹⁸³ Access Now. *Revised draft U.N. treaty on business and human rights: a few steps forward, a few unanswered questions*, 2019. <https://www.accessnow.org/revised-draft-u-n-treaty-on-business-and-human-rights-a-few-steps-forward-a-few-unanswered-questions/>

eligió alterar su logotipo temporalmente con un *doodle* que mostraba los colores del arco iris para los Juegos Olímpicos de Sochi, expresó un interés corporativo en los derechos de la comunidad LGBT[Q]... No obstante, a diferencia de una bandera con los colores del arco iris, otras formas de discurso sexual tienen menos aceptación... por ejemplo, en la prohibición de Facebook de los pezones femeninos durante la protesta de desnudos de Black Lives Matter en San Francisco.¹⁸⁴ Las redes sociales y otras plataformas deben tomar medidas respecto de las barreras sistémicas a fin de satisfacer realmente las necesidades y los intereses de todos sus usuarios. La investigadora de tecnología Maya Indira Ganesh propone el siguiente planteo: "¿cómo podemos redefinir el rol de estas plataformas y empresas cuando se atribuyen brindar su respaldo a revueltas de todo el mundo, pero no rinden cuentas frente a sus usuarios por la regulación del discurso?"¹⁸⁵.

Las redes sociales se denominan frecuentemente la "nueva plaza pública", una simplificación que oculta la idea de una realidad cambiante y variada. En 2011, durante la Primavera Árabe, esta función de las empresas de redes sociales fue extremadamente útil para las relaciones públicas y la imagen general de los manifestantes. No obstante, ahora muchos activistas no pueden confiar en estas plataformas para documentar las violaciones a los derechos humanos, organizarse ni desarrollar campañas en favor de estos debido a las políticas de moderación de contenido.¹⁸⁶ Facebook y su familia de empresas (Instagram, Messenger y WhatsApp) definitivamente dominan el discurso de los grupos de todos los tamaños y formas, desde grupos de amigos y familiares hasta corporaciones, grupos religiosos, deportivos y de entretenimiento y agrupaciones con otros intereses. Para cuantificar su alcance, se requieren datos proporcionados por la empresa; en los últimos 18 meses, Facebook informó más de 10 millones de grupos "con 1.400 millones de personas involucradas cada mes" y cerca de 3 mil millones de usuarios activos.¹⁸⁷ La centralidad de la firma con respecto al ejercicio de la libertad de reunión pacífica y asociación no es un hecho menor.

¹⁸⁴ Nadine Moawad. *One and the Other: Fighting Online Misogyny, Fighting a Corporatised Internet*, ARROW for Change: Sexuality, Sexual and Reproductive Health and Rights, and the Internet 22, No 1 (2016): 8. https://www.apc.org/sites/default/files/AFC22.1-2016_0.pdf, pág. 8.

¹⁸⁵ Maya Indira Ganesh. *The New Green: The Landscapes of Digital Activism*, ARROW for Change: Sexuality, Sexual and Reproductive Health and Rights, and the Internet 22, No 1 (2016): 8. https://www.apc.org/sites/default/files/AFC22.1-2016_0.pdf, pág. 4.

¹⁸⁶ Ver, p. ej., Pete Fussey, Daragh Murray, *supra*, nota 122; NBC News. 'Facebook doesn't care': Activists say accounts removed despite Zuckerberg's free-speech stance, 2020. <https://www.nbcnews.com/tech/tech-news/facebook-doesn-t-care-activists-say-accounts-removed-despite-zuckerberg-n1231110>

¹⁸⁷ Facebook for Business. *Gen Z: Getting to Know the 'Me Is We' Generation*, 2019. <https://www.facebook.com/business/news/insights/generation-z>; VentureBeat. *Facebook apps now used monthly by more than 3 billion people*, 2020. <https://venturebeat.com/2020/04/29/facebook-earnings-q1-2020/>

A pesar de la gobernanza centralizada de la empresa, en la que Mark Zuckerberg es el mayor accionista, líder de la junta directiva y director general, el impacto y el enfoque de Facebook no han sido consistentes. Facebook ha respondido previamente al Centro de Información sobre Empresas y Derechos Humanos por las alegaciones de la sociedad civil en cuanto al rol de la plataforma en la propagación del discurso de odio y la facilitación de la violencia en Sri Lanka.¹⁸⁸ La compañía reiteró su compromiso con el abordaje de estos desafíos y la implementación y mejora de sus políticas mediante la interacción con sus socios. También presentó un informe sobre las evaluaciones del impacto en los derechos humanos en Sri Lanka, Indonesia y Cambodia.¹⁸⁹ Sin embargo, el progreso de Facebook con respecto a estos problemas ha sido insignificante en otras partes del mundo. En mayo de 2020, los senadores de EE.UU. le escribieron una carta al director general de Facebook, Mark Zuckerberg, en la que expresaban sus preocupaciones respecto de la política de la empresa en cuanto a la desinformación, en particular, considerando las elecciones presidenciales de EE.UU. que se avecinaban.¹⁹⁰ Las partes interesadas manifestaron otros riesgos similares a la empresa recientemente, durante la Reunión General Anual de Facebook de 2020.¹⁹¹ Incrementar el diálogo entre las plataformas de medios sociales y los grupos de la sociedad civil en distintas regiones podría ayudar a comprender mejor y abordar las manifestaciones de violencia en el espacio digital, pero es posible que se necesiten cambios estructurales para lograr un progreso real en favor del respeto por los derechos humanos en el grupo de empresas de Facebook.

CASOS PRÁCTICOS

Las motivaciones basadas en ganancias y las tendencias corporativas en torno a la privatización tienen un alto costo para aquellos que promueven los derechos a la libertad de reunión pacífica y asociación. Los siguientes casos prácticos domésticos destacan algunas de las medidas que han tomado las empresas de tecnología con respecto a los defensores de los

¹⁸⁸ Business and Human Rights Resource Centre. *Facebook response re allegations regarding Facebook's role in amplifying hate speech and facilitating violence in Sri Lanka, as well as its role generally with exacerbating the spread of false information*, 2018.

https://www.business-humanrights.org/sites/default/files/documents/Facebook%20response_19%20Nov%202018.pdf

¹⁸⁹ Facebook. *An Update on Facebook's Human Rights Work in Asia and Around the World*, 2020.

<https://about.fb.com/news/2020/05/human-rights-work-in-asia/>

¹⁹⁰ Bob Menendez Senate. *Menendez, Harris, Blumenthal, Blast Facebook's Continued Failure to Protect Users from Hate Speech and Misinformation*, 2020.

<https://www.menendez.senate.gov/news-and-events/press/menendez-harris-blumenthal-blast-facebooks-continued-failure-to-protect-users-from-hate-speech-and-misinformation>

¹⁹¹ OpenMIC. *Senators ask Facebook's Zuckerberg to address civil and human rights concerns ahead of 2020 election*, 2020.

<https://www.openmic.org/news/facebook-civil-rights-letter-from-senators-menendez-harris-blumenthal>

derechos humanos, los activistas, los movimientos obreros y el disenso en general, tanto en línea como en el entorno físico.

**Activision
Blizzard
Hong Kong** En octubre de 2019, la empresa de videojuegos Activision Blizzard penalizó a un jugador profesional de Hong Kong por expresar su apoyo a las protestas de Hong Kong durante una transmisión en línea en vivo.¹⁹² Si bien, posteriormente, la empresa redujo las penalizaciones, el incidente puso de manifiesto la amplia variedad de espacios en línea que presentan riesgos para el derecho a la protesta.

**Whole Foods
(Amazon)
Estados Unidos** Documentos internos revelaron que el supermercado propiedad de Amazon Whole Foods utiliza mapas de calor interactivos para supervisar sus tiendas en todo el mundo.¹⁹³ La cadena también asigna a cada tienda un puntaje de riesgo de sindicalización basado en los datos demográficos de los empleados y el bienestar socioeconómico general de la comunidad. Estas iniciativas de vigilancia en contra de la sindicalización podrían tener un impacto negativo en los casi 95.000 empleados de Whole Foods, ya que permiten a sus empleadores predecir qué etnias y clases sociales tienen más probabilidades de sindicalizarse, lo cual aumenta el riesgo de discriminación en el proceso de contratación.

¹⁹² Access Now. *Blizzard must demonstrate its commitment to respecting the human rights of its users*, 2019. <https://www.accessnow.org/blizzard-must-demonstrate-its-commitment-to-respecting-the-human-rights-of-its-users/>

¹⁹³ Observer. *Whole Foods Secretly Upgrades Tech to Target and Squash Unionizing Efforts*, 2020. <https://observer.com/2020/04/amazon-whole-foods-anti-union-technology-heat-map/>

Twitter

Egipto

En septiembre de 2019, estallaron en todo el país las manifestaciones en contra del presidente de Egipto, Abdel Fattah el-Sisi.¹⁹⁴ Los egipcios utilizaron Twitter, Facebook y otras plataformas de medios sociales para publicar comentarios sobre las protestas. El gobierno respondió con arrestos y bloqueos de los sitios web y medios independientes.¹⁹⁵ Además, Twitter comenzó a suspender las cuentas que publicaban críticas explícitas al gobierno. Se suspendieron las cuentas de más de 100 activistas, incluidas las del activista de derechos humanos Hend Nafea, el artista Ganzeer y el periodista Ahmad Hasan al-Sharqawi.¹⁹⁶ Twitter luego pidió disculpas por esta medida.¹⁹⁷ Muchas de las cuentas suspendidas publicaron palabras específicas en árabe características de un contexto sociopolítico crítico del gobierno del presidente Sisi; el algoritmo de Twitter calificó estos términos como "manipuladores".¹⁹⁸ Los activistas afirman que este incidente demuestra que o Twitter no cuenta con suficientes moderadores humanos que supervisen las redes en árabe, o bien se realizaron informes masivos intencionales de ciertas cuentas para reprimir las voces disidentes durante las protestas.¹⁹⁹

¹⁹⁴ The New York Times. *Rare Protests Against Egypt's Leader Erupt in Cairo and Elsewhere*, 2019. <https://www.nytimes.com/2019/09/20/world/middleeast/anti-government-protests-egypt.html>

¹⁹⁵ The New York Times. *In Egypt, Scattered Protests Break Out for Second Week*, 2019. <https://www.nytimes.com/2019/09/27/world/middleeast/egypt-protests.html>

¹⁹⁶ Middle East Eye. *Egyptian activists sound alarm over Twitter account suspensions*, 2019. <https://www.middleeasteye.net/news/egyptian-activists-sound-alarm-over-twitter-account-suspensions>

¹⁹⁷ BuzzFeed News. *Twitter "Silenced" Dissenting Voices During Anti-Government Protests In Egypt*, 2019. <https://www.buzzfeednews.com/article/meghara/twitter-egypt-protests-accounts-suspended>

¹⁹⁸ Middle East Eye, *supra*, nota 196.

¹⁹⁹ *Ibíd.*

VI. RECOMENDACIONES PARA LAS POLÍTICAS PÚBLICAS

Ahora, más que nunca, el contexto global requiere que todas las partes interesadas renueven su compromiso con la protección, el respeto y el restablecimiento de los derechos a la libertad de reunión pacífica y asociación tanto en el entorno físico como digital. Según el análisis anterior, es evidente que estos derechos, en particular, no cuentan con suficiente desarrollo para sostenerse en el contexto digital cambiante actual. No obstante, diversos expertos en derechos humanos internacionales, como algunos Relatores Especiales de la ONU y los miembros de la OHCHR, actualmente, examinan y evalúan cada vez más de cerca la intersección de los derechos humanos y las tecnologías digitales, incluidos los derechos a la libertad de reunión pacífica y asociación.²⁰⁰ Las siguientes recomendaciones se basan en dichos esfuerzos con el fin de amplificar el llamado a la acción a las partes interesadas para que sostengan estos derechos en la era digital.

RECOMENDACIONES PARA LOS ESTADOS

General

1. Proteger y promover los derechos a la libertad de reunión pacífica y asociación, incluso en los contextos de crisis.
2. Garantizar el acceso universal a las TIC, que es esencial para el ejercicio de los derechos a la libertad de reunión y asociación pacíficas en la era digital.
3. Reconocer y proteger el derecho a la protesta incluso en los espacios digitales, ya sean de propiedad y administración pública o privada.

Apagones de Internet, acceso y conectividad

1. Cumplir con las obligaciones internacionales de proteger los derechos a las libertades de reunión pacífica y asociación, la expresión y el acceso a la información, permitiendo a los manifestantes reunirse tanto en el entorno físico como digital, garantizando que el acceso a Internet no se encuentre bloqueado, limitado o interrumpido y asegurando que los medios puedan funcionar libremente.
2. Priorizar la financiación del desarrollo digital y reasignar los fondos existentes a la creación de una infraestructura digital inclusiva, particularmente en los contextos de crisis.
3. Adoptar e implementar un enfoque basado en los derechos humanos que integre los derechos civiles y políticos con los derechos económicos, sociales y culturales a fin de cerrar las brechas digitales y garantizar que todos puedan hacer uso de su derecho a la libertad de reunión pacífica y asociación tanto en el entorno físico como el digital.

²⁰⁰ Ver, p. ej., OHCHR. *New technologies must serve, not hinder, right to peaceful protest, Bachelet tells States*, 2020. <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=E>

Vigilancia y derecho a la privacidad

1. Evitar emplear o invertir en tecnologías que utilicen análisis biométricos para identificar a quienes participan de forma pacífica en reuniones, incluidas, entre otras, las tecnologías de reconocimiento facial, de voz y del movimiento.
2. Considerar el impacto que el uso de los sistemas de inteligencia artificial y aprendizaje automático en la moderación y curación de contenido puede tener sobre los derechos a la libertad de reunión pacífica y asociación, en especial, en contextos en que estas libertades son difíciles de ejercer en línea.
3. Regular estrictamente el uso de las tecnologías de reconocimiento facial. En particular, establecer limitaciones claras para su utilización y requerir transparencia pública a fin de proteger el ejercicio efectivo del derecho a la reunión pacífica.
4. Prohibir el uso de tecnologías de vigilancia, en particular, los sistemas de vigilancia masiva basados en identificadores biométricos, para la vigilancia indiscriminada e injustificada de los individuos que ejercen su derecho a la reunión pacífica.
5. Tomar todas las medidas posibles para supervisar y prevenir la venta y el uso de tecnologías de vigilancia masiva (incluidos los programas espía y el malware orientado) para monitorear a los manifestantes y otros individuos que hagan uso de sus derechos.
6. Proteger el imperio de la ley y garantizar que los acuerdos de intercambio de datos entre los estados y las empresas se basen en la ley.
7. Aplicar leyes y principios de privacidad y protección de datos que garanticen, en particular, que la aplicación de la ley no otorgará acceso a los datos personales almacenados por agentes públicos o privados sin una orden judicial o de autoridad competente. Cumplir con los 13 Principios de Necesidad y Proporcionalidad y aplicar las leyes de derechos humanos para la vigilancia de las comunicaciones.
8. Proteger y promover las tecnologías que mejoran la privacidad y defender el uso de encriptación, alias y anonimato, que son esenciales para el respeto por los derechos humanos.
9. Garantizar el respeto por los derechos de privacidad y protección de datos en los casos de abuso por parte de agentes privados.
10. Implementar evaluaciones oportunas, accesibles y públicas del impacto en los derechos humanos, así como procesos de debida diligencia de carácter obligatorio, en todas las asociaciones de entidades públicas y privadas y las contrataciones públicas.
11. Investigar adecuadamente los incidentes policiales y otros tipos de brutalidad o uso excesivo de fuerza, divulgar los resultados, incluidas las filmaciones de vigilancia, y llevar los responsables a la justicia, acorde con los estándares internacionales.
12. Prevenir y procesar las represalias en contra de aquellos que documentan protestas, manifestaciones y otras reuniones, y diseminan dicha información a través de medios digitales.
13. No integrar programas de identificación digital, incluidos certificados de salud digitales, en estrategias de vigilancia ilícitas y represivas, en especial si se orientan a quienes hacen uso de sus derechos a la libertad de reunión pacífica y asociación.

La influencia del sector privado en el espacio cívico en línea

1. Las colaboraciones entre los estados, las autoridades y el sector privado deben ser transparentes y permitir el uso de estándares de adquisiciones abiertas, datos abiertos y gobierno abierto, así como requerir informes de transparencia. La colaboración también debe facilitar el acceso público a la información.
2. Requerir evaluaciones del impacto en los derechos humanos que (a) se realicen periódicamente, antes de la adquisición pública, durante su desarrollo, en momentos clave regulares y a lo largo de su uso en un contexto específico, (b) incluyan una estimación de las posibles transformaciones que podrían generar en las estructuras sociales, institucionales y gubernamentales existentes, (c) incluyan consultas con las comunidades afectadas y (d) sean fácilmente accesibles para el público y legibles por máquina.
3. Garantizar que todos los defensores de los derechos humanos y todos los medios puedan operar sin restricciones, incluido el acoso judicial.

RECOMENDACIONES PARA EL SECTOR PRIVADO

General

1. Satisfacer las obligaciones internacionales diseñadas para proteger los derechos a la libertad de reunión pacífica y asociación.

Apagones de Internet, acceso y conectividad

1. Invertir en el mantenimiento y la mejora de las redes a fin de garantizar un acceso a Internet de alta calidad durante los contextos de crisis y en el futuro.
2. Tomar medidas preventivas para una variedad de amenazas a los derechos de los usuarios, en particular, si el ancho de banda suele congestionarse o desbordarse cuando hay manifestaciones, y brindar capacidad adicional durante los eventos.
3. Desafiar las solicitudes de censura y limitación del servicio provenientes de los estados mediante el uso de todas las herramientas que ofrecen la ley y las políticas, tanto en los procedimientos como en la práctica. Notificar a los usuarios afectados y el público sobre cualquier solicitud de este tipo y cualquier pedido implementado de manera periódica y oportuna.

Vigilancia y derecho a la privacidad

1. Aplicar los principios de privacidad y protección de datos.
2. Proteger la privacidad y la seguridad de los usuarios mediante la encriptación y la anonimización de sus datos, y la transmisión de estos a través canales encriptados, siempre que sea posible.

3. Tratar todo el tráfico de datos de manera equitativa independientemente de su origen, tipo, destino o contenido.
4. Comprometerse públicamente a no reutilizar o monetizar datos y establecer limitaciones claras para los usos secundarios posibles o el procesamiento futuro de los datos.
5. Sancionar la reutilización de datos por parte de terceros sin autorización previa.
6. Realizar evaluaciones oportunas y accesibles sobre el impacto en los derechos humanos antes de formar cualquier tipo de asociación público-privada o realizar adquisiciones públicas que involucren tecnologías de vigilancia.

La influencia del sector privado en el espacio cívico en línea

1. Reconocer explícitamente las plataformas de tecnología y comprometerse a mantenerlas como espacios que facilitan la realización de los derechos humanos, como el derecho a la libertad de reunión pacífica y asociación, a través del funcionamiento pleno de los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas.
2. Insistir en el hecho de que las restricciones sobre los derechos de los usuarios deben satisfacer estrictamente los estándares y las leyes de derechos humanos y el imperio de la ley, así como ser necesarias y proporcionadas para cumplir con un propósito público legítimo y definido claramente.
3. Emitir informes de transparencia, como mínimo, una vez al año y garantizar que estos documentos sean accesibles para todos los usuarios. Esto incluye, al menos, asegurar que los informes (a) puedan encontrarse fácilmente en el sitio web de la empresa, (b) cuenten con una interfaz de usuario intuitiva, (c) presenten un formato accesible para los usuarios con incapacidades y (d) incluyan glosarios o explicaciones de los términos necesarios y se encuentren en los idiomas relevantes.
4. Implementar procesos de debida diligencia para el cumplimiento de los derechos humanos con respecto a productos y servicios particulares que requieran un alto nivel de consideración respecto del impacto potencial en los derechos fundamentales que un producto o una política pueden tener, así como diversas medidas actuales y potenciales para remediarlo.
5. Poner en marcha mecanismos significativos que involucren a múltiples partes interesadas, incluidas aquellas que ofrecen evaluaciones de terceros y expertos, como la Iniciativa de Red Global y otras.
6. Garantizar el derecho de los usuarios de realizar apelaciones y brindar medidas correctivas acordes con los estándares internacionales de derechos humanos que ayuden a equilibrar los derechos, los intereses y las necesidades de las víctimas; además, las empresas deben tener la capacidad de ejecutar de manera efectiva dichos mecanismos.
7. Brindar a los usuarios canales apropiados y accesibles para comunicar sus preguntas, inquietudes y preocupaciones en cuanto a las condiciones de uso, las políticas de la empresa o las restricciones de acceso, libertad de expresión o privacidad.
8. Permitir a las partes interesadas independientes, como las organizaciones de la sociedad civil o los expertos en derechos humanos, que revisen con regularidad los sistemas de moderación y distribución de contenido y garantizar que las políticas de las plataformas se alineen con los

estándares legales internacionales de derechos humanos a fin de mitigar el riesgo que suponen las decisiones algorítmicas sobre los derechos humanos.

RECOMENDACIONES PARA LAS INSTITUCIONES INTERNACIONALES

General

1. Priorizar y desarrollar, mediante la participación de múltiples partes interesadas, interpretaciones sobre el derecho a la libertad de asociación, como la Observación General sobre el Derecho a la Libertad de Asociación (artículo 22), del Comité de Derechos Humanos de la ONU.

Apagones de Internet, acceso y conectividad

1. Reconocer la obligación de los estados de garantizar el acceso a una Internet estable, segura, abierta, asequible y universal como medio para asegurar el cumplimiento de los derechos humanos, incluido el derecho a la libertad de reunión pacífica y asociación.
2. Instar a los estados que niegan deliberadamente el acceso a Internet y otros medios de comunicación, en particular, en el contexto de las reuniones, para que no interrumpan estos servicios.
3. Fomentar la participación de múltiples partes interesadas en la sistematización del monitoreo, la documentación y el registro de las violaciones de los derechos a la libertad de reunión pacífica y asociación en los contextos físico y en línea. A su vez, se aconseja desarrollar constantemente prácticas recomendadas a partir de los datos recopilados para permanecer al tanto del cambiante entorno digital.
4. Establecer un fondo global para incrementar el acceso a Internet en los países menos desarrollados de acuerdo con los objetivos de desarrollo sustentable (SDG) 9.C. Este fondo debe involucrar la participación de las comunidades locales y la sociedad civil en la transferencia de habilidades técnicas y los programas de alfabetismo digital, con foco especial en el género (basado en los proyectos Global Connect Initiative y EQUALS) para garantizar la inclusión digital.

Vigilancia y derecho a la privacidad

1. Prohibir la vigilancia indiscriminada y generalizada de los individuos que hacen uso de su derecho a la libertad de reunión pacífica.
2. Establecer un registro global de las firmas del sector privado que desarrollan y venden tecnologías de vigilancia generalizada que se utilizarán en agencias estatales, en sus respuestas a crisis, incluida la respuesta al COVID-19.

3. Solicitar informes anuales de las compras y el uso de tecnologías de vigilancia en cada estado a las legislaturas y los organismos nacionales independientes correspondientes de supervisión de implementación de derechos humanos.
4. Evaluar y fortalecer la seguridad digital existente y las herramientas de encriptación utilizadas en las iniciativas como la estrategia de datos del Secretario General de las Naciones Unidas.

La influencia del sector privado en el espacio cívico en línea

1. Comprometerse a tomar medidas adecuadas para resolver cualquier caso informado de intimidación o represalias en relación con la participación en procesos públicos a través de una plataforma digital directamente con el estado en cuestión y en asociación con el oficial superior responsable de las represalias.
2. Desarrollar e implementar una oficina dedicada o asignar un Representante Especial exclusivo para monitorear las asociaciones público-privadas, garantizar la transparencia y asegurar el respeto de los derechos humanos.
3. Investigar los compromisos asumidos por los estados y el sector privado en función de los PRNU (Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas), así como su aplicación en el desarrollo, el comercio y el uso de tecnologías que infrinjan los derechos humanos, como las tecnologías de rastreo de contactos. Además, considerar la aplicación de un organismo de monitoreo para informar a la ONU el estado de dichas implementaciones.
4. Garantizar la protección del interés público, los derechos humanos y el espacio cívico en foros y organismos de gobernanza de Internet.
5. Garantizar un espacio abierto: al organizar reuniones físicas o virtuales, se debe dar prioridad y transparencia a las oportunidades de libre organización de las asociaciones y reuniones, así como ampliar la accesibilidad y respetar la confidencialidad según sea necesario.

VII. CONCLUSIÓN

El contexto global actual, en particular con respecto a la pandemia del COVID-19, está provocando cambios profundos en el panorama de las reuniones, tanto en el entorno físico como el digital. Por ejemplo, los individuos solían utilizar máscaras faciales para combatir el poder del estado y las corporaciones (en especial, de Guy Fawkes), y ahora esta técnica se usa en reuniones, en parte, para cumplir con las políticas estatales y evitar la diseminación del COVID-19. De hecho, al escribir este artículo, las estadísticas indican que no hubo evidencia de picos de contagio de COVID-19 tras las protestas masivas en las distintas ciudades de EE.UU., incluida Nueva York.²⁰¹ Además, tal como lo evidencia el movimiento liderado por jóvenes y desarrollado en TikTok con respecto al evento de Trump en Tulsa, tanto los individuos como los grupos están evolucionando rápidamente para adaptar las herramientas digitales a fin de aprovechar su eficiencia y utilidad. Las personas se adaptan día a día para seguir haciendo uso de sus derechos.

Al mismo tiempo, los estados y el sector privado implementan rápidamente nuevas tácticas para adaptarse a las nuevas normas de las protestas. Por ejemplo, tal como lo discutimos en este artículo, los desarrolladores están entrenando tecnologías de reconocimiento facial para identificar a los individuos que usan máscaras.²⁰² Adicionalmente, el monitoreo de redes sociales se implementa día a día como una forma de vigilancia generalizada (sin respetar los principios de necesidad y proporcionalidad que establecen las leyes internacionales de derechos humanos) a fin de reprimir el disenso, prever las protestas y justificar medidas arbitrarias, como las detenciones y multas.

Si bien el respaldo en foros internacionales, nacionales y regionales logró detener el cierre de los espacios digitales para las comunidades en riesgo (más recientemente, a partir de la resolución del Consejo de Derechos Humanos de la ONU, liderada por el Grupo Africano, las decisiones en contra de los apagones de Internet en Indonesia y ECOWAS y las leyes del Consejo de la Ciudad de Nueva York sobre el uso policial de tecnologías de vigilancia masiva), queda claro que se necesitan más medidas para abordar los problemas menos evidentes respecto de los derechos a la libertad de reunión pacífica y asociación, y específicamente, en el contexto digital.

²⁰¹ Ver, p. ej., Buró Nacional de Investigación Económica. *Black Lives Matter Protests, Social Distancing, and Covid-19*, 2020. <http://www.nber.org/papers/w27408>

²⁰² GCN, *supra*, nota 109.

En primer lugar, antes de la pandemia del COVID-19, el mundo ya mostraba indicios de que no cumpliría el prometedor objetivo 9.C de los SDG. El impacto económico de la pandemia del COVID-19 inevitablemente exacerbará las dificultades financieras de los individuos (en particular en las comunidades marginadas) y, por lo tanto, limitará aún más el acceso a Internet. En consecuencia, todas las partes interesadas deben trabajar para resolver las divisiones digitales, en especial, en relación con los derechos sociales, económicos y culturales, así como cívicos y políticos.

En segundo lugar, como ya lo mencionamos, antes de la pandemia del COVID-19, los estados de todo el mundo ya estaban recopilando datos personales, incluidos datos biométricos, a través del uso creciente de programas de identificación digital (en muchos casos, en detrimento de la privacidad y otros derechos fundamentales).²⁰³ A medida que la pandemia del COVID-19 promueve nuevas discusiones en cuanto a la recopilación de datos personales con fines de salud, como el uso de certificados de salud digitales, los estados y el sector privado deben ratificar su compromiso con los derechos humanos y garantizar que estos datos no se utilizarán como un pretexto para impedir que las voces más críticas accedan a espacios públicos y desafíen a las autoridades. Las instituciones multilaterales, como los organismos creados por tratados de la ONU, los organismos regionales, como la Asociación de Naciones del Sudeste Asiático y la Organización para la Cooperación y el Desarrollo Económicos, y las asociaciones de estándares técnicos deben actualizar sus lineamientos para proteger los derechos a la protesta y la reunión en línea.

Por último, el sector tecnológico debe adoptar una postura firme y dejar de inhibir los derechos a la libertad de reunión pacífica y asociación en pro de intereses económicos, tendencias monopólicas y políticas discriminatorias. Esta industria debe establecer específicamente mecanismos efectivos de prevención y monitoreo para resguardar estos derechos.

En conclusión, instamos a todas las partes interesadas a supervisar, proteger y promover los derechos a la libertad de reunión pacífica y asociación, un conjunto de libertades aún en vías de desarrollo y consideración que requieren atención urgente en los espacios y organismos dinámicos que habitamos y creamos en la era digital.

²⁰³ Ver #WhyID. *An open letter to the leaders of international development banks, the United Nations, international aid organisations, funding agencies, and national governments*, 2019. <https://www.accessnow.org/whyid/>

Para obtener más información, comuníquese con:

Laura O'Brien | Oficial de Campañas de la ONU, Access Now | laura@accessnow.org

Peter Micek | Asesor General y Director de Políticas Públicas de la ONU, Access Now | peter@accessnow.org