cade Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

Fundación Karisma

BLOQUEOS DE INTERNET EN AMÉRICA LATINA

Estudios de caso en 6 países de la región

Compilación por: Pilar Sáenz

Publicación: Mayo del 2026

cade Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

CORTES Y BLOQUEOS DE INTERNET EN AMÉRICA LATINA ESTUDIOS DE CASO EN 6 PAÍSES DE LA REGIÓN

Autorías:
Jacobo Nájera
Norman García Aguilar
Grupo Dikyton
Venezuela Sin Filtro
Catalina Moreno
Lorena Peralta
Camila Galvis
Luis Delascar Valencia Mena

Revisión y apoyo:
Catalina Moreno
Paula Rodríguez
Laura Grisales

Compilación
Pilar Sáenz

Dirección de Karisma:
Catalina Moreno Arocha
Juan Diego Castañeda

Coordinación editorial:
Natalia Andrade Fajardo

Corrección de estilo:
Nelson Enrique La Rotta

Identidad gráfica y diseño editorial:
Daniela Moreno Ramírez

Este documento fue realizado en el marco del proyecto CADE – Civil Society Alliances for Digital Empowerment. Ver más en https://cadeproject.org/

Esta publicación está cofinanciada por la Unión Europea. Su contenido es responsabilidad exclusiva de Fundación Karisma y no refleja necesariamente las opiniones de la Unión Europea.

Fundación Karisma
comunicaciones@karisma.org.co

CONTENIDO

Introducción a la recopilación 5

- Características y motivaciones de los cortes en América Latina 7
- Afectaciones al ejercicio de derechos 8
- Recomendaciones generales 8

Cortes y bloqueos de internet en México
Jacobo Nájera 11

Censura digital en El Salvador: el caso del bloqueo de Telegram
Norman Antonio García Aguilar 21

Eliminación de dominios .ni: una nueva forma de censura en Nicaragua
Norman Antonio García Aguilar 27

Interrupciones del internet en Cuba: censura, crisis y derechos vulnerados (2020–2025)
Diktyon Cuba 35

Censura en internet en Venezuela durante elecciones presidenciales: bloqueo de medios, herramientas anticensura y servidores DNS públicos (julio 2024 - enero 2025)
Organización VE Sin Filtro 44

Cortes totales de internet en Quibdó, Chocó
Luis Delascar Valencia Mena 54

Coljuegos y su apuesta de bloquear internet en Colombia
Catalina Moreno Arocha 65

Elementos hacia una documentación de los cortes y bloqueos de internet desde una perspectiva psicosocial
Lorena Peralta 84

INTRODUCCIÓN A LA RECOPILACIÓN

Los cortes, bloqueos y disrupciones de internet no son nuevos en la región, desde hace décadas encontramos casos documentados sobre este tipo de situaciones. Es un fenómeno que no solo preocupa a las poblaciones que se quedan sin acceso a un servicio cada vez más fundamental para el ejercicio de derechos. También alarma a organizaciones de sociedad civil que trabajan sobre los derechos en medios digitales; a organismos internacionales que generan estándares de derechos humanos, como La Relatoría Especial para la Libertad de Expresión (RELE) de la Comisión Interamericana de Derechos Humanos (CIDH)[1]; a quienes generan recomendaciones para extender el acceso en la región como la CEPAL[2] o ISOC[3]; a los gobiernos comprometidos con políticas de inclusión que aprovechan las capacidades del mundo digital; e, incluso, a las empresas prestadoras de servicios en internet que se pueden ver comprometidas al tener que implementar medidas de bloqueo.

Según las cifras de la alianza Keep It On, en 2024 se presentaron 296 casos de cortes de internet y existen registros de 59 bloqueos parciales en su base de datos. En la región hay casos de cortes totales intencionados reportados en los últimos años en Venezuela y Cuba; y para 2024, había registros de bloqueos en servicios de redes sociales en Venezuela, El Salvador y Brasil, asociados a momentos de tensión política. Estas cifras, sin embargo, no reflejan la totalidad del fenómeno: es claro que existe un subregistro importante.

1. En 2019, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos presentó el informe Protesta y Derechos Humanos: Estándares sobre los derechos involucrados en la protesta social y las obligaciones que deben guiar la respuesta estatal donde se desarrolla un capítulo sobre Protestas e Internet. Allí se resalta cómo "las limitaciones en el acceso a Internet, incluyendo las desconexiones totales o parciales, la ralentización de internet, los bloqueos temporales o permanentes de distintos sitios y aplicaciones, antes durante o después de reuniones pacíficas constituyen restricciones ilegítimas a los derechos de asociación y reunión". Disponible en:

https://www.oas.org/es/cidh/expresion/publicaciones/ProtestayDerechosHumanos.pdf

2. En el Informe sobre la situación regional 2020 de la Red de políticas de internet y jurisdicción y la Comisión Económica para América Latina y el Caribe (CEPAL) se desarrollan los temas de filtrado de contenidos, suspensiones y bloqueos derivados de notificaciones y órdenes judiciales y administrativas, bloqueo de sitios y aplicaciones y cortes de servicio como parte de los principales enfoques técnicos de los dilemas transfronterizos de Internet en América Latina y el Caribe. Disponible en: https://www.internetjurisdiction.net/uploads/pdfs/Informe-sobre-la-situación-regional-2020.pdf

3. En su portal Pulse, Internet society dispone de un tablero con información actualizada sobre Apagones de internet. Disponible en: https://pulse.internetsociety.org/es/shutdowns/
También publicó un informe sobre el bloqueo de servicios previo a las elecciones presidenciales de 2024 en Venezuela. Disponible en:https://pulse.internetsociety.org/es/blog/2024/07/internet-censorship-verging-on-service-blocking-ahead-of-venezuela-elections/

En Colombia, quienes seguimos el tema localmente nos encontramos con reportes dispersos de bloqueos de páginas, aplicaciones o servicios que en muchos casos pasan desapercibidos, así como con informes sobre problemas de conectividad localizados que, igualmente, limitan el acceso y el ejercicio de derechos de las personas que habitan estas áreas.

Para entender mejor estos fenómenos y ampliar el ejercicio local, cuya documentación reposa en el micrositio del Observatorio de bloqueos de internet de Fundación Karisma, hemos decidido plantear una recopilación de casos de cortes y bloqueos en la región de Latinoamérica y del Caribe. Para esto hicimos un llamado abierto a personas y organizaciones expertas que han realizado la documentación de estos casos en sus respectivos territorios. De esta forma recopilamos siete casos de estudio.

El primero, es de México, donde no hay cortes totales, pero sí bloqueos que obedecen mayoritariamente a decisiones implementadas por privados como Claro. Allí también documentamos el retiro de una medida de bloqueo a la red Tor que realizó el Estado mexicano por más de una década. El cambio de esta política demuestra que la situación sobre bloqueos innecesarios puede cambiar.

El segundo, de El Salvador, donde hay documentación del bloqueo de la red Telegram para dos fechas, junio y septiembre de 2024, coincidentes con momentos de tensión política para el gobierno de Bukele. Acá destaca la denuncia hecha por organizaciones de sociedad civil y la respuesta estatal de aprobación de leyes que podrían generar nuevos hechos de censura.

El tercero, de Nicaragua, con un caso sin precedentes: la eliminación de los registros de nombre de dominio de cinco medios digitales independientes y la falta de competencia de instancias internacionales de gobernanza sobre los dominios de código país.

El cuarto, de Cuba, ofrece una larga recopilación de los apagones y microcortes ocurridos durante los últimos cinco años. Este caso nos permite identificar una tipología, ya que incluye tanto acciones intencionadas del gobierno cubano en todo el país por varios días, como eventos locales de pocas horas y casos desencadenados por fallas en la infraestructura eléctrica y de telecomunicaciones. Nos permite analizar, además, la importancia de la documentación sostenida en el tiempo.

El quinto caso, de Venezuela, plantea un panorama completo de la censura generada en Internet durante el último periodo electoral y cómo la ciudadanía generó estrategias de evasión para contrarrestar la situación.

Finalmente, presentamos dos casos de Colombia. La recopilación de los cortes en Quibdó, la capital del Chocó, en el noroccidente del país, una región con una infraestructura deficiente. El caso habla directamente de las afectaciones a sus habitantes, de su percepción sobre la ausencia de internet y la necesidad de mejorar la conectividad de la región.

El segundo caso colombiano es de orden nacional. Realiza una descripción del mecanismo utilizado por Coljuegos, la autoridad que regula y administra los juegos de suerte y de azar en el país y que por años ha tenido la facultad de ejecutar bloqueos de internet sin un marco legal suficientemente claro, preciso y garantista. Esto ha generado afectaciones a la libertad de expresión, la intimidad y al debido proceso con el bloqueo de sitios de medios de comunicación y redes sociales.

Además de estos casos, este documento incluye una propuesta para la documentación de cortes y bloqueos desde una perspectiva psicosocial que reconoce otras afectaciones para la población, más allá de aquellas relacionadas con el derecho a la libre expresión y el acceso a la información. Esta perspectiva parte de entender que los cortes y bloqueos obedecen a intenciones, intereses y actores que afectan el ejercicio de los derechos humanos y que, como acciones violentas y de control social, generan miedo, sensación de aislamiento, desconfianza e impotencia. En este último apartado se analizan tres casos —Brasil, El Salvador y Ecuador— desde esta perspectiva.

Características y motivaciones de los cortes en América Latina

El análisis conjunto de los casos expuestos nos permite distinguir tres tipos de cortes y bloqueos: los que afectan todo internet en un territorio nacional, los que afectan una región o lugar específico, y aquellos que solo afectan algunos servicios, como servidores de DNS, la red Tor, las VPN, los servicios de mensajería, las redes sociales, o páginas web, direcciones IP y dominios específicos vinculados con mecanismos de control o censura.

El fenómeno es complejo y tiene múltiples motivaciones que, además, abarcan diferentes mecanismos. Por una parte, surgen motivaciones obvias como reprimir disidencias y protestas sociales, algo evidente en el caso cubano, pero también la necesidad de controlar información y narrativas, como en los casos de El Salvador y Nicaragua, o de manera particular en contextos electorales, como evidencia el caso venezolano. En Colombia y México, en cambio, se observa a los operadores siguiendo o resistiendo órdenes de bloqueo cuya necesidad e impacto no resultan claros.

Emergen también problemas de infraestructura que abarcan tanto fallas en la red eléctrica y de telecomunicaciones como disputas por el control de esa infraestructura. Estas deficiencias son estructurales, como se evidencia en el caso de Quibdó, y se acentúan con el aumento de fenómenos producto del cambio climático, como sequías, inundaciones, huracanes y otros desastres naturales, algo visible en los casos de México, Cuba y Ecuador. Este último aparece brevemente en la documentación desde una perspectiva psicosocial.

Afectaciones al ejercicio de derechos

Esta recopilación de casos también nos permite reconocer el perjuicio a la libertad de expresión y el acceso a la información generados por los cortes y bloqueos de internet. A la vez, encontramos otras afectaciones derivadas, como las dificultades para ejercer el derecho a la participación, la reunión pacífica e, incluso, la protesta. En los casos en que estas acciones son intencionadas, retan el derecho a la asociación, a la intimidad y al voto informado.

En todos los casos existe, además, una limitación al desarrollo económico y social al afectar el trabajo, la educación, el acceso a la salud y al sistema financiero, debido a la actual dependencia tecnológica en estos servicios. Finalmente, en la medida en que se generan impactos psicoemocionales, se afecta el derecho a la salud mental en todas sus dimensiones.

Muchas de estas medidas resultan arbitrarias, deliberadas e incluso ilegales. A lo largo de los casos identificamos ausencia de información sobre lo que sucede, lo que genera falta de transparencia sobre las acciones, los actores y el alcance de algunas medidas. En los casos derivados de órdenes administrativas, como en Nicaragua, Colombia y México, algunas se hacen sin debido proceso. En los casos en que intervienen privados, como operadores y plataformas, hay una falta de canales de comunicación con ellos y de información que permita entender la situación, su rol, el alcance y las medidas que podrían tomarse para mitigar las afectaciones.

Los cortes y bloqueos además propician climas favorables para la desinformación y la manipulación porque generan una sensación de censura e instalan un clima de intervención y miedo, en los casos más complejos. Además, esta percepción se incrementa ante la falta de autoridades de control efectivas y la ausencia de instancias internacionales que puedan tomar medidas frente a estas situaciones.

Recomendaciones generales

Tras analizar los casos podemos plantear una serie de recomendaciones para los diferentes tipos de cortes y bloqueos de internet que se han documentado en la región en los últimos años.

Sobre los cortes totales, si bien no se han presentado de forma reciente en la región, salvo en Cuba, es necesario recordar que cualquier acción deliberada que restrinja el acceso a Internet, por parte de los Estados, es una grave violación a los derechos humanos. Es fundamental que los Estados se comprometan a evitarlo. Además, se debe contar con información que permita conocer las medidas que se toman para evitar estas acciones.

Sobre los bloqueos que solo afectan algunos servicios, se requiere que las medidas cumplan como mínimo con las condiciones de legalidad, necesidad y proporcionalidad. Por parte de los Estados y de los intermediarios es importante, antes de ordenar o implementar medidas de este tipo, hacer un análisis de riesgos e impacto de estas medidas de dichas en derechos como la libertad de expresión, de información, de intimidad y al debido proceso. Adicionalmente, los gobiernos deben entender de qué manera estos bloqueos pueden afectar el acceso de la ciudadanía a servicios antes de ordenarlos. Para las empresas sería importante analizar el alcance de las medidas que se les pide implementar y abstenerse de hacerlo si se generan afectaciones desproporcionadas.

Sobre los bloqueos de páginas web o de contenidos puntuales, es necesario que quienes los ordenan cuenten con mecanismos claros que faciliten conocer las órdenes públicamente, que garanticen mecanismos de revisión y que las órdenes estén dirigidas a enfrentar el problema por el directamente responsable de la página, o el contenido, o por intermediarios. La evaluación periódica de estas medidas y la participación de múltiples actores interesados facilitan que estos mecanismos no se presten para abusos o censura.

Frente a lo que hemos denominado microcortes es necesario desplegar mecanismos de monitoreo permanente de las redes de telecomunicaciones y el contexto en el que se presentan, de forma que se puedan alertar sobre estas disrupciones de la red con documentación clara y suficiente, no solo de forma anecdótica. La documentación puede nutrirse de mecanismos de seguimiento de la infraestructura provenientes de los privados, pero también del Estado o de la sociedad civil. Comprender mejor la calidad del servicio facilita que las personas usuarias sean conscientes de la importancia de reportar los casos y ayudar en su documentación.

Por su parte, los esfuerzos para documentar los casos de cortes y bloqueos en la región son desiguales entre países, tanto en términos de conocimientos técnicos como de acciones de incidencia. Hay experiencias consolidadas que dependen en gran medida de unas pocas personas y organizaciones, con financiación escasa y trabajo mayormente voluntario, por lo que este es un campo que se beneficiaría de proyectos de financiación orientados a ampliar y sostener los observatorios e iniciativas de documentación existentes.

Se destacan iniciativas de publicación de documentación, casos y metodologías que han facilitado el intercambio de información sobre cortes y bloqueos de internet en la región; este estudio de casos es una de ellas. De parte de la comunidad técnica existe una buena disposición a abordar el tema, si bien no es frecuente su abordaje en dimensiones más políticas o de incidencia, es fundamental continuar promoviendo y facilitando espacios para el intercambio técnico.

Es necesario fortalecer estas redes, sobre todo, de cara a los problemas derivados de una infraestructura de telecomunicaciones y eléctrica débil e insuficiente; y del aumento de fenómenos producto del cambio climático que estresan cada vez más esa infraestructura. La pregunta por la soberanía, la autonomía y la resiliencia de nuestra conectividad, no solo relacionada a los datos, la información y los servicios; sino, también, de la infraestructura que lo soporta será importante para futuros debates sobre el tema.

Finalmente, aunque la denuncia de los cortes y bloqueos ha sido constante, no siempre la respuesta manifiesta voluntad política real por parte de las administraciones para atender esta problemática. El desarrollo de medidas efectivas para evaluar y prevenir las afectaciones es mínimo por parte de los Estados de la región y, en pocos casos, el comienzo de alguna implementación significativa ha tomado años de esfuerzo por parte de la sociedad civil. Una respuesta efectiva frente a los cortes y bloqueos de internet sigue requiriendo el trabajo sostenido de documentación, investigación, visibilización y, eventualmente, denuncia, acciones ejercidas por organizaciones y personas interesadas. Sin embargo, urge establecer y fortalecer espacios regionales para esta discusión en modelos de múltiples partes interesadas. Los espacios de gobernanza de Internet regionales y nacionales, concebidos precisamente para abordar estos temas de manera abierta, inclusiva y colaborativa; están llamados a desempeñar un papel central en futuras discusiones.

Escrita por Pilar Sáenz.

Fundación Karisma

CORTES Y BLOQUEOS DE INTERNET EN MÉXICO

Jacobo Nájera

Tecnólogo e investigador, con interés en la artesanía tecnológica y los derechos a la comunicación. En 2019 recibió el Premio Gabo de Periodismo en la categoría de Innovación. Actualmente es colaborador principal en The Tor Project.

Ha realizado investigación en el proyecto Mecanismos de Privacidad y Anonimato de la Universidad Nacional Autónoma de México y en el laboratorio Stratosphere IPS de la Universidad Técnica Checa.

Cofundó la organización social Enjambre Digital (2014–2019), en el contexto de la reforma de telecomunicaciones en México. Asimismo, formó parte de los colectivos Internet para Todos, ContingenteMX y Zonainter (2005–2013), y fue integrante del último comité de dirección de la cooperativa May First Movement Technology.

cade Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

RESUMEN

Este artículo intenta caracterizar el fenómeno de bloqueos y cortes de Internet en México, así como dar cuenta de algunos casos documentados en la última década, principalmente el de Tor, y de cómo estos afectan derechos humanos como la libertad de expresión, la intimidad y el acceso a la información. A través de mediciones técnicas de red, análisis documental y análisis de datos en herramientas distribuidas como OONI e IODA, se identificaron cinco categorías principales de estos fenómenos en México: 1) Bloqueos administrativos por derechos de autor; 2) Cortes por fenómenos naturales; 3) Acciones discrecionales entre autoridades y empresas; 4) Cortes físicos derivados de conflictos entre gobiernos municipales y operadores; y 5) Bloqueos específicos contra el uso de la red Tor.

PALABRAS CLAVE:

México, bloqueos, cortes, Internet, telecomunicaciones.

Este documento fue realizado en el marco del proyecto CADE – Civil Society Alliances for Digital Empowerment. Ver más en https://cadeproject.org/

Esta publicación está cofinanciada por la Unión Europea. Su contenido es responsabilidad exclusiva de Fundación Karisma y no refleja necesariamente las opiniones de la Unión Europea.

INTRODUCCIÓN

Durante la última década, en México, el fenómeno de los cortes y bloqueos de Internet se puede caracterizar y analizar a partir de sus causas y motivos. Entre estas causas se incluyen: 1) los bloqueos de sitios web a través de la legislación vigente de derecho de autor; 2) cortes en la conexión a Internet como resultado de fenómenos meteorológicos violentos; 3) acciones discrecionales de algunos gobiernos en colaboración con algunas empresas dedicadas al hospedaje y registradores de dominios; 4) cortes físico-administrativos por conflicto de competencias entre autoridades locales y regulación federal; y 5) medidas realizadas por proveedores de telecomunicaciones bajo el supuesto de mitigar ataques informáticos, estas comprenden formas de bloqueo para las personas usuarias de Tor y que intentan ingresar a los principales sitios web del Gobierno de México.

DEFINICIONES

Para este análisis, se entiende por bloqueo o corte de internet al fenómeno resultante de la implementación deliberada de obstáculos técnicos que impiden, limitan o interfieren la transmisión de datos a nivel capa de red, a través de las redes que conforman Internet, como se describe en la Guía para seguir comunicándonos ante bloqueos de internet (Avendaño y Najera, 2022). Sin embargo, para este análisis de caso, también se incorporan los obstáculos producidos por fenómenos meteorológicos violentos, que actualmente también son considerados por las personas que documentan los cortes en América Latina (Ballesteros, Najera y Saenz, 2025).

METODOLOGÍA

Las metodologías que dan cuenta de los bloqueos a lo largo de la última década en México consisten en registros técnicos, documentales y solicitudes de información pública. En algunos de los casos, estas abarcan medición, registro, análisis y reporte. Para las mediciones técnicas se implementó tanto mediciones de red intencionadas, como las provenientes de otras plataformas conocidas: del Observatorio Abierto de Interferencias en la Red (OONI) y de Internet Outage Detection and Analysis (IODA).

CARACTERÍSTICAS DEL FENÓMENO DE BLOQUEO Y CORTES DE INTERNET

Las características de los cortes y bloqueos de internet permiten conocer los actores responsables y sus posibles motivaciones. A continuación, se abordan brevemente los diferentes tipos de casos y, posteriormente, el de Tor que se abordará con mayor profundidad.

1. Bloqueos que resultaron de medidas discrecionales del gobierno en conjunto con empresas privadas

Para ilustrar este tipo de bloqueos, resulta útil un ejemplo concreto: el sitio web 1dmx.org fue creado por algunas colectividades para informar y documentar los abusos del gobierno y la fuerza pública durante las protestas previas y posteriores a la posesión del presidente Enrique Peña Nieto, en el periodo 2012-2018.

El 2 de diciembre de 2013 este sitio dejó de estar disponible porque la empresa GoDaddy.com, responsable del registro del dominio, lo dio de baja argumentando que había violado las condiciones del servicio. En ese momento, las personas administradoras del sitio contaron que las razones de GoDaddy para la suspensión se debían a que "había una investigación policial en curso" y que la solicitud de dar de baja el dominio habría sido emitida por la Comisión Nacional de Seguridad en México, con el apoyo del Departamento de Seguridad Interior de la Embajada de los Estados Unidos en México (Avila y Ordoñez, 2014). El sitio fue restablecido tres meses después sin explicaciones (Igartua, 2014).

2. Bloqueos por derechos de autor

La Pirateca es una colectiva dedicada, desde 2019, a la digitalización de libros para compartirlos en un sitio web. En julio de 2022 comenzó a sufrir bloqueos de acceso en tres de los más grandes operadores de telecomunicaciones de México: Telmex, Megacable e Izzi, este último después dejó de bloquearla.

Las mediciones de red de este caso indican que se realizó un bloqueo de DNS. Telmex y Megacable explicaron que implementaron estas medidas porque recibieron un oficio del Instituto Mexicano de la Propiedad Industrial (Najera, 2022).

Desde 2020, la legislación mexicana en materia de derechos de autor contempla un procedimiento administrativo que permite solicitar a los operadores de telecomunicaciones el bloqueo provisional de acceso a sitios web, sin necesidad de una resolución judicial. En el caso de La Pirateca, las acciones de bloqueo derivaron de un procedimiento administrativo, mas no de un juicio. Este es el primer caso público documentado con estas características en el país. Para evadir el bloqueo la colectiva ha registrado nuevos dominios; sin embargo, su actividad ha sido intermitente.

3. Cortes de internet y de los sistemas de telecomunicaciones por fenómenos meteorológicos

El huracán Otis, un ciclón tropical de categoría 5, azotó la costa del Pacífico de México el 25 de octubre de 2023 y produjo marejadas ciclónicas, inundaciones y deslizamientos de tierra, así como daños en la infraestructura y en un aeropuerto (Nasa, 2023).

Tras su impacto, el regulador de telecomunicaciones informó sobre afectaciones en la infraestructura de los diferentes operadores de servicios fijos y móviles y falta de energía eléctrica (IFT, 2023). Prácticamente, mientras se reparaban los daños, todas

las telecomunicaciones dejaron de funcionar, las comunicaciones de emergencia se realizaron por vía satelital y mediante los sistemas de transmisión de personas radioaficionadas (Unesco, 2024).

4. Casos en donde autoridades municipales realizan acciones de corte de cables de empresas dedicadas a proveer internet

En julio de 2021, el gobierno municipal de Guanajuato cortó los cables de la empresa Megacable afectando el servicio de decenas de miles de personas del municipio. El argumento con que justificaron el acto fue la existencia de una deuda por concepto de uso del derecho de vía (Serna, 2021). El proveedor negó la existencia de esa deuda, manifestó estar al día en todos los impuestos y contribuciones indicadas por ley, así como una concesión federal.

Después de un juicio que demoró cinco años, un juez determinó a favor del municipio de Guanajuato imponiendo a la empresa Megacable un pago de más de 111 millones de pesos mexicanos por exceso de cableado (Dámaso, 2024).

5. El caso de Tor

La red Tor es una herramienta global que permite a las personas ejercer libertad de acceso y expresión en internet, manteniendo su privacidad y anonimato. Para ello utiliza más de 6000 nodos distribuidos mundialmente por los que se enruta la navegación de las personas usuarias.

En México se calcula que entre 30.000 y 40.000 personas utilizan esta red diariamente. La sociedad civil y diversos colectivos han promovido su uso, entre ellos quienes implementan buzones anónimos en redacciones periodísticas y personas y organizaciones que trabajan en la defensa de los derechos humanos. La administración federal utiliza la red Tor para combatir la corrupción en la implementación del buzón de la Secretaría de la Función Pública (Riquelme, 2019). Los lineamientos de operación de este buzón establecen que es necesario garantizar el anonimato (DOF, 2016). Sin embargo, como se muestra a continuación, se han encontrado medidas de bloqueo ejercidas por un operador de telecomunicaciones y por el gobierno federal.

Bloqueo por Telmex

La documentación e investigación sobre el bloqueo realizado durante cinco años por el operador más grande de México surgió a partir de los efectos que este provocó. Telmex, el operador en cuestión, bloqueó siete direcciones IP pertenecientes a la red Tor. Si bien este bloqueo no impedía el acceso a dicha red, sí limitaba la instalación de nodos. La red Tor está compuesta por nodos distribuidos alrededor del mundo, operados de forma voluntaria por distintas personas. Con estos nodos la red asegura una máxima dilución del tráfico de cada persona usuaria, para así lograr el anonimato que ofrece a nivel capa de red. Tener nodos en diferentes regiones fortalece a la red en su propósito.

El primer registro público de los efectos de esta medida se conoció cuando un nodo de la red Tor[4], que había operado por más de cinco años, dejó de funcionar la noche del 31 de diciembre de 2015. La persona responsable del nodo comunicó la falla el 9 de enero de 2016 mediante la lista de correo de personas operadoras de la red Tor. Los datos históricos muestran un decrecimiento de los nodos funcionales instalados en México, que pasó de entre cinco y ocho nodos a solo uno.

Solo hasta 2017, un grupo de activistas e investigadores interesados en la participación y despliegue de la red Tor en México encontró que, a pesar de la limitación de instalar nodos en la red del proveedor más grande de internet en México, las personas sortearon esta dificultad al instalar nodos en otros proveedores. Se reconoce el interés de las personas operadoras de la red Tor en México, pero dicha limitación significó una barrera para la participación futura.

Esto llevó a una investigación en profundidad de los antecedentes y motivos de este bloqueo. Así, se logró conocer con precisión y evidencias que la medida consistía en el bloqueo a nivel ruta de siete direcciones IP correspondientes al sistema central de la red conocido como “Autoridades Directorio” (Wolf, 2019).

En 2020, en un artículo periodístico de Global Voices (Nájera y Ververis, 2020), se publicaron los hallazgos y el recuento mencionado. Tras la publicación, Telmex reconoció públicamente que realizaron el bloqueo de las siete direcciones IP y dijeron que fueron “reportados en su momento por estar asociados con la distribución del ransomware WannaCry”.

Hay razones de peso para afirmar que este bloqueo a la red Tor no estuvo vinculado con una respuesta al ransomware WannaCry. La primera y más obvia es que dicho ataque, que duró cuatro días entre el 12 y el 15 de mayo de 2017, inició un año después del bloqueo. La segunda es que, en caso de un ataque de ransomware, sería ineficaz e inoperante técnicamente. Las medidas de bloqueo no tenían ningún efecto sobre la propagación de un software malicioso con estas características, ya que las siete direcciones bloqueadas no pueden participar de una tarea de esta naturaleza, debido a que tienen un rol asignado de administración y gestión de la red y no manejan directamente el tráfico de personas usuarias. Estos argumentos fueron entregados el 2 de junio de 2020 en una carta a Telmex (Alcantar, Najera, Ververis y Wolf, 2020).

Dos días después, el bloqueo de las siete direcciones IP del sistema de autoridades del directorio de la red Tor fue levantado por Telmex.

4. Disponible en: https://archive.torproject.org/websites/lists.torproject.org/pipermail/tor-relays/2016-January/008491.html

Bloqueo al principal sitio web del Gobierno de México para las personas usuarias de Tor

Actualmente, el acceso a sitios web de comunicación y de información pública del Gobierno Federal está bloqueado para quienes usan la red Tor. Este bloqueo es resultado de una medida implementada desde la infraestructura de la administración pública. Existen registros que indican que esta práctica se ha presentado durante, al menos, las dos últimas administraciones federales y la actual, por tanto, se trataría de una medida con más de 13 años de vigencia.

Un estudio completo de esta situación concluye que la medida del gobierno comprende a 21 dependencias, que incluyen los sitios web datos.gob.mx y www.gob.mx (Nájera y Trujillo, 2023). No se conocen los motivos que tuvo la administración 2012–2018 para realizar este bloqueo. La administración federal 2018–2024 respondió que la medida se implementó como una forma de protección frente a posible tráfico malicioso, argumentando que no se puede diferenciar "entre el usuario medio y el automatizado", lo que consideraron un riesgo, por lo que se bloqueó dicha red (Guerrero, 2023). Por su parte, la administración actual respondió que no cuenta con soporte documental o política que ampare la medida (Vázquez, 2025).

Frente a estos argumentos, Tor Project ha señalado que bloquear secciones completas de Internet bajo la creencia de que el tráfico de Tor es indistinguible o inherentemente malicioso es una postura obsoleta, errónea y que pone en riesgo a las personas usuarias. Además, explican que existen métodos para proteger los sitios web de amenazas, como ataques DoS u otros, sin necesidad de restringir grandes secciones de Internet. También señalan ejemplos de implementaciones que, según su valoración, logran un mejor equilibrio entre seguridad y acceso (Najero y Trujillo, 2023).

Este caso permite analizar dos dimensiones clave: por un lado, el impacto en los derechos de quienes desean acceder a los servicios del gobierno federal o a información pública a través de Tor. Esto, al menos, afecta a las 40.000 personas usuarias que utilizan la red Tor desde México, aunque en un sentido amplio se limita el acceso a información pública de México a las millones de personas usuarias de la red Tor en el mundo.

Por otro lado, está la justificación técnica del bloqueo, ya que la medida no cumple el test tripartito de proporcionalidad, necesidad y legalidad, que debería suplir una medida que limita la libertad de expresión siguiendo los estándares de la Comisión Interamericana de Derechos Humanos (Chocarro, 2017). Existen alternativas menos lesivas para abordar los riesgos señalados por una de las administraciones gubernamentales. Además, falta el soporte documental, legal y político que justifique mantener la medida de bloqueo por la actual administración pública federal.

CONCLUSIONES

Los primeros cuatro casos introductorios y surgidos en el contexto Mexicano permiten reconocer algunas de las principales características de los cortes y bloqueos en el país: bloqueos por derechos de autor, cortes por fenómenos meteorológicos extremos, acciones discrecionales de gobiernos en colaboración con empresas, medidas desproporcionadas bajo los supuestos de seguridad tanto por parte del proveedor más grande de México y el Gobierno Federal.

Finalmente, en el caso de Tor, sobresale que las declaraciones del proveedor Telmex evidencian un desconocimiento técnico sobre el funcionamiento tanto del malware WannaCry como de la red Tor. Las medidas tomadas no solo fueron ineficaces, sino que se basaron en supuestos incorrectos que cuestionan la capacidad técnica con que se toman decisiones de alto impacto en materia de derechos humanos en el contexto digital. También, es diciente que la autoridad reguladora no haya investigado ni ofrecido una explicación sobre las causas del bloqueo, a pesar de que se le solicitó expresamente que lo tomara como un caso de estudio y de aprendizaje para forjar una mejor normativa (Annon, 2020) y, así, prevenir futuras vulneraciones similares. Asimismo, el bloqueo para las personas usuarias de Tor al principal sitio web del Gobierno de México presenta una medida no proporcional en la práctica. Como un símil, y bajo los supuestos que expone la autoridad, sería como cerrar caminos, carreteras y puentes ante posibles excesos de velocidad.

REFERENCIAS

Anon. (2020). Bloqueo de la red Tor contrario a las mejores prácticas de seguridad, derechos humanos y neutralidad de la red. https://internetanonima.net/bloqueo-de-la-red-tor-contrario-neutralidad-de-la-red/

Avendaño, T. y Nájera, J. (s.f.). Guía para seguir comunicándonos ante bloqueos de internet. Digital Defenders Partnership. https://comunicandonos.codeberg.page/

Avila, R. (2014, marzo 5). México y EE.UU. censuran sitio activista, con la ayuda de GoDaddy. Global Voices en Español. https://es.globalvoices.org/2014/03/05/mexico-y-ee-uu-censuran-sitio-activista-con-la-ayuda-de-godaddy/

Ballesteros, A., Nájera, J y Saénz, P. (2025, febrero 26). ¿Por qué seguir documentando bloqueos de internet? Experiencias desde América latina. http://archive.org/details/documentando-bloqueos-de-internet-desde-america-latina

Chorraco, S. (2017, agosto). Estándares internacionales de libertad de expresión: Guía básica para operadores de justicia en América Latina. Center for International Media Assistance. https://www.corteidh.or.cr/tablas/r37048.pdf

Igartúa, S. (2014, marzo 5). Sin explicación, restablecen sitio de Internet de 1dmx.org. Proceso. https://www.proceso.com.mx/nacional/2014/3/5/sin-explicacion-restablecen-sitio-de-internet-de-1dmxorg-129912.html

Instituto Federal de Comunicaciones (IFT). (2023). El IFT informa sobre la situación de la infraestructura de telecomunicaciones y radiodifusión en Guerrero, por el huracán Otis. (Comunicado 90/2023) https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/el-ift-informa-sobre-la-situacion-de-la-infraestructura-de-telecomunicaciones-y-radiodifusion-en

Nájera, J. y Ververis, V. (2020). En México, el más grande operador de telecomunicaciones bloquea la internet segura. Global voices en español. https://es.globalvoices.org/2020/05/28/en-mexico-el-mas-grande-operador-de-telecomunicaciones-bloquea-la-internet-segura/

Nájera, J. (2022, noviembre 25). Una colectiva mexicana que piratea libros para compartir la cultura enfrenta bloqueos. Global Voices en Español. https://es.globalvoices.org/2022/11/25/una-colectiva-mexicana-que-piratea-libros-para-compartir-la-cultura-enfrenta-bloqueos/

Nájera, J. y Trujillo, M. (2023). GitHub - tor-gob/reporte-mexico: Reporte de la accesibilidad de los sitios gubernamentales mexicanos desde la red Tor. Recuperado el 6 de mayo de 2025, de https://github.com/tor-gob/reporte-mexico

Najera, J., y Trujillo, M. (2023, octubre 9). Gobierno de México recibe crítica por bloquear secciones enteras de la Internet segura. Global Voices en Español. https://es.globalvoices.org/2023/10/09/gobierno-de-mexico-recibe-critica-por-bloquear-secciones-enteras-de-la-internet-segura/

NASA (2023, octubre 31) El huracán Otis. Redacción Ciencia https://ciencia.nasa.gov/ciencias-terrestres/el-huracan-otis/

Riquelme, R. (2020a, mayo 29). Telmex bloquea siete de 10 accesos a la red Tor en México. El Economista. https://www.eleconomista.com.mx/tecnologia/Telmex-bloquea-siete-de-10-accesos-a-la-red-Tor-en-Mexico-20200528-0078.html

Riquelme, R. (2020b, junio 4). Telmex desbloquea direcciones IP de servidores de autoridad de la red Tor en México. El Economista. https://www.eleconomista.com.mx/tecnologia/Telmex-desbloquea-direcciones-IP-de-servidores-de-autoridad-de-la-red-Tor-en-Mexico-20200604-0094.html

Serna, P. (2021, julio 14). Cortan líneas de comunicación a Megacable en Guanajuato por adeudar 35 millones de pesos. El Sol de León. Recuperado el 6 de mayo de 2025, de https://oem.com.mx/elsoldeleon/local/cortan-lineas-de-comunicacion-a-megacable-en-guanajuato-por-adeudar-35-millones-de-pesos-20205072.app.json

UNESCO (2024, enero 18). Celebramos la radio, un salvavidas para cientos de familias tras el Huracán Otis en México
https://www.unesco.org/es/articles/celebramos-la-radio-un-salvavidas-para-cientos-de-familias-tras-el-huracan-otis-en-mexico

Vazquez (2025). Respuesta del gobierno mexicano sobre el bloqueo a la red Tor. Internet Archive. https://archive.org/details/gobierno-mexico-respuesta-bloqueo-red-tor-2025

Wolf, G. (2019). Distributed detection of tor directory authorities censorship in mexico. 82–86. In: The Eighteenth International Conference on Networks, 24 -- 28 Mar 2019, Valencia, España. https://archive.org/details/gobierno-mexico-respuesta-bloqueo-red-tor-2025

Wolf, G. (2021). Mecanismos de privacidad y anonimato en redes: Una visión transdisciplinaria. Instituto de Investigaciones Económicas, UNAM. https://priv-anon.unam.mx

CENSURA DIGITAL EN EL SALVADOR: EL CASO DEL BLOQUEO DE TELEGRAM

Norman Antonio García Aguilar

Ingeniero en Telemática, especializado en seguridad informática y en la administración de servidores y redes. A lo largo de su trayectoria, ha trabajado en auditorías informáticas y en la implementación de políticas de seguridad orientadas a proteger el flujo de datos y garantizar la integridad de la información en entornos digitales.

Su trabajo se sitúa en la intersección entre la informática y los derechos humanos, con énfasis en temas como la censura en Internet, la gobernanza de Internet y los mecanismos que inciden en la libertad de expresión en línea.

Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

RESUMEN

Entre junio y septiembre de 2024, organizaciones internacionales como Netblocks y OONI informaron sobre bloqueos a Telegram en El Salvador. Esta aplicación es ampliamente utilizada por periodistas, activistas y ciudadanos que difunden información para la ciudadanía salvadoreña y sus audiencias. Este bloqueo afectó la libertad de expresión y el derecho al acceso a la información, obligando a las personas usuarias a utilizar VPN para conectarse. El primer incidente ocurrió en un contexto de filtraciones masivas de datos personales de más de 5,1 millones de personas salvadoreñas, atribuidas al grupo hacktivista Ciber Inteligencia SV, que expuso información de entidades públicas y de la billetera digital oficial del gobierno. Sumado a esto, el 31 de mayo, el grupo Los Pelaos Bro (@lospelaosbro) difundió contenido ofensivo contra el presidente Bukele en la capital de El Salvador. Organizaciones como AccessNow y la APES condenaron el bloqueo. A raíz de estos hechos, en noviembre se aprobaron las leyes para la protección de datos personales, ciberseguridad y seguridad de la información. Existe preocupación de que sean utilizadas para censurar. Este caso evidencia la necesidad de mejorar la seguridad digital, promover el uso de herramientas de protección como las VPN (Virtual Private Network) y de documentación como OONI, y de fortalecer la defensa de los derechos digitales en el país.

PALABRAS CLAVE:

El Salvador, bloqueo, Telegram, ciberseguridad.

Este documento fue realizado en el marco del proyecto CADE – Civil Society Alliances for Digital Empowerment. Ver más en https://cadeproject.org/

Esta publicación está cofinanciada por la Unión Europea. Su contenido es responsabilidad exclusiva de Fundación Karisma y no refleja necesariamente las opiniones de la Unión Europea.

INTRODUCCIÓN

En abril de 2024, bases de datos con información personal de aproximadamente 5,1 millones de salvadoreños empezaron a ser publicadas de manera gratuita. Estas incluían datos sensibles como el Documento Único de Identidad (DUI), fecha de nacimiento, nombre completo y direcciones de correo electrónico, así como las residenciales (ubicación de la casa), números telefónicos, entre otros (La Prensa Gráfica, 2024).

Estas filtraciones y otras provenientes del Instituto Salvadoreño del Seguro Social (ISSS), el Ministerio de Transporte, la Sociedad de Ahorro y Crédito Constelación y el Ministerio de Educación, así como de Chivo Wallet (la billetera digital oficial de Bitcoin y dólar de El Salvador, administrada por el gobierno), fueron expuestas por un autodenominado grupo hacktivista llamado Ciber Inteligencia SV. Este se identifica como un grupo que realiza ciberataques al Estado salvadoreño con fines políticos, ideológicos y de protesta (Global Voices, 2024).

Es importante mencionar que los datos filtrados por este grupo ciberhacktivista no fueron “tratados” previamente y con esto se expuso información personal sensible de millones de salvadoreños. Se comprometió la integridad de las personas, desde su seguridad física, digital, psicoemocional y financiera; esto podría servir para ataques de ingeniería social, ya que la información salarial y el DUI exponen a los afectados a robos o secuestros.

En esas mismas semanas, específicamente el 31 de mayo de 2024, un grupo denominado Los Pelaos Bro se adjudicaron la autoría de un ataque directo en contra del presidente Nayib Bukele, en el que se mostraban montajes pornográficos del presidente en vallas publicitarias en un sector de la ciudad capital de El Salvador (El diario de hoy, 2024).

ANTECEDENTES Y DESARROLLO

El primero de junio de 2024, la ciudadanía de El Salvador vivió un incidente de censura digital que generó alertas a nivel nacional e internacional, al percatarse de que Telegram, una plataforma popular de mensajería instantánea fue bloqueada a nivel nacional (Prensa Gráfica, 2024b). Según reportes de organizaciones como Netblocks (2024a, el incidente coincidió con la toma de posesión del segundo mandato del presidente Nayib Bukele y la aparición de vallas publicitarias con contenido ofensivo contra el mandatario, además de amenazas de filtraciones de bases de datos estatales por parte del grupo ciberhacktivista CiberInteligencia SV.

Un segundo bloqueo a Telegram sucedió el 15 de septiembre de 2024. Este nuevo bloqueo también fue reportado nuevamente por Netblock (OONI, 2024b) y por el Observatorio Abierto de Interferencias de Red (OONI, 2024). Este bloqueo coincide con la publicación de reportajes periodísticos sobre la muerte del exasesor de seguridad nacional del Gobierno de El Salvador, Alejandro Muyshondt, bajo custodia del Estado y la revelación de conversaciones de altos funcionarios en las que se habla de una oficina para espiar a políticos y periodistas que han sido críticos con la actual administración.
Telegram se ha convertido en un canal clave para la difusión de información crítica hacia el Gobierno, incluidos grupos de periodistas independientes y activistas. Al impedir el acceso a esta aplicación, se limitó no solo la comunicación interpersonal, sino también el ejercicio del periodismo y la organización social, violentando los derechos de libertad de expresión y de acceso a la información.

Debido a los bloqueos a Telegram ocurridos en junio y septiembre de 2024, y que fueron documentados por la organización Netblocks, los usuarios salvadoreños tuvieron que usar VPN para superar la censura.

Los dos bloqueos ocurridos entre junio y septiembre de 2024 representan una grave afectación a los derechos humanos de la ciudadanía salvadoreña, puesto que Telegram es una aplicación de mensajería instantánea usada por diferentes sectores de la sociedad para comunicarse. Su uso constituye una forma de ejercer el derecho a la libre expresión mediante la participación en grupos de chat, y el derecho a la información al ser un canal de distribución de contenidos de medios de comunicación y organizaciones de sociedad civil.

Organizaciones internacionales como AccessNow, Artículo 19, la Red Centroamericana de Periodistas y la Asociación de Periodistas de El Salvador emitieron un comunicado en septiembre 2024, donde expresaban su preocupación ante este acto de censura y llamaron al Estado a investigar el incidente y a garantizar el ejercicio de la libertad de expresión para la ciudadanía (AccessNow, 2024).

RETOS PARA LA INCIDENCIA

La denuncia pública, los comunicados y las colaboraciones entre organizaciones nacionales e internacionales han sido clave para promover una campaña de concientización sobre el alcance que tiene censurar aplicaciones de mensajería instantánea.

La ciudadanía difundió y utilizó las VPN como una herramienta para evadir la censura y poder usar Telegram. También se propagó el uso de la aplicación OONI para hacer mediciones y pruebas de conectividad, permitiendo a los analistas tener más datos para diagnosticar bloqueos.

Estos incidentes también plantearon la discusión sobre la importancia de la seguridad en el resguardo de los datos personales por parte del Estado, lo que llevó a que el 11 de noviembre la comisión de Seguridad Nacional y Justicia de la Asamblea Legislativa avalara la Ley de Ciberseguridad y Seguridad de la Información, y a que el 12 de noviembre de 2024 se aprobara la Ley de Protección de Datos Personales. La diputada Alexia Rivas, del partido Nuevas Ideas, señaló la importancia de estos marcos normativos, ante la ausencia de legislación que proteja a la población de hackers, del robo de fotografías del celular o de la suplantación de identidad (ElSalvador.com, 2024).

Organizaciones como Humans Rights Watch (2024) alertaron sobre el peligro que representan ambas leyes a la libertad de prensa y a la intimidad, ya que pueden ser usadas por el Estado para eliminar publicaciones críticas en contra del Gobierno con el pretexto de estar protegiendo datos personales.

El monitoreo y las mediciones de pruebas de conectividad son herramientas necesarias para recolectar datos que ayuden a evidenciar técnicamente un bloqueo o una caída; es importante promover esto a través de mediciones automáticas hechas por OONI para contar con más datos.

La concientización y la difusión de la importancia de la seguridad digital, el uso de VPN, el resguardo de información sensible y el cifrado en las comunicaciones, a través de campañas de sensibilización, son necesarias para evitar la censura y proteger nuestra identidad.

Los lazos y colaboración con la comunidad técnica tuvieron un rol importante en este caso, estos deben mantenerse y reforzarse con el fin de tener organizaciones amigas que hagan investigación sobre caídas de internet que difundan y denuncien estos ataques digitales.

Para mantener a la población informada, es importante promover y dar a conocer los derechos que tenemos como personas usuarias de Internet, bien sea a través de conferencias, charlas o talleres en universidades y en medios de comunicación.

REFERENCIAS

Access Now. (2024, junio 3). Telegram confirma el bloqueo de su servicio en El Salvador. https://www.accessnow.org/press-release/telegram-comunicado-el-salvador/
ElSalvador.com. (2024a). Hackean vallas publicitarias en San Salvador con mensajes contra Nayib Bukele. https://www.elsalvador.com/noticias/nacional/hackean-valla-publicitarias-san-salvador-nayib-bukele/1146001/2024/

ElSalvador.com. (2024b). Comisión avala leyes de ciberseguridad y de protección a datos personales. https://www.elsalvador.com/noticias/nacional/seguridad-nacional-y-justicia-cibercriminales-ciberataques-ataques-ciberneticos-asamblea/1180628/2024/

Global Voices. (2024, julio 12). Polémicos hacktivistas habrían provocado censura de Telegram en El Salvador. https://es.globalvoices.org/2024/07/12/polemicos-hacktivistas-habrian-provocado-censura-de-telegram-en-el-salvador/

Human Rights Watch. (2024). El Salvador: Nuevas leyes amenazan la libertad de expresión y la privacidad. https://www.hrw.org/es/news/2024/12/12/el-salvador-nuevas-leyes-amenazan-la-libertad-de-expresion-y-la-privacidad

La Prensa Gráfica. (2024a, junio 1). Observatorios de censura y usuarios reportan bloqueo de la aplicación Telegram en El Salvador. https://www.laprensagrafica.com/elsalvador/Observatorios-de-censura-y-usuarios-reportan-bloqueo-de-la-aplicacion-Telegram-en-El-Salvador-20240601-0019.html

La Prensa Gráfica. (2024b, abril 6). Filtran base con datos personales de 5.1 millones de salvadoreños tras no lograr venderlos en línea. https://www.laprensagrafica.com/elsalvador/Filtran-base-con-datos-personales-de-5.1-millones-de-salvadorenos-tras-no-lograr-venderlos-en-linea-20240406-0021.html

NetBlocks. (2024a, junio 1). Confirmed: Messaging app Telegram is currently restricted in #ElSalvador. Mastodon. https://mastodon.social/@netblocks/113141516044118853

Netblocks. (2024b, septiembre 15). Confirmed: Live metrics show a disruption to Telegram backend and frontend services in #ElSalvador. https://mastodon.social/@netblocks/113141516044118853

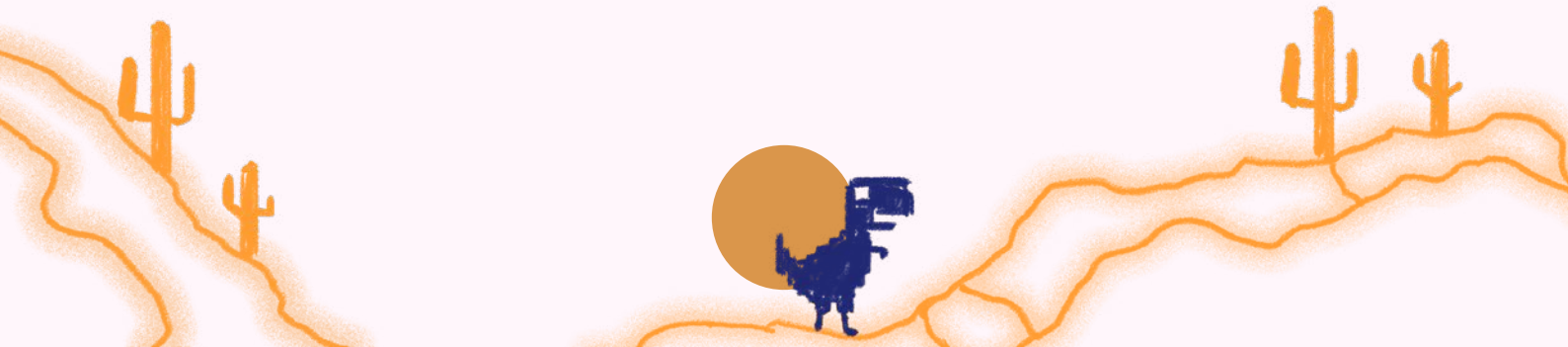
OONI. (2024). Evidence of Telegram blocking in El Salvador. Open Observatory of Network Interference. https://explorer.ooni.org/findings/26818990400

ELIMINACIÓN DE DOMINIOS .NI: UNA NUEVA FORMA DE CENSURA EN NICARAGUA

Norman Antonio García Aguilar

Ingeniero en Telemática, especializado en seguridad informática y en la administración de servidores y redes. A lo largo de su trayectoria, ha trabajado en auditorías informáticas y en la implementación de políticas de seguridad orientadas a proteger el flujo de datos y garantizar la integridad de la información en entornos digitales.

Su trabajo se sitúa en la intersección entre la informática y los derechos humanos, con énfasis en temas como la censura en Internet, la gobernanza de Internet y los mecanismos que inciden en la libertad de expresión en línea.



Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

RESUMEN

En marzo de 2025, nic.ni, el administrador de registro de los dominios de nivel superior de Nicaragua, adscrito a la Secretaría General de la Universidad Nacional de Ingeniería (UNI), eliminó sin previo aviso los registros de nombre de dominio .ni de cinco medios digitales independientes, afectando su identidad en Internet y limitando el derecho de acceso a la información a la ciudadanía. Esta acción se enmarca en una política estatal sistemática contra la prensa, que incluye acoso, ataques digitales y censura. Algunos medios estaban preparados ante este escenario y contaban con dominios globales alternativos, pero otros fueron obligados a rediseñar estrategias de comunicación y de presencia en Internet.

Organizaciones y activistas en derechos digitales confirmaron la eliminación mediante pruebas técnicas, denunciaron el caso y generaron espacios de colaboración para compartir herramientas de evasión y seguridad digital. Aunque este incidente fue denunciado ante la Organización de Apoyo para Nombres con Código de País (ccNSO), que desarrolla políticas para los dominios de código país, esta se declaró sin competencia directa sobre decisiones internas del administrador de dominios en Nicaragua. A pesar de las limitaciones institucionales y financieras, se han impulsado campañas de denuncia y acompañamiento a medios afectados. Según informes de PCIN (Periodistas y Comunicadores Independientes de Nicaragua), los ataques digitales van en aumento, por lo que es necesario un análisis de riesgos y amenazas, protección proactiva y participación en espacios de gobernanza de Internet para defender la libertad de expresión en el país.

PALABRAS CLAVE:

Nicaragua, dominios, censura.

Este documento fue realizado en el marco del proyecto CADE – Civil Society Alliances for Digital Empowerment. Ver más en https://cadeproject.org/

Esta publicación está cofinanciada por la Unión Europea. Su contenido es responsabilidad exclusiva de Fundación Karisma y no refleja necesariamente las opiniones de la Unión Europea.

INTRODUCCIÓN

En marzo de 2025, la división de tecnologías de la información de la Universidad Nacional de Ingeniería de Nicaragua, administradora del dominio de nivel superior geográfico correspondiente a Nicaragua (nic.ni), eliminó, sin previo aviso, los registros de servidores de nombre de dominio de cinco medios de comunicación digital. Esto representa una afectación directa a estos medios para conservar su identidad nicaragüense en el mundo digital y una arbitrariedad en detrimento de la libertad de expresión.

El Estado de Nicaragua ha mantenido una política de ataque en contra del periodismo en el país. Intimidaciones, ataques físicos y a sitios web, acoso digital y fiscal, expropiaciones y órdenes de cierres, son algunas de las estrategias usadas para atacar a los medios de comunicación nicaragüenses , lo que ha obligado a equipos periodísticos a exiliarse.

ANTECEDENTES Y DESARROLLO

En este documento abordaremos este incidente partiendo de los antecedentes de censura digital en el país, así como las implicaciones de la censura con sus problemas y las posibles recomendaciones para mitigar riesgos derivados.

En 2022, el proyecto South Lighthouse logró documentar, de forma técnica, irregularidades en antenas de telefonía celular para uso de antenas falsas o imsi-catchers (dispositivos usados por terceros actores para hacer vigilancia telefónica) en diferentes puntos del país. Estas, presuntamente, son usadas para la vigilancia de la ciudadanía (Confidencial, 2024). Otras investigaciones como las de Surveillance Watch han documentado la compra de equipo de espionaje telefónico ruso como SORM-3 (Surveillance Watch, s.f.) y otras investigaciones periodísticas han evidenciado la existencia de estos sistemas en el país (Infobae, 2024).

En el informe de PCIN del 2024, de enero del 2024 a febrero del 2025, se identificaron los ataques virtuales contra periodistas y medios de comunicación como un nuevo patrón en crecimiento, con el objetivo de usar nuevos mecanismos para silenciar a la prensa crítica (PCIN, 2025).

Sobre el sistema de nombres de dominios

El sistema de nombres de dominios (DNS) es el directorio de Internet. Las personas acceden a la información en línea a través de nombres de dominio como google.com o yahoo.com. Los navegadores web interactúan mediante direcciones de protocolo de Internet (IP). Los servidores DNS traducen los nombres de dominio a direcciones IP para que los navegadores puedan cargar los recursos de Internet.

Esta guía, o directorio de dominios, se mantiene mediante un listado de registros de Internet: los registros Whois, que son ampliamente utilizados e identifican quién posee un dominio y cómo ponerse en contacto con ellos. La Corporación de Internet para la Asignación de Nombres y Números (ICANN) regula el registro y la propiedad de los nombres de dominio. Los registros Whois han demostrado ser bastante útiles, convirtiéndose en un recurso esencial para mantener la integridad del proceso de registro de nombres de dominio y propiedad de sitios web.

Un nombre de dominio consta de una o más partes, técnicamente llamadas etiquetas, que se concatenan convencionalmente y se delimitan por puntos, como ejemplo.com. La etiqueta más a la derecha transmite el dominio de nivel superior; por ejemplo, el nombre de dominio www.ejemplo.com pertenece al dominio de nivel superior .com, por lo tanto, lo más importante está al final del dominio.

La extensión de un sitio web corresponde a una designación definida en el momento que se creó el Sistema de Nombres de Dominios. Tiene dos grupos que pueden ir juntos, o por separado, después del nombre de dominio.

El primer grupo corresponde a los dominios territoriales, basado en dos caracteres que identifican el país de acuerdo con las abreviaciones ISO-3166. Este grupo es denominado ccTLD (country code top level domain o dominio de nivel superior geográfico). Ejemplos de extensión ccTLD:

- **.ni para servicios de Nicaragua**
- **.co para servicios de Colombia**
- **.sv para servicios de El Salvador**
- **.ar para servicios de Argentina**
- **.hn para servicios de Honduras**

Los ccTLD son funcionales para identificar la región a la que pertenece un sitio web y su contenido, lo cual tiene varios beneficios. Por ejemplo, para un eCommerce, facilita identificar el país al que pertenece la tienda online y permite a los usuarios saber si pueden comprar con su moneda local y recibir el producto sin tener que coordinar un envío del exterior.

El segundo grupo es denominado gTLD (generic Top Level Domain o Dominios de Nivel Superior genéricos). Representa una serie de nombres y multiorganizaciones.

La administración de las bases de datos o directorio para los dominios de nivel superior geográfico, o ccTLD, se delega a instituciones ubicadas en los respectivos países, que pueden variar desde universidades, empresas privadas a organizaciones sin fines de lucro. Cada entidad registradora de un ccTLD establece sus propias políticas para el registro de dominios y mantiene autonomía sobre la gestión del directorio local.

La situación de los nombres de dominios en Nicaragua

En 1989, se le adjudicó a la Universidad Nacional de Ingeniería la administración de los dominios .ni, a través del nic.ni, y lo ha mantenido hasta la fecha. La UNI es una universidad estatal que responde a intereses del Gobierno de Nicaragua.

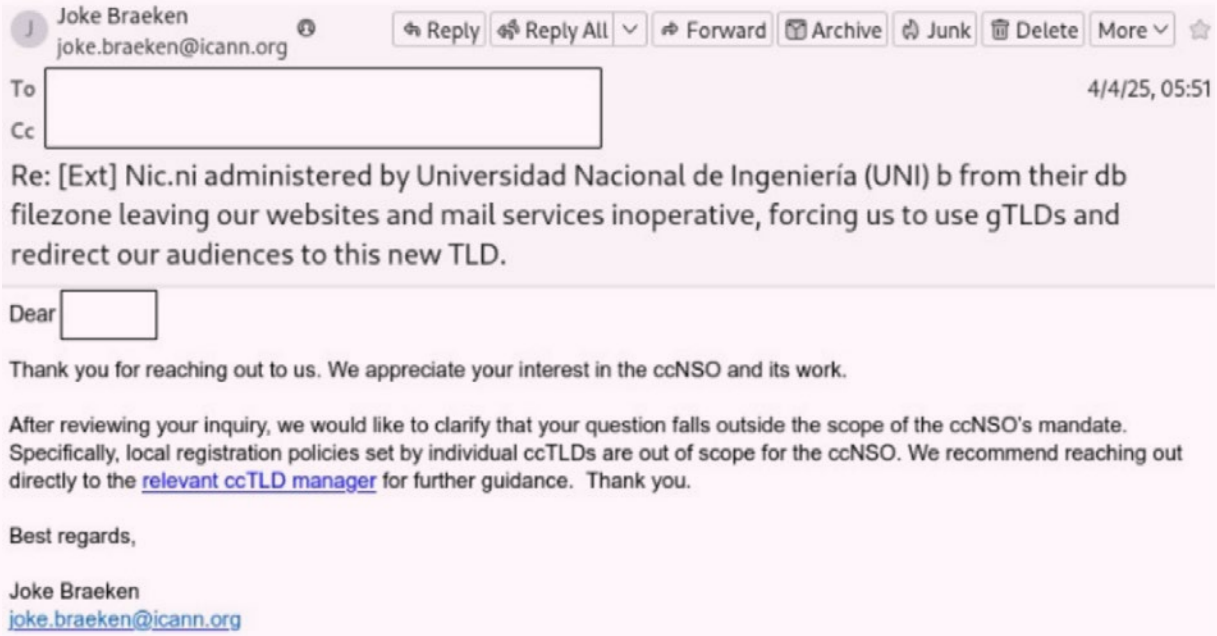
La situación sociopolítica actual de Nicaragua está marcada por un régimen autoritario, encabezado por el copresidente Daniel Ortega y su esposa, la copresidenta Rosario Murillo. Desde las protestas masivas de 2018, el Gobierno ha intensificado la represión contra la oposición, la sociedad civil y los medios independientes, recurriendo al encarcelamiento, el exilio forzado y al retiro de la ciudadanía a disidentes. Las elecciones han sido ampliamente cuestionadas por su falta de transparencia y pluralismo, consolidando un poder prácticamente absoluto. Además, la militarización del Estado y el cierre de organizaciones no gubernamentales han aislado más al país de la comunidad internacional, profundizando una crisis de derechos humanos y gobernabilidad (El País, 2025).

En este escenario, se esperaba que, como otro acto de represión contra los medios independientes, se les privara del derecho de usar dominios ccTLD para posicionar localmente sus medios con una marca nicaragüense. Si bien algunos medios digitales ya tenían un plan preventivo y habían adquirido dominios globales secundarios (gTLD) que ya usaban activamente, otros anticipaban que el Gobierno iniciaría nuevos métodos de censura pero no habían comenzado a usar sus gTLD secundarios. A través de esta acción se ha impedido a los medios independientes mantener su identidad nacional en internet mediante el dominio .ni, lo que los obliga a redirigir a su audiencia a un nuevo dominio y a replantear su estrategia de difusión para que el público pueda seguir accediendo a su contenido (Amnesty International, 2024).

La eliminación sin previo aviso de estos nombres de dominio evidencian que el Estado nicaragüense inició un nuevo tipo de ataque contra el periodismo y la libertad de expresión, así como hacia el derecho de la ciudadanía a mantenerse informada. Otros medios de comunicación y organizaciones de sociedad civil deberán prepararse ante este tipo de ataques.

A raíz de este incidente, grupos y personas activistas en la defensa de los derechos digitales realizaron un análisis técnico sobre lo sucedido y determinaron que efectivamente el nic.ni había eliminado los registros de servidores de nombre de sus bases de datos y, posteriormente, eliminó el registro del sistema Whois. También, en colaboración con organizaciones y personas activistas, se contactó a los medios de comunicación afectados y se realizaron reuniones virtuales para socializar y compartir experiencias y herramientas que puedan usarse para evadir la censura y mantener su presencia en Internet, así como determinar otros riesgos que puedan presentarse.

Uno de los acuerdos de estas reuniones fue la redacción de una carta dirigida al ccNSO, con el fin de documentar y exponer el caso. Esta carta fue bien recibida por el personal de ccNSO, pero su respuesta oficial indicó que no era su competencia, ya que solo desarrollan políticas y no pueden interferir en las decisiones de las organizaciones que administran los dominios a nivel país.



Joke Braeken
joke.braeken@icann.org

Reply | Reply All | Forward | Archive | Junk | Delete | More

To
Cc

4/4/25, 05:51

Re: [Ext] Nic.ni administered by Universidad Nacional de Ingeniería (UNI) b from their db filezone leaving our websites and mail services inoperative, forcing us to use gTLDs and redirect our audiences to this new TLD.

Dear

Thank you for reaching out to us. We appreciate your interest in the ccNSO and its work.

After reviewing your inquiry, we would like to clarify that your question falls outside the scope of the ccNSO's mandate. Specifically, local registration policies set by individual ccTLDs are out of scope for the ccNSO. We recommend reaching out directly to the relevant ccTLD manager for further guidance. Thank you.

Best regards,

Joke Braeken
joke.braeken@icann.org

Figura 1. Correo en respuesta a la carta enviada a la ccNSO

Dada la autonomía con la que cuentan los administradores de dominios de código país, considerando el contexto represivo de Nicaragua y el constante ataque hacia la libertad de expresión y el acceso a la información, no se espera que el nic.ni restablezca los dominios.

RETOS PARA LA INCIDENCIA

Las medidas tomadas hasta el momento abarcan la denuncia pública, capacitaciones para identificar riesgos, estrategias y procedimientos que ayuden a prepararse ante estos ataques, así como la incidencia dentro de espacios de gobernanza de Internet como LACNIC (Registro de Direcciones de Internet de América Latina y Caribe) y LACIGF (Foro de Gobernanza de Internet de América Latina y el Caribe), para exponer el caso y plantear la necesidad de una revisión de las políticas existentes.

Es necesario el apoyo de activistas en derechos digitales que acompañen a las organizaciones de sociedad civil y medios de comunicación en la protección y reserva de su identidad en Internet, para así mitigar las amenazas derivadas de estos ataques.

Como es mencionado por el PCIN en su informe (2025), el Estado de Nicaragua está incrementando sus ataques digitales a la libertad de expresión, por lo que es fundamental hacer un análisis de riesgos digitales del gremio periodístico en Nicaragua para identificar y, de manera preventiva, iniciar procesos de protección en seguridad digital que permitan anticiparse y mitigar estos ataques.

La participación en espacios de toma de decisión para la administración de nombres como ccNSO, grupos de usuarios At-Large a través de LACRALO (Latin American and Caribbean Islands Regional At-Large Organization) y foros como el LACIGF es un factor importante que ayudaría a buscar soluciones, en donde se le puede exigir responsabilidad a los entes administradores de los dominios de primer nivel de código país.

De manera proactiva, un constante monitoreo técnico del estado de dominios .ni aportaría a identificar la baja de un dominio de parte del nic.ni y funcionaría como mecanismo de documentación y alerta para detectarlo de manera temprana. Esto se puede realizar a través de la herramienta OONI, con apoyo de organizaciones y personas interesadas.

La denuncia pública de estos ataques de censura genera una mayor conciencia colectiva nacional e internacional, por lo que es importante mantener estas campañas de denuncia pública ante la censura digital.

El acompañamiento, capacitación y asistencia técnica ante incidentes digitales como estos son estrategias necesarias para guiar y brindar mejores herramientas de protección digital a los medios de comunicación. Es importante mantener lazos de colaboración con diversas organizaciones que puedan apoyar ante esta nueva ola de ataques digitales.

REFERENCIAS

Confidencial. (2024, abril 29). Descubren 39 antenas falsas que vigilan celulares en Nicaragua. Confidencial. https://confidencial.digital/nacion/descubren-39-antenas-falsas-que-vigilan-celulares-en-nicaragua/

Surveillance Watch. (s.f.). Rohde & Schwarz in Nicaragua. Surveillance Watch. https://www.surveillancewatch.io/?entity=Rohde+%26+Schwarz&country=Nicaragua

Infobae. (2024, octubre 1). Centros de espionaje rusos en Latinoamérica: Cerro Mokorón,

SORM-3 y los efectos en la región. https://www.infobae.com/america/america-latina/2024/10/01/centros-de-espionaje-rusos-en-latinoamerica-cerro-mokoron-sorm-3-y-los-efectos-en-la-region/

PCIN. (2025, febrero 24). Informe sobre el estado de la libertad de prensa en Nicaragua. Periodistas y Comunicadores Independientes de Nicaragua. https://pcinnicaragua.org/wp-content/uploads/2024/08/PCIN-24-febrero-2025-1.pdf

El País. (2025, marzo 16). La última ofensiva de Ortega contra la prensa: el régimen bloquea el dominio ".com.ni" de cinco medios independientes de Nicaragua. https://elpais.com/america/2025-03-16/la-ultima-ofensiva-de-ortega-contra-la-prensa-el-regimen-bloquea-el-dominio-comni-de-cinco-medios-independientes-de-nicaragua.html

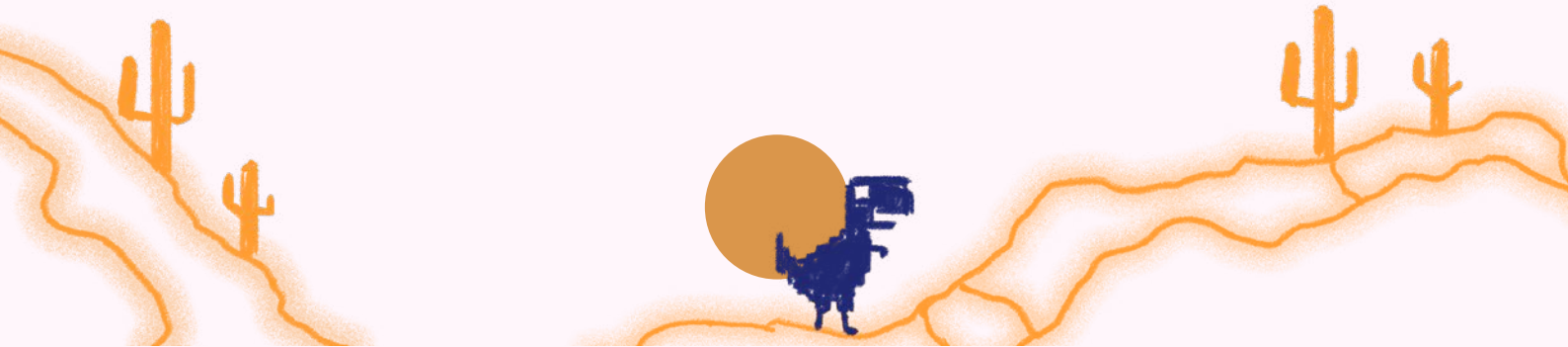
Amnesty International. (2024, diciembre 17). Nicaragua: Cierra el año con represión sistemática y perfeccionamiento de la estrategia estatal contra cualquier forma de disidencia (Índice AMR 43/8834/2024). https://www.amnesty.org/es/documents/amr43/8834/2024/es/

INTERRUPCIONES DEL INTERNET EN CUBA:

CENSURA, CRISIS Y DERECHOS VULNERADOS (2020–2025)

Diktyon Cuba

Grupo independiente dedicado al monitoreo de la censura digital, la salud de Internet y el estado de la conectividad en Cuba. A través de mediciones técnicas y análisis de datos abiertos, el grupo documenta las restricciones al acceso a la información y las interrupciones en la conectividad que afectan a las personas usuarias dentro de la isla.



Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

RESUMEN

Este caso de estudio analiza los apagones y microcortes de internet ocurridos en Cuba, entre 2020 y 2025, en contextos de protestas sociales, fallos del sistema eléctrico y desastres naturales. A través del registro de doce eventos significativos se evidenció un patrón sistemático de interrupciones del servicio por parte del Estado, especialmente durante manifestaciones ciudadanas, con el objetivo de limitar la organización social, frenar la difusión de información y controlar la narrativa pública. Además, se examinó cómo la fragilidad de la infraestructura eléctrica y de telecomunicaciones agrava la desconexión digital, afectando de forma desproporcionada a comunidades vulnerables y profundizando la brecha digital. Las afectaciones en derechos humanos, particularmente la libertad de expresión, el derecho a la información y la participación ciudadana, son un eje central del análisis. Este artículo también resalta la importancia de documentar estas prácticas de censura digital, así como los desafíos para incidir en espacios regionales de gobernanza de Internet desde contextos autoritarios. Finalmente, se plantea la necesidad de reformas estructurales, mayor transparencia y colaboración regional para proteger los derechos digitales en Cuba y prevenir que estas prácticas se repliquen en otros países de América Latina.

PALABRAS CLAVE:

Cuba, apagones de internet, censura digital, derechos humanos, protestas sociales.

Este documento fue realizado en el marco del proyecto CADE – Civil Society Alliances for Digital Empowerment. Ver más en https://cadeproject.org/

Esta publicación está cofinanciada por la Unión Europea. Su contenido es responsabilidad exclusiva de Fundación Karisma y no refleja necesariamente las opiniones de la Unión Europea.

INTRODUCCIÓN

En los últimos años, Cuba ha experimentado múltiples interrupciones en el servicio de internet, incluyendo apagones totales y microcortes selectivos, en un contexto marcado por protestas sociales, fallos estructurales del sistema eléctrico y fenómenos naturales extremos. Estas interrupciones no son meramente técnicas o accidentales, en numerosos casos, se han implementado de manera deliberada por parte del Estado como estrategia para contener la organización ciudadana y limitar la difusión de información.

El acceso a internet en Cuba ha sido históricamente controlado y costoso pero desde la introducción del internet móvil en 2018, la población ha logrado una mayor conectividad. Sin embargo, este avance ha estado acompañado de nuevas formas de censura digital. Entre 2020 y 2025 se han documentado al menos doce eventos significativos en los que el acceso a internet fue restringido parcial o totalmente, muchos de ellos en momentos de gran tensión social.

Estas acciones han tenido un impacto directo en los derechos humanos, especialmente en la libertad de expresión, el derecho a la información, la participación política y la libertad de reunión pacífica. La desconexión deliberada priva a la ciudadanía de herramientas fundamentales para ejercer sus derechos y evidencia la necesidad urgente de mecanismos de protección regional e internacional.

ANTECEDENTES Y DESARROLLO

El acceso a Internet en Cuba ha estado históricamente condicionado por un fuerte control estatal. Aunque la conectividad comenzó a expandirse lentamente desde finales de los años noventa, no fue hasta 2013 que se habilitaron puntos públicos de acceso gestionados por la estatal ETECSA (Empresa Estatal de Telecomunicaciones de Cuba). La llegada del internet móvil en 2018 fue celebrada como un hito, pero vino acompañada de precios elevados, vigilancia constante y frecuentes interrupciones del servicio. Esta infraestructura limitada y controlada se ha utilizado como un mecanismo de censura, especialmente durante momentos de tensión social.

Entre 2020 y 2025 se han documentado al menos doce eventos significativos en los que se interrumpió parcial o totalmente el acceso a internet, ya sea como respuesta deliberada del Estado ante manifestaciones sociales o como consecuencia de fallos estructurales del sistema eléctrico o desastres naturales. A continuación, se presentan estos casos, documentados por medios independientes como Cubanet, Cibercuba y Yucabyte, así como por plataformas de monitoreo como IODA y por el equipo Diktyon Cuba.

27 de noviembre de 2020: Bloqueo de redes sociales por protesta en San Isidro, La Habana

El Movimiento San Isidro, compuesto por artistas y disidentes, protagonizó una huelga en La Habana para exigir la liberación del rapero Denis Solís. En respuesta, el Gobierno de Cuba bloqueó el acceso a redes sociales como Facebook, Instagram y YouTube, con el objetivo de impedir la transmisión en directo del desalojo de los activistas. Según CiberCuba, esta acción buscaba evitar la coordinación de los manifestantes y frenar la cobertura internacional, esto evidencia el uso de la censura digital como herramienta de control (CiberCuba, 2020).

27 de enero de 2021: Corte por protesta en el Ministerio de Cultura

Una manifestación frente al Ministerio de Cultura en La Habana, liderada por artistas y activistas del grupo 27N, demandaba mayor libertad de expresión. El gobierno cortó el acceso a internet para frenar la organización y visibilidad del evento. CiberCuba reportó que las autoridades intensificaron la censura digital (Gonzales, 2021), afectando plataformas como WhatsApp y redes sociales.

11 de julio de 2021: Apagones masivos por protestas nacionales

Las protestas del 11J, las más grandes en décadas, se extendieron por varias ciudades,

17 de marzo de 2024: Microcortes por protestas en el oriente cubano

Ante las protestas en pueblos de la región oriental, como Santiago de Cuba, motivadas por la escasez de alimentos y electricidad, se presentaron microcortes selectivos de internet. Yucabyte reportó que estas interrupciones se focalizaron en zonas de mayor agitación social (Diktyon, 2024), lo que evidencia un uso cada vez más preciso de la censura digital.

18 de octubre de 2024: Apagón por colapso eléctrico y huracán

Un fallo del sistema eléctrico nacional, agravado por el paso de un huracán por el oriente del país, provocó un apagón general en el servicio de internet. Según Diktyon, la combinación de la crisis energética y el desastre natural colapsó la infraestructura de telecomunicaciones especialmente en La Habana, exigiendo mejoras económicas y libertades políticas. El gobierno implementó cortes generalizados de internet para evitar la difusión de videos y convocatorias. Yucabyte señaló que ETECSA, la empresa estatal de telecomunicaciones bloqueó servicios de mensajería y redes sociales, afectando a millones de usuarios (Yucabyte, 2021).

15 de julio de 2022: Corte por protestas en Pinar del Río y La Habana

Protestas en Los Palacios, Pinar del Río, y en el Parque del Curita, en La Habana, motivadas por problemas económicos y cortes eléctricos, llevaron a un nuevo apagón de internet. Según Yucabyte, el gobierno buscaba contener la escalada de manifestaciones (Yucabyte, 2022), utilizando cortes selectivos en las zonas afectadas para limitar la comunicación.

30 de septiembre de 2022: Protestas por apagón eléctrico prolongado

Tras un apagón eléctrico masivo que dejó a varias regiones sin servicio por más de tres días, ciudadanos protestaron en diferentes puntos del país. El gobierno cortó internet para evitar la organización de nuevas manifestaciones. Cubanet destacó que las protestas reflejaban el creciente descontento por la crisis energética y económica (2022).

1 de octubre de 2022: Continuación de los cortes por protestas

Las protestas iniciadas a finales de septiembre continuaron y el gobierno mantuvo los cortes de internet para controlar la situación. Cibercuba informó que los apagones digitales se concentraron en áreas urbanas (2022) donde las manifestaciones eran más visibles, afectando la comunicación entre activistas.

6 de mayo de 2023: Corte por protestas en Caimanera

Durante protestas en el municipio de Caimanera, Guantánamo, motivadas por la escasez de alimentos y servicios básicos, se registró un corte de internet. Según Proyecto Inventario, la interrupción coincidió con la difusión en redes sociales de videos de las manifestaciones (Proyecto Inventario, 2023), lo que sugiere una acción deliberada para frenar la circulación de información.(Dikyton y IODA, 2024), dejando a la población incomunicada durante días.

6 de noviembre de 2024: Corte por el huracán Rafael

El paso del huracán Rafael causó interrupciones en el servicio de internet debido a daños en la infraestructura eléctrica y de telecomunicaciones. Cubanet señaló que las autoridades priorizaron la recuperación de servicios básicos, dejando el acceso a internet en segundo plano (González, 2024), lo que afectó la comunicación en zonas golpeadas por el huracán.

4 de diciembre de 2024: Apagón por nuevo fallo eléctrico

Otro colapso del sistema eléctrico nacional derivó en un apagón de Internet a nivel nacional. CiberCuba reportó que la fragilidad de la infraestructura eléctrica cubana, sumada a la falta de mantenimiento, fue la causa principal (2024), afectando no solo el acceso a internet, sino también la economía digital.

14 de marzo de 2025: Apagón por fallo eléctrico

Un nuevo fallo del sistema eléctrico provocó otro apagón masivo de internet. Según El País, este evento reflejó la persistente crisis energética del país (2025), con consecuencias graves para la conectividad y la comunicación, especialmente en un contexto de creciente dependencia de internet para actividades cotidianas.

DISCUSIÓN DESDE LOS RETOS PARA LA INCIDENCIA

El contexto cubano representa un desafío extremo para la incidencia en espacios de gobernanza de Internet. Dentro del país, las organizaciones de la sociedad civil enfrentan una vigilancia constante, criminalización de la disidencia y restricciones a la libertad de asociación, lo que limita gravemente su capacidad de acción pública. Por ello, muchas de las denuncias sobre apagones digitales y censura han tenido que canalizarse desde el exilio o a través de redes informales de documentación, como las impulsadas por medios independientes, activistas digitales y grupos como Diktyon Cuba.

Uno de los principales obstáculos para la incidencia internacional es la falta de reconocimiento institucional y de recursos para participar en espacios multilaterales como el Foro de Gobernanza de Internet (IGF) o sus versiones regionales (LACIGF). Además, el propio acceso limitado a internet en Cuba impide que muchas personas estén al tanto de estos espacios o puedan participar de forma efectiva en ellos.

En este contexto, la colaboración con organizaciones aliadas como Fundación Karisma (Colombia), IODA, YucaByte, Cubanet, Diario de Cuba y Ve Sin Filtro (Venezuela) ha sido clave para documentar y visibilizar los cortes de internet, fortalecer procesos de monitoreo y análisis técnico, y generar redes de apoyo y trabajo conjunto. Estas alianzas han permitido dar mayor legitimidad y difusión a los casos documentados, aunque los desafíos para sostener una participación constante y articulada en espacios de incidencia internacional aún persisten.

La experiencia acumulada en estos años sugiere que es necesario seguir fortaleciendo las capacidades técnicas, de documentación y de comunicación estratégica de los actores cubanos y caribeños, especialmente aquellos que operan desde contextos autoritarios o con limitaciones severas. También, es fundamental generar rutas de entrada más accesibles a los espacios de gobernanza de Internet para personas y grupos sin experiencia previa, incluyendo formación específica en incidencia internacional, mecanismos de financiamiento y alianzas regionales que sirvan como plataformas de respaldo.

CONCLUSIONES Y RECOMENDACIONES

Los apagones y microcortes de internet en Cuba entre 2020 y 2025 no pueden entenderse como fallos aislados ni meramente técnicos. Se trata de una estrategia estatal de control social en momentos clave, especialmente durante protestas, que vulnera derechos fundamentales como la libertad de expresión, la información y la participación ciudadana. A su vez, la precariedad de la infraestructura tecnológica y energética del país agrava la desconexión, con consecuencias profundas para la vida cotidiana, la economía digital y la brecha tecnológica.

Frente a esta realidad, es urgente visibilizar la situación de Cuba en los espacios regionales de gobernanza de Internet. La comunidad internacional y regional debe priorizar mecanismos que incluyen a actores de contextos represivos, ofreciendo acompañamiento técnico, formación y protección. A nivel nacional, se requiere promover un marco legal y político que garantice el acceso a Internet como derecho humano y que limite el uso arbitrario de apagones digitales. Esto implica exigir mayor transparencia a ETECSA y documentar sistemáticamente cada caso de interrupción del servicio.

Recomendamos crear redes de documentación colaborativa en la región, con metodologías accesibles para quienes trabajan en condiciones de riesgo. Asimismo, los foros regionales deben generar mecanismos más inclusivos para que organizaciones emergentes puedan incidir, aunque no cuenten con respaldo institucional. La lucha por los derechos digitales en Cuba es parte de una causa regional y requiere alianzas, solidaridad y visibilidad constante.

REFERENCIAS

CiberCuba. (2024, diciembre 4). Apagón general en Cuba provoca caída masiva de la conexión a Internet. https://www.cibercuba.com/noticias/2024-12-04-u1-e43231-s27061-nid293231-apagon-general-cuba-provoca-caida-masiva-conexion

CiberCuba. (2020, noviembre 27). Movimiento San Isidro: Cubanos proponen que el 26 noviembre sea el Día de la Vergüenza Nacional. CiberCuba. https://www.cibercuba.com/noticias/2020-11-27-u1-e192519-s27061-movimiento-san-isidro-cubanos-proponen-26-noviembre-dia

CiberCuba. (2022, octubre 1). Gobierno corta acceso a internet tras segunda jornada de protestas en Cuba. https://www.cibercuba.com/noticias/2022-10-01-u1-e207888-s27061-gobierno-corta-acceso-internet-tras-segunda-jornada-protestas

CubaNet. (2022, septiembre 30). Gobierno cubano corta el servicio de internet tras manifestaciones populares de este jueves. https://www.cubanet.org/gobierno-cubano-corta-el-servicio-de-internet-tras-manifestaciones-populares-de-este-jueves/

DiktyonYucaByte. (2024, marzo 17). Protestas en Santiago de Cuba y microcortes de internet. YucaByte. https://www.yucabyte.org/2024/12/31/apagones-internet-cuba-2024/

Diktyon Cuba y IODA. (2024, octubre 18). Cuba enfrenta apagones y cortes de Internet tras falla de la red eléctrica nacional. https://ioda.inetintel.cc.gatech.edu/reports/cuba-enfrenta-apagones-y-cortes-de-internet-tras-falla-de-la-red-electrica-nacional/

El País. (2025, marzo 15). Un nuevo apagón deja a Cuba a oscuras en su peor crisis energética en décadas. https://elpais.com/america/2025-03-15/un-nuevo-apagon-deja-a-cuba-a-oscuras-en-su-peor-crisis-energetica-en-decadas.html

González, M. (2021, enero 27). Gobierno corta datos móviles de los teléfonos en Cuba. CiberCuba. https://www.cibercuba.com/noticias/2021-01-27-u185759-e185759-s27061-gobierno-corta-datos-moviles-telefonos-cuba

González, P. (2024). Plataformas registraron caída de internet en Cuba tras el apagón de este miércoles. Cubanet. https://www.cubanet.org/plataformas-registraron-caida-de-internet-en-cuba-tras-el-apagon-de-este-miercoles/

Proyecto Inventario. (2023, junio 5). Caimanera: primera trinchera de la censura digital para frenar una revuelta nacional. https://proyectoinventario.org/caimanera-primera-trinchera-censura-digital-apagon-internet-cuba-6-mayo-2023/

The Guardian. (2024, noviembre 6). Cuba hit by second nationwide blackout as Hurricane Rafael makes landfall. https://www.theguardian.com/world/2024/nov/06/cuba-blackout-hurricane-rafael

YucaByte. (2021, julio 12). #11J: bloqueo de internet y redes para esconder las protestas en Cuba. https://www.yucabyte.org/2021/07/12/11j-internet-cuba/

YucaByte. (2022, julio 15). 15J: protestas en Cuba y apagón de internet. https://www.yucabyte.org/2022/07/15/15j/

CENSURA EN INTERNET EN VENEZUELA DURANTE ELECCIONES PRESIDENCIALES: BLOQUEO DE MEDIOS, HERRAMIENTAS ANTICENSURA Y SERVIDORES DNS PÚBLICOS (JULIO 2024 - ENERO 2025)

Organización VE Sin Filtro

Dedicada a la defensa y promoción de los derechos humanos en el entorno digital. Su trabajo abarca el diagnóstico, la documentación y la mitigación de la censura en internet, así como el fortalecimiento de capacidades tecnológicas en organizaciones de la sociedad civil, activistas y comunidades, con el objetivo de promover el acceso seguro, libre e informado a internet y a las tecnologías digitales.

Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

RESUMEN

Durante el período electoral venezolano, de julio de 2024 a enero de 2025, se incrementaron en un 87% los bloqueos de dominios por ocho proveedores de servicios de internet (ISP) principales, afectando medios de comunicación, herramientas anticensura y servidores DNS públicos, mediante técnicas DNS, HTTP/HTTPS y TCP IP aplicadas arbitrariamente. Esta censura gubernamental buscaba controlar la información y reprimir la disidencia, vulnerando derechos humanos y la democracia en el país. A pesar de estrategias ciudadanas de evasión como el uso de VPN, el aumento de la censura generó represión digital. Iniciativas como Noticias Sin Filtro y Operación Retuit, junto con programas de seguridad digital y herramientas de participación política como Toma el Control, buscan mitigar esta situación. Sin embargo, la falta de transparencia gubernamental representa un desafío persistente que requiere alianzas y estrategias innovadoras.

PALABRAS CLAVE:

Venezuela, censura en internet, derechos humanos, bloqueos de dominios, herramientas anticensura, servidores DNS bls.

Este documento fue realizado en el marco del proyecto CADE – Civil Society Alliances for Digital Empowerment. Ver más en https://cadeproject.org/

Esta publicación está cofinanciada por la Unión Europea. Su contenido es responsabilidad exclusiva de Fundación Karisma y no refleja necesariamente las opiniones de la Unión Europea.

INTRODUCCIÓN

Durante el periodo electoral presidencial en Venezuela, que abarcó desde el inicio de la campaña en julio de 2024 hasta la posesión en enero de 2025, se observó un aumento significativo en la censura en internet, con un incremento del 87% en el total de dominios bloqueados. Las categorías más afectadas fueron las relacionadas con el anonimato y anticensura, alojamiento, blogging y noticias. Estos bloqueos fueron implementados por, al menos, ocho de los principales proveedores de servicios de internet (ISP) en Venezuela, incluyendo la empresa estatal CANTV. Las técnicas de bloqueo utilizadas incluyeron el bloqueo de tipo DNS, HTTP/HTTPS y TCP IP, aplicadas de manera arbitraria y sin transparencia.

Durante el periodo electoral el gobierno venezolano demostró un claro esfuerzo por censurar la información en internet y dificultar los intentos de evasión de censura. Al bloquear sitios de noticias, limitó el acceso a información crucial y coartó la libertad de expresión durante un período crítico para la democracia venezolana. Desde 2007 hay registro de estas prácticas, la ciudadanía ha desarrollado estrategias para evadir la censura, como el uso de VPN y el cambio de configuración de DNS. Sin embargo, en esta ocasión, incluso sitios web de VPN y servidores DNS públicos fueron afectados.

La censura en internet durante el período electoral vulneró gravemente derechos humanos fundamentales como la libertad de expresión, el acceso a la información, la libertad de prensa, la participación política, la libertad de asociación y la seguridad digital, limitando la capacidad de la ciudadanía para informarse y participar en el proceso electoral. Estas prácticas generaron un clima de intimidación y miedo, afectando la seguridad e integridad personal de quienes expresaron sus opiniones. Estas acciones contravienen los estándares internacionales de derechos humanos y debilitan los principios esenciales de un proceso electoral justo y democrático, evidenciando un intento de controlar la información y reprimir la disidencia.

ANTECEDENTES Y DESARROLLO

Venezuela, bajo el gobierno autocrático de Nicolás Maduro, desde 2013 experimenta concentración del poder, debilitamiento institucional y una creciente oposición, inicialmente fragmentada. El gobierno controla las principales instituciones estatales, como el poder judicial y el Consejo Nacional Electoral (CNE) que enfrenta un creciente rechazo a nivel nacional e internacional debido a acusaciones de corrupción, represión y mala gestión económica (Mijares, 2024).

El 28 de julio de 2024 se celebraron elecciones presidenciales en Venezuela, seis años después de los comicios del 20 de mayo de 2018 en los que Nicolás Maduro fue reelecto, en concordancia con el período constitucional de seis años establecido en el artículo 230 de la Constitución (Asamblea Nacional de Venezuela, 1999). En estas elecciones participaron Nicolás Maduro y el candidato opositor Edmundo González Urrutia, quien representó a María Corina Machado tras su inhabilitación.

En este contexto, la censura en Internet se consolidó como una herramienta política para el control social en Venezuela, institucionalizada a través de organismos y leyes que supervisan y penalizan la libertad de expresión. Esta práctica es cuestionada por organizaciones nacionales e internacionales como una forma de represión. Un estudio de Medianálisis revela que solo una minoría de los ciudadanos se siente bien informada (20%), mientras que la mayoría se siente poco o nada informada, y un 73% teme represalias por expresar opiniones políticas. Esta represión digital reduce la participación ciudadana y debilita la democracia al limitar la capacidad de los ciudadanos para supervisar al gobierno e involucrarse en la vida pública, lo que impacta negativamente la estabilidad democrática del país (Navarro, 2024).

Freedom House califica a Venezuela como “no libre”, siendo el segundo país de América con la menor clasificación de esta evaluación después de Cuba (Agarwal et al., 2024). A su vez la Relatoría Especial para la Libertad de Expresión (RELE) de la Comisión Interamericana de Derechos Humanos (CIDH) señala que los bloqueos en Internet son parte de un patrón sistemático del gobierno para controlar la narrativa pública, restringir el flujo de información, silenciar voces críticas y dificultar la movilización y la protesta social (RELE, 2025).

La regulación y censura de contenido en Internet en Venezuela tiene evidencias desde 2007, cuando días después del cierre del canal privado de televisión RCTV, las estaciones de radio en línea Radionexx y CaracasRadioTV fueran bloqueadas por CANTV (Kelly y Cook, 2018). A inicios de 2016, IPYS Venezuela, basándose en datos de Venezuela Inteligente, reportó al menos 37 sitios bloqueados; luego en el 2017 por primera vez la organización Freedom House calificó como “no libre” a Venezuela en su reporte Freedom On The Net 2017 (Huici e Iglesias, 2022). En mayo del mismo año, el decreto presidencial N° 2849 estableció un estado de excepción que permitió la regulación y vigilancia de contenidos en internet con la justificación de proteger la economía nacional y combatir campañas de desestabilización (VE Sin Filtro, 2017).

Desde VE Sin Filtro se han denunciado diversas estrategias de censura dirigidas a iniciativas políticas, incluyendo campañas de phishing contra voluntariados de ayuda humanitaria (Azpúrua y Guerra, 2019), así como bloqueos de plataformas de redes sociales durante protestas y eventos políticos. Incluso el sitio coronavirusvenezuela.info, una plataforma organizada por la Asamblea Nacional y Juan Guaido, fue bloqueado durante la pandemia (VE Sin Filtro, 2020).

Durante el período electoral presidencial de julio de 2024 a enero de 2025, se registró un notable aumento del 87% en la censura en internet en Venezuela, elevándose inicialmente a 227 dominios bloqueados, aunque esta cifra descendió a 180 al final del período. Esta censura persistió tras la cuestionada reelección de Nicolás Maduro y las posteriores protestas por descontento social y rechazo electoral a nivel nacional e internacional. El bloqueo continuo de plataformas digitales y medios independientes se mantuvo como una estrategia de control para restringir la difusión de información, la libertad de expresión, y la capacidad de organización y protesta, creando un entorno favorable para la desinformación y campañas de influencia destinadas a manipular a los venezolanos y desalentar a la oposición.

Antes de las elecciones del 28 de julio, aproximadamente 60 medios de comunicación en línea ya estaban bloqueados, lo que debilitó el panorama mediático, especialmente crítico en un contexto electoral. Tras la campaña y las elecciones, la censura se intensificó, afectando a redes sociales, aplicaciones de mensajería, servidores DNS públicos y sitios web de VPN.

Entre julio y agosto de 2024, se bloquearon 13 dominios de sitios de noticias, incluyendo plataformas de verificación de hechos como Cazadores de Fake News y Es Paja. Después del anuncio de los resultados electorales y las protestas subsiguientes, se implementaron nuevos bloqueos que afectaron a sitios como elecciones2024venezuela (donde se especulaba que el equipo opositor comandoVZLA publicaría las actas electorales), La Prensa Lara, The Wall Street Journal, Versión Final, La República (Perú) y Vendata.org.

La censura también se extendió a herramientas de evasión como VPN y servidores DNS públicos. Antes del proceso electoral, Tunnelbear y Psiphon ya estaban bloqueados. Durante el mismo, se sumaron Proton VPN y Windscribe después de ofrecer sus servicios de forma gratuita. Entre julio de 2024 y enero de 2025, se registraron 58 nuevos bloqueos a herramientas de evasión, incluyendo 26 sitios web de VPN, el Proyecto Tor y 30 servidores DNS públicos.

A partir de enero de 2025, se implementaron restricciones a servidores DNS públicos, afectando a usuarios de CANTV, el más importante proveedor de internet residencial y empresa estatal. Durante estos bloqueos, quienes habían configurado el uso de estos servidores para eludir algunos bloqueos quedaron sin conexión efectiva a internet en los días previos a la toma de posesión presidencial; a menos que regresaran a la configuración DNS por defecto, mientras la inmensa mayoría de los afectados no sabía por qué no funcionaba su conexión a internet (VE Sin Filtro, 2025).

La Comisión Nacional de Telecomunicaciones (CONATEL) en Venezuela ordenó a los ISP aplicar la censura en internet de manera opaca, en decisiones de oficio que son arbitrarias y no cumplen con los estándares de derechos humanos. Se observa un aumento en la censura aplicada por proveedores de internet más pequeños y una multiplicación y diversificación en las técnicas de bloqueo. Anteriormente, la mayoría de proveedores aplicaban bloqueos DNS, siendo únicamente CANTV y Movistar quienes implementan bloqueos HTTP/HTTPS y DNS simultáneamente. Sin embargo, ahora diferentes ISP también utilizan múltiples técnicas de manera simultánea para aumentar su efectividad y dificultar la evasión, incluyendo bloqueos TCP/IP.

Para que exista una democracia, se requieren al menos tres condiciones fundamentales: libertad de expresión, participación informada y acceso a diversas fuentes de información. Estos elementos son indispensables para ejercer de manera efectiva la principal manifestación democrática: el voto (Navarro, 2024). En Venezuela, estos tres requisitos se vieron comprometidos por la censura en internet, lo que consecuentemente debilita la calidad de la democracia en el país.

DISCUSIÓN DE LOS PROBLEMAS DESDE LOS RETOS PARA LA INCIDENCIA

La censura en internet en Venezuela, evidenciada por el bloqueo de dominios de medios en los últimos años, ha impulsado la creación de proyectos y alianzas dentro de la sociedad venezolana. Un ejemplo exitoso es Noticias Sin Filtro, una aplicación desarrollada por Conexión Segura y Libre en colaboración con medios nacionales. Lanzada antes de las elecciones del 28 de julio de 2024, esta aplicación permite acceder a noticias de medios bloqueados sin necesidad de una VPN.

Además, los medios han buscado alternativas fuera de sus sitios web, como la difusión de noticias en papelógrafos en espacios públicos y el desarrollo de canales o bots informativos en WhatsApp y Telegram. Durante las elecciones y las protestas posteriores, varios medios venezolanos se unieron a la Operación Retuit. Una iniciativa que utiliza avatares generados por inteligencia artificial para proteger la identidad de los periodistas al compartir información en redes sociales, evitando así la persecución gubernamental.

También existen estrategias de información offline hiperlocales como El Bus TV, que lleva noticias a los pasajeros de autobuses, demostrando los esfuerzos para superar la censura en internet. Estas organizaciones han demostrado una gran capacidad de adaptación, desarrollando rápidamente nuevas herramientas y estrategias en respuesta a los cambios impuestos por la censura.

Algunas empresas de herramientas de evasión de censura, en respuesta a la denuncia del aumento de eventos de bloqueos en Venezuela, en el mes de julio de 2024, ofrecieron sus servicios gratuitos para usuarios en el país. Sin embargo, esta iniciativa fue saboteada al bloquearse 30 dominios pertenecientes a plataformas de VPN.

Organizaciones de la sociedad civil como Conexión Segura y Libre y Redes Ayuda desarrollan programas educativos para mantener informada a la comunidad venezolana sobre temas de seguridad digital. Estos esfuerzos ayudan a mitigar amenazas y proteger la información, asegurando que personas líderes y ciudadanos puedan seguir informando sin comprometer su integridad al navegar en Internet.

En Venezuela, la falta de figuras creíbles en el poder obstaculiza cambios legales y judiciales contra estos abusos. La documentación existente sobre la censura ha sido proporcionada por VE Sin Filtro y por organizaciones locales e internacionales como la RELE de la CIDH y la Oficina del Alto Comisionado de los Derechos Humanos, entre otros. Su difusión se ha realizado para concientizar y denunciar. Sin embargo, el costo político y reputacional para detener este abuso es insuficiente, salvo excepciones.

El abordaje de la censura en internet en Venezuela ha enfrentado múltiples retos. Aunque se han implementado acciones exitosas, como el desarrollo de nuevas iniciativas, la capacitación sobre seguridad digital y la denuncia ante organizaciones internacionales, persisten desafíos significativos. La falta de transparencia y la resistencia del gobierno a reconocer estas prácticas dificultan la incidencia efectiva. Es necesario fortalecer las alianzas y seguir desarrollando estrategias nuevas e innovadoras.

CONCLUSIONES Y RECOMENDACIONES

La censura en internet en Venezuela representa un desafío significativo para la libertad de expresión, el acceso a la información y la participación política. A pesar de los esfuerzos implementados por diversas organizaciones y la sociedad civil, la censura continúa siendo una barrera que afecta los derechos humanos y la democracia en el país. Sin embargo, las acciones desarrolladas hasta ahora han demostrado que es posible innovar y adaptarse a este entorno restrictivo.

Organizaciones venezolanas demuestran gran adaptabilidad ante la censura con herramientas y estrategias innovadoras como Noticias Sin Filtro y Operación Retuit. La colaboración entre organizaciones a nivel local, nacional e internacional es crucial para el éxito de estas iniciativas. A pesar de los avances, la censura persiste por la falta de transparencia y resistencia gubernamental, lo que requiere el desarrollo continuo de estrategias y el fortalecimiento de alianzas.

RECOMENDACIONES

1. ***Fortalecimiento las capacidades en seguridad digital:*** continuar desarrollando programas educativos y talleres sobre seguridad digital para periodistas, activistas y ciudadanos. Esto incluye la creación de guías claras y accesibles sobre el uso de herramientas de evasión de censura.

2. ***Innovación en herramientas tecnológicas:*** seguir innovando en el desarrollo de aplicaciones y tecnologías que permitan acceder a información de manera segura y eficiente. Esto incluye la mejora continua de aplicaciones como Noticias Sin Filtro y la exploración de nuevas tecnologías emergentes.

3. ***Ampliación de las alternativas de difusión offline:*** expandir iniciativas como El Bus TV y otras formas de difusión offline para llegar a comunidades con acceso limitado a internet. Esto puede incluir el uso de radios comunitarias, periódicos impresos y otros medios tradicionales.

4. ***Denuncia y presión internacional:*** continuar denunciando la censura en foros internacionales y colaborar con organizaciones de derechos humanos para presionar al gobierno venezolano a cesar estas prácticas. La visibilización del problema a nivel global es crucial para generar apoyo y encontrar soluciones.

5. ***Desarrollo de políticas y normativas:*** trabajar con otros países de la región y organismos internacionales para desarrollar políticas y normativas que protejan los derechos digitales y promuevan un internet libre y abierto.

6. ***Creación de espacios de discusión:*** establecer y participar en espacios de discusión y colaboración para compartir experiencias, aprender de otros y desarrollar nuevas soluciones. Estos espacios pueden ser tanto locales como internacionales y deben incluir a diversos actores, desde organizaciones de la sociedad civil hasta instituciones académicas y medios de comunicación.

REFERENCIAS

Agarwal, A., Barak, M., Brody, J., Grothe, C., Loldj, M., Masinsin, M., y Sutterlin, E. (2024, octubre). Freedom on the net 2024. Freedom House. https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf

Asamblea Nacional de Venezuela. (1999). Constitución de la República Bolivariana de Venezuela. Gaceta Oficial.

Azpúrua, A., y Guerra, C. (2019, febrero 15). Phishing impulsado por el gobierno de Venezuela pone en riesgo a activistas y usuarios de internet. VE Sin Filtro. https://vesinfiltro.org/noticias/Phishing_impulsado_por_gobierno_de_Venezuela/

Huici, H., e Iglesias, R. H. (2022, noviembre). Bloqueados: La práctica de los "bloqueos" en internet y tres estudios de caso latinoamericanos. Lacnic. https://descargas.lacnic.net/lideres/2022/lacnic-lideres_hectorhuici.pdf

Kelly, S., y Cook, S. (2018, abril 18). Freedom on the net 2011: A global assessment of internet and digital media. Freedom House. https://freedomhouse.org/sites/default/files/2020-02/FOTN_2011_Booklet.pdf

Mijares, V. (2024). Legitimacy crisis and Venezuela's long road to democratic transition (GIGA Focus Latin America, No. 4). German Institute for Global and Area Studies (GIGA). https://doi.org/10.57671/gfla-24042

Navarro, Y. R. (2024, enero 29). Percepción de la censura y la autocensura: efectos en el ejercicio de la condición ciudadana. Medianálisis. https://www.medianalisis.org/percepcion-de-la-censura-y-la-autocensura-efectos-en-el-ejercicio-de-la-condicion-ciudadana/

Nuvan R., L. C. (2022). Capitalismo de la vigilancia y censura en internet: Estudio aplicado a la democracia y el autoritarismo en los casos de Estados Unidos y Myanmar. Pontificia Universidad Javeriana, Facultad de Ciencias Políticas y Relaciones Internacionales. https://apidspace.javeriana.edu.co/server/api/core/bitstreams/a6d30db8-83d4-40fd-bfa7-06babff16cfe/content

Relatoría Especial para la Libertad de Expresión. (2025, mayo). RELE advierte sobre el grave deterioro del ecosistema mediático en Venezuela y urge al Estado a respetar y garantizar la libertad de expresión y de prensa (No. R088/25). Comisión Interamericana de Derechos Humanos. https://www.oas.org/es/CIDH/jsForm/?File=%2Fes%2Fcidh%2Fexpresion%2Fprensa%2Fcomunicados%2F2025%2F088.asp

VE Sin Filtro. (2017, mayo). Comunicado sobre limitaciones a los derechos fundamentales en internet a propósito del estado de excepción en Venezuela. https://vesinfiltro.org/noticias/comunicado_regional_2017-05-26/

VE Sin Filtro. (2020, marzo). Bloquean sitio sobre coronavirus COVID-19 organizado por la AN y Juan Guaidó. https://vesinfiltro.org/noticias/bloqueado_portal_coronavirus_AN

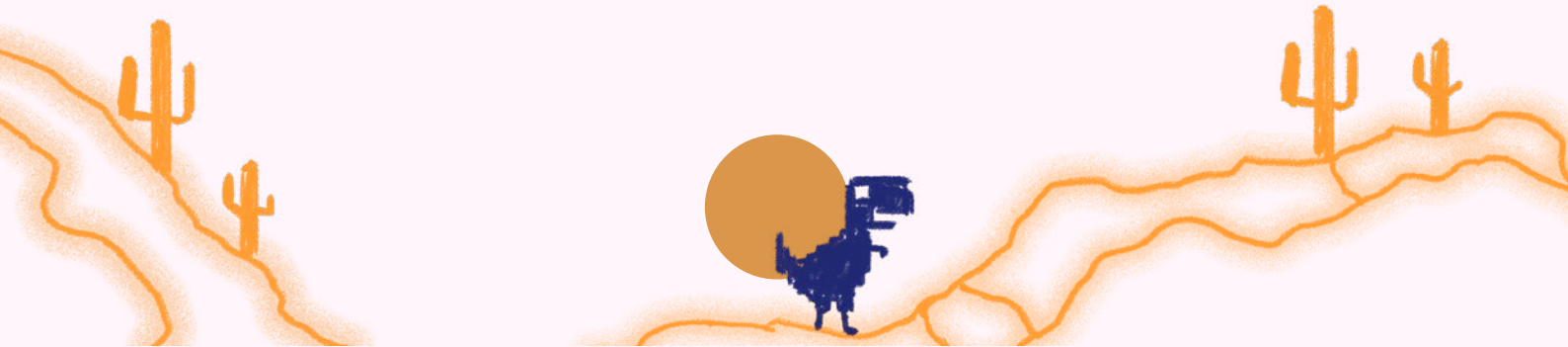
VE Sin Filtro. (2025). Redes de control: Informe sobre censura y represión digital en las elecciones presidenciales en Venezuela. https://vesinfiltro.org/noticias/2025-03-12-reporte-elecciones-presidenciales/

CORTES TOTALES DE INTERNET EN QUIBDÓ, CHOCÓ

Luis Delascar Valencia Mena

CIO de Dirsoft y profesional en el área de tecnología. Es docente en la Universidad Uniclaretiana y en la Universidad Tecnológica del Chocó. Cuenta con amplia experiencia en el desarrollo de soluciones digitales, el liderazgo de equipos de ingeniería y la formulación de proyectos de innovación. Su trayectoria se ha enfocado en la aplicación de inteligencia artificial, la transformación digital y el desarrollo de plataformas tecnológicas orientadas al impacto social, especialmente en territorios como el Chocó.

Ha liderado iniciativas en sectores como la educación, el gobierno digital y el desarrollo sostenible, integrando tecnologías emergentes para mejorar la toma de decisiones, optimizar procesos y fortalecer capacidades locales. Asimismo, cuenta con experiencia en la estructuración de proyectos bajo metodologías ágiles y marcos de inversión pública, articulando actores institucionales, académicos y comunitarios.



Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

RESUMEN

Durante los últimos años el municipio de Quibdó, capital del departamento del Chocó en Colombia, ha enfrentado múltiples episodios de cortes totales del servicio de internet, que han afectado profundamente la vida social, económica, educativa y de acceso a la información de sus habitantes. En este caso de estudio se sistematiza la información documentada sobre estas disrupciones, sus causas multifactoriales: fenómenos climáticos, fallos en infraestructura de conectividad débil, aislamiento geográfico, daños o vandalismo intencional a la única línea principal de conexión de fibra óptica y deficiencias en el suministro eléctrico que genera impacto social derivado. También se resalta cómo estas interrupciones afectan derechos humanos fundamentales, como el acceso a la información, a la comunicación, a la educación y la participación ciudadana en todo el departamento. Además, se recopilan y exploran los retos para la gobernanza de Internet en la región y las acciones gubernamentales y comunitarias emprendidas para mitigar el problema, como la instalación de nueva infraestructura y el fortalecimiento de redes alternativas. Este análisis busca visibilizar la problemática estructural de la desconexión en Quibdó y proponer recomendaciones para garantizar derechos digitales y mejorar la resiliencia de la conectividad en la región.

PALABRAS CLAVE:

Quibdó, cortes de internet, derechos humanos, conectividad, gobernanza digital.

Este documento fue realizado en el marco del proyecto CADE – Civil Society Alliances for Digital Empowerment. Ver más en https://cadeproject.org/

Esta publicación está cofinanciada por la Unión Europea. Su contenido es responsabilidad exclusiva de Fundación Karisma y no refleja necesariamente las opiniones de la Unión Europea.

INTRODUCCIÓN

En primera instancia, este documento presenta un panorama general acompañado de un análisis contextual y una revisión de antecedentes relevantes. A continuación, se documentan y sistematizan diversos casos representativos de caídas del servicio de internet. Posteriormente, se presenta un análisis de latencia como documentación técnica que evidencia una de estas caídas. Finalmente, se abordan los principales desafíos en materia de gobernanza digital y se formulan recomendaciones estratégicas orientadas a fortalecer la continuidad del servicio y garantizar el ejercicio pleno de los derechos digitales.

Quibdó, capital del departamento del Chocó en Colombia, enfrenta desde hace años problemas severos de conectividad a Internet, que abarcan cortes totales, caídas prolongadas y bloqueos intermitentes del servicio. Cada tipo de disrupción afecta particularmente la vida en esta región, pero todas comparten la sensación de que el internet en Quibdó a veces parece tener “vida propia”.

En el contexto de la expansión global de las tecnologías digitales, el acceso a internet se ha convertido en un derecho esencial para el ejercicio de múltiples libertades fundamentales. Sin embargo, esta realidad dista de ser cierta en regiones como el Chocó.

Según información del DANE (2024) en este departamento solo el 18% de hogares cuenta con internet: 9,2% fijo y 11,5% móvil. A pesar de estas cifras, en el Chocó, solo el 43,4% de la población se conecta, 66,2% en cabeceras municipales y 25,7% en centros poblados y zonas rurales dispersas. Estos valores están lejos de los promedios nacionales.

A la baja conectividad, se suman los cortes totales severos, al igual que las caídas prolongadas y los bloqueos intermitentes en el servicio de internet; que han provocado la interrupción de procesos educativos, comerciales, administrativos y de salud, afectando a una población, de por sí, históricamente marginada.

Un corte total es como si alguien hubiera bajado todas las conexiones a Internet de golpe. Nada funciona: ni mensajes, ni páginas, ni llamadas. Es la desconexión absoluta, como si el mundo digital se hubiera esfumado y el tiempo se detuviera, dejando a las personas completamente incomunicadas por horas, días o, incluso, semanas; sometidas al silencio digital mientras se espera. Porque se sabe que eventualmente regresará, pero agota la incertidumbre de no saber cuándo vuelve.

Los bloqueos intermitentes son los más impredecibles; la conexión a internet va y viene sin avisar, en un momento funciona perfectamente y al siguiente se cae repentinamente. Se cree que todo va a funcionar bien, pero justo cuando más se necesita, el internet decide fallar, dejando a las personas con una sensación de frustración que solo entiende quien la ha vivido.

Es importante indicar que los problemas técnicos en Quibdó se derivan principalmente de una infraestructura de telecomunicaciones débil y vulnerable, resultado de factores geográficos y sociales. En particular, la ciudad cuenta con un único canal de fibra óptica, haciéndola altamente susceptible a interrupciones. Esta limitación se agrava debido a los frecuentes actos de sabotaje y vandalismo sobre las redes, lo que genera fallos recurrentes en los servicios de comunicación y conectividad. La dependencia de un solo canal no solo reduce la capacidad de respuesta ante emergencias, sino también dificulta el desarrollo económico y social de la región, al limitar el acceso a herramientas digitales esenciales para la educación, el trabajo y la comunicación desde la región.

Las disrupciones son frecuentes y se presentan con duraciones que van desde varias horas hasta días, afectando tanto a proveedores móviles como fijos y a la mayoría de la población (Botero, 2024). Las causas son múltiples, incluyen condiciones climáticas extremas que provocan cortes eléctricos prolongados, daños intencionales a la infraestructura de fibra óptica, y deficiencias en la redundancia y mantenimiento de las redes (Impacto TIC, 2023).

Estas interrupciones impactan directamente a los derechos humanos esenciales como el derecho a la información, la educación, la participación política y la comunicación, especialmente en un contexto donde Internet es un medio clave para denunciar violencia y acceder a servicios básicos. La desconexión prolongada profundiza la brecha digital y la exclusión social, afectando especialmente a comunidades vulnerables y rurales. Por lo tanto, esta situación debe entenderse como un problema estructural que requiere atención urgente y necesaria desde la gobernanza de internet y políticas públicas orientadas a garantizar los derechos digitales y la inclusión tecnológica.

ANTECEDENTES Y DESARROLLO

La infraestructura de conectividad en Chocó, a pesar de contar con proyectos de fibra óptica y redes de alta velocidad en las cabeceras municipales, enfrenta limitaciones serias en la cobertura y calidad del servicio. Solo un pequeño porcentaje de la población accede a internet, dejando de lado las zonas rurales, que permanecen mayormente desconectadas. En Quibdó se han documentado múltiples episodios de cortes totales de internet, con reportes recientes sobre desconexiones de hasta tres días; como en noviembre de 2023, debido a un daño intencional en la fibra óptica. Otros cortes han estado asociados a tormentas y fallos eléctricos que dejaron sin energía a la ciudad por más de 12 horas, afectando la operación de estaciones base y equipos de red (OBI, 2024).

Tabla 1. Cortes de internet más relevantes en los últimos años en Quibdó

N.	Fecha del corte	Duración	Alcance	Causa principal	Pronunciamientos oficiales	Consecuencias destacadas
1	Noviembre de 2023	3 días	Quibdó y zonas aledañas	Sabotaje a la red de fibra óptica (Azteca Comunicaciones)	Alcaldía de Quibdó solicitó apoyo para reparación	Interrupción de servicios bancarios, educativos y administrativos
2	Agosto de 2022	14 horas	Quibdó y municipios cercanos	Tormenta eléctrica y falla en red eléctrica	Azteca Comunicaciones reportó la restauración	Caída total del servicio, afectación en hospitales y centros de emergencia
3	Marzo de 2021	36 horas	Cabeceras municipales del Chocó	Falla técnica en nodo troncal de Azteca	Comunicado técnico escueto de Azteca Comunicaciones	Interrupción de servicios ciudadanos y de emergencia
4	Septiembre de 2020	4–8 horas diarias × 3 días	Quibdó y municipios del departamento	Posible restricción durante protestas sociales	Gobernación del Chocó pidió investigación	Afectación a conectividad de instituciones educativas y gubernamentales
5	Julio de 2019	20 horas	Quibdó y corregimientos interconectados	Sobrecarga + mantenimiento no programado	No hubo pronunciamiento oficial	Trámites virtuales suspendidos, afectación a bancos y educación en época de matrículas

Los cortes de internet en Quibdó no son hechos aislados ni recientes. Al menos desde 2017, se han documentado episodios frecuentes en los que el municipio ha quedado sin acceso a internet durante horas, días o incluso semanas. Organizaciones como Fundación Karisma y reportes de medios regionales y nacionales han dado cuenta de cómo, en varias ocasiones, los cables de fibra óptica fueron cortados por grupos armados o delincuencia común. En algunos casos, los proveedores de servicio han confirmado que no existen rutas de respaldo, lo que amplifica la vulnerabilidad del sistema.

En 2022, por ejemplo, Quibdó experimentó un apagón digital de más de 72 horas, lo que provocó la suspensión de clases virtuales, la inoperancia de sistemas bancarios y administrativos y afectaciones graves a procesos judiciales y de salud que dependían de sistemas conectados.

Durante el último año, el monitoreo técnico realizado mediante sondas RIPE Atlas ha permitido identificar patrones de microcaídas y desconexiones prolongadas, evidenciando que las interrupciones no solo responden a fallos técnicos, sino también a factores externos como condiciones climáticas adversas y actos de vandalismo (OBI, 2024a). La coincidencia de algunas caídas con eventos políticos o de seguridad sugiere la necesidad de un seguimiento más riguroso para detectar posibles bloqueos intencionales o manipulaciones del servicio (OBI, 2024b).

Los informes del Observatorio de Bloqueos de Internet (OBI) de Karisma, disponibles en sus enlaces oficiales, proporcionan un análisis detallado de cómo las mediciones realizadas en Quibdó, Chocó, permiten detectar y comprender las microcaídas en el servicio de internet ocurridas en agosto de 2024. Gracias a una red de sondas que emplean herramientas como ping, traceroute y pruebas HTTP, se identificaron interrupciones breves pero que impactan la calidad de la conectividad, incluso sin producir cortes totales. Estos datos revelan que no todas las fallas en la red tienen una causa estructural evidente; algunas, como en el primer evento, parecen estar vinculadas a problemas eléctricos ocasionados por tormentas; mientras que otras, como la del segundo evento, podrían deberse a causas relacionadas con la infraestructura de red o eventos específicos, en este caso, una visita oficial del Gobierno.

El concepto de microcaída, poco explorado a nivel global, ayuda a entender esas interrupciones sutiles y localizadas que afectan el derecho a la conectividad en contextos donde la estabilidad del servicio es crucial. La detección de estas microcaídas mediante monitoreo constante evidencia que no siempre las causas son visibles o estructurales, por lo que resulta fundamental ampliar la red de sondas, fortalecer los sistemas de medición en tiempo real y promover la colaboración con proveedores y autoridades. Incrementar estos esfuerzos permitirá no solo detectar con mayor precisión estas interrupciones, sino también entender sus causas, facilitando la formulación de políticas públicas más efectivas para garantizar un acceso a internet estable, equitativo y de calidad en regiones marginadas como el Chocó.

En términos de derechos humanos, la desconexión afecta la dignidad, la igualdad y el acceso a servicios esenciales, como la educación y la salud, además de limitar la capacidad de la población para ejercer su derecho a la libertad de expresión y a la participación ciudadana (Acuña, 2022). La falta de conectividad también agrava la vulnerabilidad social en un departamento marcado por problemas históricos de pobreza, corrupción y violencia.

La crisis de conectividad en Quibdó, Chocó, puede entenderse en gran parte gracias a las evidencias y mediciones recogidas por las sondas del Observatorio de Bloqueos de Internet. Estos registros permiten establecer que la infraestructura de la región depende en gran medida de un único operador: Azteca Comunicaciones. La existencia de una única línea de conexión y un solo proveedor crea una vulnerabilidad significativa, ya que cuando este operador se enfrenta a fallas o interrupciones en su servicio, toda la región queda desprotegida. La dependencia exclusiva a un operador hace que las microcaídas y fallas en su infraestructura tengan un impacto directo y casi total en la conexión de la comunidad, evidenciando la fragilidad del sistema actual.

Frente a esta situación, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha anunciado medidas para responder a esta crisis. Entre ellas, se destaca la inversión en la instalación de 172 nuevas antenas y la construcción de una segunda línea de conexión que busca reducir la dependencia frente a Azteca y fortalecer la resistencia de la red en la región. Sin embargo, la implementación de estas soluciones enfrenta desafíos importantes, como las dificultades logísticas y sociales derivadas de la geografía del territorio y las condiciones de seguridad en la zona. Para garantizar una conectividad más estable, confiable y equitativa en el Chocó, es necesario continuar con estas inversiones y adoptar enfoques coordinados y sostenidos que superen los obstáculos existentes.

MEDICIONES DE CONEXIÓN Y LATENCIA EN EL SERVICIO DE INTERNET EN QUIBDÓ

La ciudad de Quibdó, Chocó, enfrenta una realidad difícil con respecto a su conexión a internet. La necesidad de estar conectados es fundamental para actividades diarias como estudiar, trabajar y acceder a servicios básicos; sin embargo, los datos de medición, como los registrados por la plataforma RIPE Atlas, muestran que la calidad del servicio es muy precaria. Frecuentemente, la señal desaparece por largos periodos y, en ocasiones, la conexión se detiene por completo, o la velocidad es tan baja que tareas simples, como videollamadas o acceder a plataformas educativas, se vuelven imposibles. Por ejemplo, en diciembre de 2024, la ciudad estuvo hasta tres días sin internet, lo que paralizó actividades y afectó a miles de personas.

Estas interrupciones se reflejan en los niveles de latencia (el tiempo que tarda un paquete en viajar y regresar) y en la pérdida de datos, generando que navegar sea lento, frustrante o, incluso, imposible. Esto no es solo un problema técnico; limita el acceso a la información, la educación y la participación social, derechos fundamentales de toda población. La principal causa de esta fragilidad es que Quibdó depende exclusivamente de una sola empresa proveedora de internet por fibra óptica, Azteca Comunicaciones, que ha enfrentado dificultades financieras y técnicas. Además, la infraestructura está saturada y es vulnerable a daños, lo que provoca fallas prolongadas y cortes masivos. Aunque el gobierno ha anunciado proyectos para mejorar la situación, como la instalación de una segunda línea de fibra y nuevos puntos de acceso, los retrasos e incumplimientos en los plazos mantienen a la comunidad en una situación de vulnerabilidad digital.

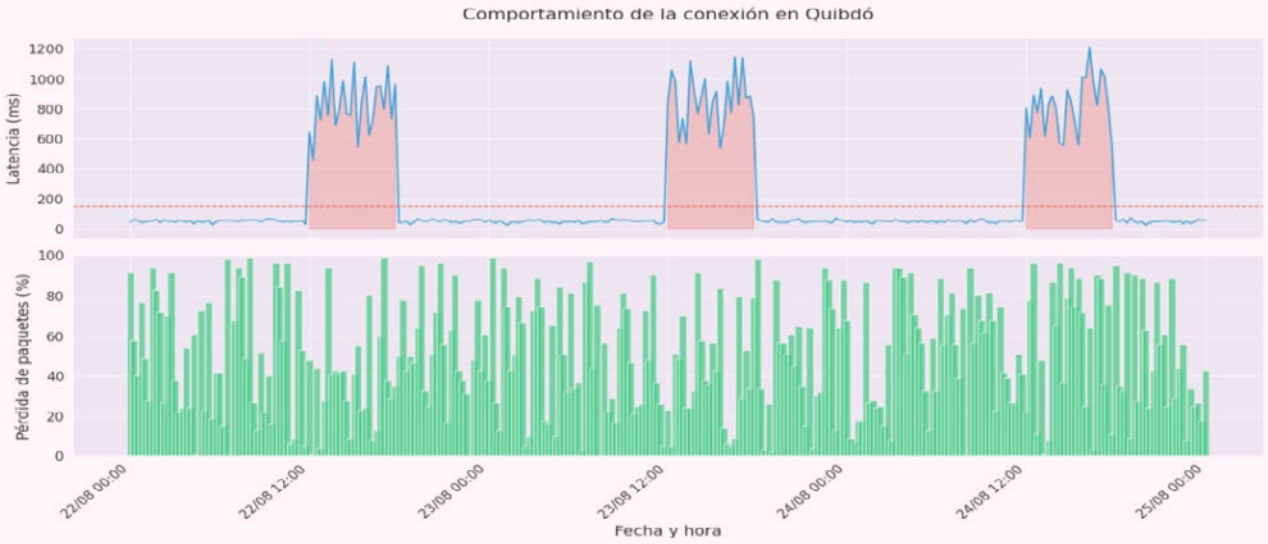


Figura 2. Comportamiento de la conexión en Quibdó (Abril - Julio de 2025)

Estadísticas clave:

- **Latencia máxima: 1209 ms**
- **Pérdida máxima: 99%**
- **Tiempo con latencia >150 ms: 18 horas**

Así, se puede concluir que la conectividad en Quibdó sigue siendo frágil. Para cambiar esto es necesario fortalecer la infraestructura, diversificar los proveedores y garantizar una gestión transparente y participativa, priorizando el acceso universal y la calidad del servicio para reducir la brecha digital en la región.

DISCUSIÓN DE LOS PROBLEMAS DESDE LOS RETOS PARA INCIDENCIA EN GOBERNANZA

La desconexión digital en Quibdó es una grave barrera al desarrollo humano. Enfrentarla con decisión y creatividad desde el territorio permitirá no solo resolver una necesidad urgente, sino también construir un modelo participativo de soberanía tecnológica para las regiones históricamente excluidas. Por último, y no menos importante, es necesario aclarar que estas recomendaciones deben implementarse coordinadamente entre el gobierno nacional, autoridades locales, operadores de telecomunicaciones y la sociedad civil; donde se consideren tanto los aspectos técnicos como sociales y de derechos humanos integralmente.

El abordaje de la problemática de los cortes de internet en Quibdó enfrenta múltiples retos en los espacios de gobernanza digital. Por un lado, la falta de información sistematizada y transparente dificulta la incidencia efectiva y la formulación de políticas públicas adecuadas. Aunque existen esfuerzos de monitoreo técnico y algunas acciones gubernamentales, la coordinación con actores locales, comunidades y organizaciones de la sociedad civil es limitada.

Las acciones exitosas incluyen la reciente intervención del MinTIC para acelerar la instalación de infraestructura y la apertura de convocatorias para proveedores locales, lo cual puede fortalecer la diversidad y competencia en el mercado de servicios de internet (MinTIC, 2024). Sin embargo, persisten dificultades en la implementación debido a factores como la inseguridad, vandalismo, falta de capacidades técnicas y de recursos en la región para participar activamente en espacios de gobernanza de Internet.

De esta manera, el panorama ha cambiado con la incorporación de tecnologías de monitoreo y la visibilización pública de los cortes, fallos, disrupciones y demás acciones que afecten los servicios de comunicación. Esto ha permitido un mayor conocimiento del problema y ha concretado una presión para construir soluciones estructurales. No obstante, las incidencias requieren que se fortalezcan las capacidades locales para una mejor participación en gobernanza digital, incluyendo formación técnica, acceso a información y alianzas estratégicas con organizaciones nacionales e internacionales.

CONCLUSIONES Y RECOMENDACIONES

La situación de desconexión recurrente en Quibdó es una violación sistemática de derechos humanos y una muestra de cómo las brechas digitales agravan las desigualdades históricas. Más que un problema técnico, se trata de un fenómeno estructural que requiere una atención urgente desde una perspectiva de justicia social, territorial y tecnológica. De esta manera se recomienda lo siguiente:

Implementar soluciones técnicas estructurales como la segunda línea de fibra óptica y la instalación de antenas adicionales para garantizar redundancia y resiliencia en la red. Fortalecer el monitoreo continuo y transparente de la conectividad para detectar y responder rápidamente a interrupciones, incorporando tecnología y participación ciudadana en el proceso.

Generar capacidades locales a través de la formación técnica y política en derechos digitales y gobernanza de internet para líderes comunitarios y organizaciones sociales del Chocó.

Articularse con redes nacionales e internacionales en aras de lograr participar en espacios de incidencia y discusión como el Foro de Gobernanza de Internet, en Colombia, Latinoamérica y global, la Coalición de Derechos Digitales o la coalición #KeepItOn liderada por Access Now, entre otros, para amplificar la voz del territorio y sumar apoyo técnico y político sobre los temas de cortes y bloqueos de internet.

Desarrollar estrategias de protección y mantenimiento de la infraestructura, incluyendo medidas de seguridad para prevenir actos de vandalismo y daños intencionales a la red. Garantizar la protección de los derechos digitales como parte integral de los derechos humanos, promoviendo el acceso universal a Internet como un servicio esencial para la vida en sociedad.

REFERENCIAS

Access Now. (2023). #KeepItOn: Informe anual de apagones de internet 2022.
Acuña Guerrero, R. E. (2022). El PAE en Chocó: Derechos humanos y corrupción.

Universidad Católica de Colombia [Tesis de grado]. https://repository.ucatolica.edu.co/server/api/core/bitstreams/03fb9165-d5bb-481e-b41e-1149cba732c3/content

Azteca Comunicaciones Colombia. (2021). Boletín técnico interno – Nodo Chocó https://aztecacomunicaciones.com.co

Botero Cabrera, C. (2024). Más información para enfrentar la desconexión del Chocó. El Espectador. https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/mas-informacion-para-enfrentar-la-desconexion-del-choco/

Caracol Radio. (2023, noviembre). Sabotaje deja sin internet a Quibdó por tres días. https://caracol.com.co

Consonante. (2024). Azteca, la empresa detrás del monopolio del internet en el Chocó. https://consonante.org/noticia/azteca-la-empresa-detras-del-monopolio-del-internet-en-el-choco/

Departamento Administrativo Nacional de Estadística (DANE). (2024). Boletín técnico: Indicadores básicos de tenencia y uso de tecnologías de la información y las comunicaciones (TIC) en hogares y personas de 5 y más años de edad departamental 2023. https://www.dane.gov.co/files/operaciones/TICH/bol-TICH-2023.pdf

Fundación Karisma. (2021). Apagones digitales en Colombia: Una mirada desde los derechos humanos.

Fundación Karisma. (2022). Internet y derechos humanos en Colombia. https://karisma.org.co

Impacto TIC. (2023). Quibdó estuvo sin internet por 3 días: causas y responsabilidades. https://impactotic.co/noticias-tic/quidbo-estuvo-sin-internet-por-3-dias-y-mas-noticiasticInforme sobre derechos humanos en Chocó. (2022). Universidad Católica.

Mario en tu radio. (2024). El Chocó lleva cinco días completamente incomunicado debido a problemas con la conexión a internet, los datos y la telefonía. https://marioenturadio.com/el-choco-lleva-cinco-dias-completamente-incomunicado-debido-a-problemas-con-la-conexion-a-internet-los-datos-y-la-telefonia/

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2024). Anuncio de segunda línea de conectividad y nuevas antenas para Chocó. https://www.mintic.gov.co/portal/715/w3-article-338307.html

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2025). Comunicado sobre conectividad en Chocó. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/400410:Comunicado-sobre-conectividad-en-Choco

Observatorio de Internet (OBI). (2024a). [Micro-caída] Reporte: Caída de red - Quibdó, Chocó 1. https://obi.karisma.org.co/2024-10-28-colombia-microcaida-quibdo-choco-agosto-2/

Observatorio de Internet (OBI). (2024b). [Micro-caída] Reporte: Caída de red - Quibdó, Chocó 2. https://obi.karisma.org.co/2024-10-28-colombia-microcaida-quibdo-choco-agosto/

Organización de las Naciones Unidas. (2016). El acceso a internet es un derecho humano (Resolución A/HRC/32/L.20).

Semana. (2020, septiembre). Quibdó incomunicado en medio de protestas sociales. https://semana.com

COLJUEGOS Y SU APUESTA DE BLOQUEAR INTERNET EN COLOMBIA

Catalina Moreno Arocha

Codirectora de Fundación Karisma. Abogada con maestría en Derecho Público. Su trabajo se centra en temas de derechos humanos y justicia social. Durante más de una década trabajó en la Corte Constitucional y se desempeñó como abogada de incidencia política y jurídica en asuntos de género.

En Karisma, impulsa el uso de tecnologías al servicio de la protección de grupos sociales expuestos a violencias y discriminación.

Con contribuciones en la fase preliminar de construcción de María Camila Galvis.

Abogada de la Universidad Externado de Colombia, experta en gestión y regulación en telecomunicaciones, competencia y protección de usuarios. Cuenta con más de diez años de experiencia en la implementación de proyectos con alto componente legal y técnico en el sector TIC.

Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

RESUMEN

Este artículo expone la forma en la que Coljuegos, encargada de autorizar el funcionamiento de juegos de suerte y azar en Colombia, bloquea contenido en Internet que incluye juegos o publicidad de juegos no autorizados. A través de las normas que la habilitan para el bloqueo, las respuestas que obtuvimos ante solicitudes de información y casos que hemos documentado como el bloqueo de Reddit y el periódico The Independent, evidenciamos un mecanismo de control de contenidos que opera sin un marco legal suficientemente claro y preciso. La falta de salvaguardas que rodeen la facultad de Coljuegos amenaza los derechos a la libertad de expresión, al acceso a la información, a la libertad de prensa y al debido proceso.

PALABRAS CLAVE:

Bloqueo estatal de contenidos, libertad de expresión, Coljuegos, gobernanza de Internet.

Este documento fue realizado en el marco del proyecto CADE – Civil Society Alliances for Digital Empowerment. Ver más en https://cadeproject.org/

Esta publicación está cofinanciada por la Unión Europea. Su contenido es responsabilidad exclusiva de Fundación Karisma y no refleja necesariamente las opiniones de la Unión Europea.

INTRODUCCIÓN

En Colombia diversas entidades estatales han utilizado algunas facultades legales para ordenar restricciones sobre contenidos en línea: la Superintendencia de Industria y Comercio (SIC) como autoridad de datos (Ley 1581 de 2012, artículo 21) y como autoridad de protección del consumidor (Ley 1480 de 2011, artículo 59, numeral 9); la Dirección Nacional de Derechos de Autor (DNDA) en ejercicio de la función jurisdiccional en los procesos relacionados con los derechos de autor y conexos (Ley 1564 de 2012, artículo 24, numeral 3b); el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en los procesos administrativos de sanción por material de abuso sexual infantil (Ley 679 de 2001, artículo 10); y Coljuegos como administradora del monopolio rentístico de juegos de suerte y azar (Ley 643 de 2001, artículo 38, parágrafo 3).

Cada una de esas autoridades ha adoptado procedimientos distintos para ordenar los bloqueos de contenidos en Internet. En Fundación Karisma hemos evidenciado que Coljuegos es una de las autoridades que ordena bloqueos problemáticos de forma más frecuente. Por ejemplo, en los últimos tres años, mediante esa facultad Coljuegos ha bloqueado a plataformas y sitios como Tumblr, Reddit (Enter.co, 2024; Karisma, 2024a y 2024b), Bitcoin y el periódico The Independent (Karisma, 2024c). También ha pedido a Meta bloquear 289 perfiles de Facebook e Instagram (Coljuegos, 2024f). El presidente de Coljuegos mencionó que “a la fecha, se han emitido cerca de 26.600 órdenes de bloqueo a sitios de apuestas no autorizadas” (2025) y se ha solicitado el bloqueo “de al menos 120 perfiles de redes sociales” (2024a). Además, existe un centro de inteligencia artificial para el monitoreo y detección de operaciones no autorizadas de juegos de azar (Coljuegos, 2024e).

Pese al uso extensivo de la facultad, hasta el momento no es posible que las personas identifiquen que la orden provino de esa entidad cuando no pueden acceder a un sitio. Tampoco se publican los análisis realizados para determinar que la medida de bloqueo resultaba admisible bajo los estándares para la restricción de la libertad de expresión en el sistema interamericano (Comisión Interamericana de Derechos Humanos, 2009) y en la jurisprudencia constitucional (Corte Constitucional, 2018).

Cada vez con más frecuencia, entidades tratan de incluir facultades de control de contenidos en internet en procesos de política pública para, por ejemplo, eliminar contenidos “dañinos” para niños y niñas (Karisma, 2021), desinformación, violencia política (Karisma, 2023) y para proteger el honor y la honra (Karisma, 2024d), entre otros. Usualmente, estas facultades son amplias en su objeto, dejan los detalles del funcionamiento a la reglamentación y no contienen mecanismos de salvaguarda de derechos fundamentales como la libertad de expresión y de información, la intimidad y el debido proceso. Caracterizar la forma en que Coljuegos realiza los bloqueos puede ser útil para proponer mejoras al ejercicio, así como para tener elementos para incidir en la forma como se usa la facultad y en futuras propuestas de intervención estatal en contenidos en línea.

ANTECEDENTES Y DESARROLLO

Marco jurídico de la facultad de bloqueo de Coljuegos

Coljuegos es una Empresa Industrial y Comercial del Estado (EICE) encargada de la administración permanente del monopolio rentístico de los juegos de suerte y azar (Decreto 4142 de 2011, artículo 2). Tener el monopolio rentístico significa tener la facultad exclusiva de explotar, administrar y controlar todas las modalidades de juegos de suerte y azar, también de establecer las condiciones en las cuales los particulares pueden operarlos (Corte Constitucional, 2003). Los recursos que se cobran a cada uno de los juegos se destinan únicamente a financiar el sistema de salud (Ley 643 de 2001, artículos 1 y 2).

Dentro de las funciones específicas de Coljuegos se encuentra la de "adelantar las acciones para controlar y combatir la operación ilegal de los juegos de suerte y azar" (Decreto 1451 de 2015, artículo 2, numeral 8). Para su ejercicio, Coljuegos, junto a las autoridades de inspección, vigilancia y control, y la Policía Nacional, puede:

> hacer monitoreo a los canales, entidades financieras, páginas de Internet y medios que de cualquier forma sirvan a la explotación, operación, venta, pago, publicidad o comercialización de juegos de suerte y azar no autorizados, y ordenar las alertas y bloqueos correspondientes (Ley 643 de 2001, artículo 38).

En 2020, el MinTIC, Coljuegos, la Dirección de Investigación Criminal e Interpol de la Policía Nacional de Colombia y la Federación Colombiana de Empresarios de Juegos de Suerte y Azar (Fecoljuegos) emitieron un segundo protocolo para "determinar los lineamientos a seguir frente a las órdenes de bloqueo impartidas por Coljuegos" (MinTIC et al., 2020). Aclaramos que Coljuegos (2022) informó que en abril de 2017 fue suscrita una primera versión del protocolo, pero esa versión no fue encontrada en la página web ni fue anexada a ninguna de las respuestas de la entidad a las peticiones enviadas por Karisma.

En resumen, según el protocolo, el proceso inicia cuando la entidad identifica, de oficio o por denuncia, un sitio web que presuntamente opera o promueve juegos de azar no autorizados. Tras una verificación interna para confirmar la actividad ilegal y, si es del caso, delimitar el subdominio específico involucrado; Coljuegos preserva la evidencia técnica del sitio (incluido código fuente y soportes de integridad) y la remite al Centro Cibernético de la Policía Nacional (CECIP), que dispone de 48 horas para validar la información. Posteriormente, la URL es publicada en la plataforma administrada por el MinTIC para que los proveedores de servicios de internet ejecuten el bloqueo en un plazo de 72[5] horas, mientras que, paralelamente, Coljuegos publica el listado durante cinco días hábiles y otorga hasta 15 días hábiles a los titulares para acreditar autorización, tras lo cual, de no hacerlo, el bloqueo se mantiene de manera definitiva.

5. El protocolo menciona que en cualquier momento los interesados pueden solicitar el desbloqueo de un sitio web. Una vez solicitado, Coljuegos verifica la remoción de la operación ilegal, le informa al peticionario y al CECIP (MinTIC et al., 2020).

En un boletín de prensa, Coljuegos (2024e) informó que cuenta con un Centro de Inteligencia Artificial de Coljuegos (CIAC) que permite monitorear la actividad de apuestas en línea ilegales y vigilar en tiempo real las transferencias que realizan los establecimientos autorizados. Para el control de ilegalidad existe un tablero de control desarrollado con el apoyo de Kiggu, empresa especializada en ciberseguridad que permite "identificar páginas ilícitas en la web, deepweb y darknet, así como proteger la marca de los 16 operadores autorizados de apuestas en línea frente a posibles casos de duplicidad de sus portales" (2024e).

En el contrato suscrito entre Coljuegos y Kiggu SAS (2025d) se establece que el contratista es responsable de buscar, monitorear, identificar y gestionar el control de sitios de apuestas no autorizados en diferentes espacios digitales, registrarlos en el aplicativo institucional y aportar la evidencia necesaria para solicitar su bloqueo a proveedores de servicios de internet. El proveedor también debe administrar y mantener actualizada una base de datos de estos sitios, verificar que se ejecute efectivamente el bloqueo y dar soporte técnico a Coljuegos en ese proceso. Además, debe realizar un análisis y gestión mensual de al menos 2300 sitios ilegales y atender bloqueos adicionales de portales o contenidos que sean reportados directamente por el supervisor del contrato. El contrato señala que el contratista debe adaptarse a las dinámicas de los juegos en línea. Para ello contiene la obligación de identificar contenidos en apps, sitios web, perfiles en redes sociales y entornos como la deepweb o la darkweb. Finalmente, incluye una obligación de confidencialidad sobre la información, datos e informes generados en el marco de la ejecución contractual.

En la Circular 0017 de 23 de abril de 2025, MinTIC (2025) expidió unos lineamientos para el proceso de funcionamiento de una plataforma[6] en la que se cargarían las órdenes de bloqueo. En ella se explicó que los servidores públicos autorizados de Coljuegos cargarán semanalmente la lista de URL a bloquear y que cada ISP tendría una credencial para descargar diariamente esa lista. Los ISP contarán con 72 horas para pedir la revisión del bloqueo que no sea posible.

La circular advierte que el bloqueo de "canales, páginas de Internet y medios" debe obedecer al ejercicio de operaciones ilegales y que se debe evitar bloquear "plataformas legítimas, servicios legales o contenidos no relacionados con la actividad prohibida", siendo siempre responsabilidad de Coljuegos la orden de bloqueo (MinTIC, 2025). La circular también sostuvo que Coljuegos podrá hacer seguimiento a los bloqueos, pudiendo requerir que se implementen. Esto, sin descontar que puede ejercer las acciones de vigilancia, inspección y control contra los ISP que no los lleven a cabo.

6. A la plataforma se accede mediante el siguiente enlace, pero solo está habilitada a personas con credenciales: https://cms.mintic.gov.co/

CASOS DE BLOQUEO DOCUMENTADOS

En el marco de esa competencia, Karisma ha identificado los siguientes casos de bloqueo:

2018

- ***Bloqueo de Skrill:*** en julio de 2018 varias páginas web alertaron sobre el bloqueo de Skrill, una billetera electrónica. El portal Mundovideo informó que personas usuarias en foros de juego en línea reportaron la imposibilidad de acceder al portal (Mundovideo, 2018). Al momento de entrar, aparecía que la página había sido bloqueada por disposición del MinTIC, de conformidad con las facultades de monitoreo de canales, páginas web y medios que "sirvan a la explotación, operación, venta, pago, publicidad o comercialización de juegos de suerte y azar no autorizados, y ordenar las alertas y bloqueos correspondientes".

- Bloqueo de Sportwetten y de Oddschecker: en diciembre de 2018, Carolina Botero (2018) también denunció que ambos sitios fueron bloqueados por contener publicidad de apuestas no registradas. Al tratar de ingresar aparecía la leyenda "ERR_CONNECTION_REFUSED", pero entrando a la página web usando un VPN era posible comprobar que el sitio estaba activo. Ninguna autoridad ni los operadores de telecomunicaciones dieron información sobre la razón del bloqueo.

2022

- ***Bloqueo de Tumblr:*** en enero de 2022, un medio de comunicación (Machado, 2022) dio a conocer que la plataforma Tumblr había sido bloqueada en el país. Movistar respondió, en el entonces Twitter, informando que ello obedecía a una orden de autoridad competente. Para entender cómo había ocurrido el bloqueo, Karisma realizó el reporte ante OONI (OONI Explorer, 2022) y presentó petición al MinTIC[7] para identificar la autoridad que había dado la orden, la URL bloqueada, el procedimiento seguido, las oportunidades de defensa de la plataforma y del titular de la página bloqueada, el acto administrativo en el que se consignó la decisión, el análisis de proporcionalidad y necesidad realizado y las medidas de publicidad adoptadas.

  El Ministerio (2022) sostuvo que, al momento de responder la petición, casi dos meses después del bloqueo, la página estaba activa y que no se encontró ninguna instrucción o comunicación sobre esa URL. El Ministerio dio traslado de la petición al Grupo Investigativo contra la Pornografía Infantil y otros Abusos en Internet del Centro Cibernético Policial, que a su vez la remitió por competencia a Coljuegos, sin informar las razones de esa decisión (Policía Nacional, 2022). A pesar de que desde marzo Coljuegos recibió la petición, tan solo después de insistir[8] en su respuesta, contestó indicando nuevamente que la página estaba activa y que no había orden de bloqueo.

7. La petición fue presentada el 20 de enero de 2022 y le fue asignado el radicado 22100406.
8. Karisma insistió en las peticiones ante el Ministerio y Coljuegos porque sus respuestas han sido evasivas.

Por otro lado, MinTIC (2022b) sostuvo que la URL www.tumblr.com no presentó ninguna instrucción o comunicación para reportarse en el repositorio administrado por el Ministerio. Explicó que como no existió bloqueo alguno, no debía dar otras respuestas. Después de casi seis meses, Coljuegos (2022) contestó que, al momento de responder, el sitio no estaba bloqueado. Se había ordenado el bloqueo de tumblr.com por "la publicidad de casas de apuestas de juegos de suerte y azar no autorizadas por Coljuegos para operar en el territorio nacional".

2024

- ***Bloqueo de Reddit:*** la plataforma Reddit fue bloqueada en Colombia por orden de Coljuegos a finales de mayo de 2024. Un medio de comunicación (Enter.co, 2024), y usuarios en X, reportaron la imposibilidad de acceder al sitio y a su aplicación. Verificaciones técnicas realizadas por Karisma mediante la herramienta OONI (Open Observatory of Network Interference) confirmaron que varios ISP habían implementado un bloqueo por DNS o redirección a través de un proxy, que conducía a la página de advertencia de Coljuegos (Karisma, 2024a). En ese análisis se comprobó que, al tratar de ingresar a la plataforma, existía una redirección a la página web de Coljuegos, de ahí que se desprendiera que el bloqueo ocurrió por la inclusión del dominio reddit.com en la lista que Coljuegos remite a los ISP (Karisma, 2024a). Pese a tratarse de una plataforma de gran tráfico interno, Karisma no encontró acto administrativo público que realizara un análisis del impacto del bloqueo en el ejercicio de derechos fundamentales de quienes usan la página (Karisma, 2024b).

  Para entender cómo había ocurrido, Karisma pidió información sobre la forma en la que se hacían los bloqueos, el agotamiento de medidas previas al bloqueo, y los mecanismos de contradicción de estas decisiones por parte de los ISP y de personas usuarias. Coljuegos (2024c), además de repetir lo establecido en el protocolo, explicó que cualquier apuesta por fuera de los 15 sitios autorizados se califica como ilegal y es objeto de bloqueo. También que el principio de publicidad se cumplía con la advertencia que aparece una vez un usuario trata de acceder a un sitio no autorizado (Coljuegos, 2018b). Finalmente, explicó que el bloqueo no era una sanción, sino el uso de una facultad legítima.

- ***Bloqueo a Bitcoin y The Independent:*** Karisma encontró que en octubre de 2024 Coljuegos ordenó el bloqueo del dominio de The Independent (2024c y 2024e), un reconocido periódico británico, y del portal de información sobre criptomonedas Bitcoin.com. De ninguno de los dos casos se encontró documentación en la página web de la entidad pública, a pesar de que el bloqueo a The Independent debió ser objeto de un análisis aún más riguroso por tratarse de un medio de comunicación. Al momento de cierre de este artículo, el bloqueo sobre el periódico sigue vigente.

- ***Solicitud de bloqueo de perfiles de redes sociales y de cuentas de WhatsApp a Meta:*** Coljuegos pidió a Meta el bloqueo de ocho perfiles de redes sociales (2024d), algunos de ellos de influencers como @la_liendraa (6,6 millones de seguidores), @karinagarciaoficiall (5 millones de seguidores), y @saravalentinasv (600.000 seguidores). La entidad explicó que la solicitud de bloqueo fue el resultado del "perfilamiento por la empresa Kiggu (Ciberseguridad para todos)", en el que se evidenció publicidad de casas de apuestas no autorizadas.

  Luego, en diciembre del mismo año, Coljuegos (2024f) dio a conocer que había enviado a Meta una solicitud para el bloqueo de 289 cuentas de redes sociales de Facebook e Instagram, por incumplir las reglas sobre registro de apuestas en el país. Revisado el listado de URL publicados, se tiene que fueron remitidos URL de contenido en YouTube, TikTok y Vimeo, así como a una aplicación de la tienda de Apple, que no corresponden a actividades de Meta. También se incluyeron perfiles de WhatsApp y Telegram. Se aclara que no fue posible saber si los bloqueos pedidos fueron acatados por la empresa.

2025

- ***Bloqueo a Expressen:*** en noviembre de 2025, un periodista reseñó el caso del bloqueo del diario Expressen, ante las denuncias por censura realizadas por periodistas y personas usuarias en redes sociales, después de que trataran de entrar a revisar una noticia (Hyperconectado, 2025). En su nota señaló que el bloqueo habría sido ordenado desde 2021 por Coljuegos, quién lo confirmó después en un comunicado de prensa (Coljuegos, 2025c). Karisma documentó los bloqueos en su Observatorio de Bloqueos de Internet (2025).

DISCUSIÓN DE LOS PROBLEMAS DESDE LOS RETOS PARA LA INCIDENCIA EN ESPECIAL EN ESPACIOS DE GOBERNANZA

Desde 2018 Karisma ha documentado los bloqueos realizados por Coljuegos, así como ha alertado sobre la afectación de los derechos fundamentales a la libertad de expresión, información y debido proceso que ellos suponen. De forma más reciente, en 2024, tuvo la oportunidad de reunirse con personas encargadas de la ejecución de los bloqueos dentro de la entidad. Se trató de una reunión informal en la que se buscaba entender la forma en que se realizaban los bloqueos y si existía algún análisis de impacto en otros derechos. En esa ocasión fue explicado que la ponderación con otros derechos no debía hacerse, pues los bloqueos aseguraban los derechos a la vida y a la salud. Esto, porque el dinero dejado de recaudar tiene un impacto directo en el sistema de salud.

Así, se pueden identificar dos desafíos para la incidencia directa con la entidad. El primero relacionado con la convicción de la entidad de que es posible tomar cualquier medida para controlar los juegos no autorizados, por su relación con el sistema de salud. El segundo tiene que ver con el hecho de que la facultad ha sido otorgada a una autoridad que no hace parte de las distintas instancias de gobernanza de Internet. Es cierto que MinTIC es quien remite la lista de sitios bloqueados a los ISP, pero su labor es de intermediación y parece no contar con ninguna función de revisión de fondo de las decisiones de bloqueo. Por esa misma razón, escenarios como los foros de Gobernanza de Internet de Colombia y de América Latina y el Caribe, aunque podrían ser espacios de discusión técnica, probablemente no sean útiles para generar cambios, debido a que Coljuegos no hace parte de ellos. Por eso, la incidencia más efectiva podría darse en espacios locales de toma de decisiones, como el Congreso de la República o distintas instancias judiciales.

La incidencia para incluir estándares legales para el ejercicio de la función podría ser difícil, debido a la finalidad de recaudo destinado al sector salud que podría desincentivar el interés de congresistas. De ahí que, por el momento, se propone un litigio estratégico como escenario para asegurar la materialización de los derechos fundamentales en el ejercicio del control estatal de las apuestas en línea. Las rutas serían dos, la primera, una demanda en contra de la facultad otorgada a Coljuegos, ya que que no contempla los requisitos y controles necesarios para asegurar que la restricción no afecte derechos fundamentales. La segunda, que parece tener una mayor posibilidad de éxito, sería una acción de tutela por la vulneración del derecho a la libertad de expresión por el bloqueo de páginas particulares, especialmente alguna de interés público como el periódico The Independent.

CONCLUSIONES Y RECOMENDACIONES

En principio, la función de Coljuegos responde a una finalidad legítima por controlar los juegos que no han sido autorizados, de forma que se respete el monopolio estatal de las apuestas y que, de paso, no se evadan recursos destinados al sistema de salud. También busca “proteger la marca” de los operadores autorizados (Coljuegos, 2024e). En ese marco, el bloqueo de contenido puntual en Internet puede parecer proporcionado: no se trata de una medida como la interrupción total del servicio o de ciertos canales de comunicación específicos, sino en sitios puntuales. Sin embargo, la restricción de derechos, sin importar la finalidad que busca, requiere de una actuación cuidadosa de parte de las autoridades que la realizan. El bloqueo de sitios web y de cuentas de redes sociales y de mensajería afecta distintos derechos:

- El derecho a la libertad de expresión (Constitución Política, artículo 20) que busca “la libre manifestación y comunicación del pensamiento, así como el libre flujo social de información, ideas y opiniones” para evitar el control del pensamiento (Corte Constitucional, 2007). Es un derecho con un estatus especial de protección, ya que es base fundamental de las sociedades políticas abiertas, pluralistas y democráticas.

Este derecho tiene dos dimensiones: la individual, que comprende el derecho a hablar o escribir, y el "derecho a utilizar cualquier medio apropiado para difundir el pensamiento y hacerlo llegar al mayor número de destinatarios" (Corte Interamericana de Derechos Humanos, 2001). Y la colectiva, que consiste en "el derecho de todas las personas a recibir tales pensamientos, ideas, opiniones e informaciones de parte de quien las expresa" (Corte Constitucional, 2007). Las órdenes de bloqueo limitan indudablemente la expresión de las personas usuarias que las usan, así como de quienes serían sus destinatarias.

- El derecho a la libertad de información (Constitución Política, artículo 20) que protege "la comunicación de versiones sobre hechos, eventos, acontecimientos, gobiernos, funcionarios, personas, grupos y en general situaciones, en aras de que el receptor se entere de lo que está ocurriendo" (Corte Constitucional, 2007). Este derecho se afecta con el bloqueo de espacios digitales en los que las personas reciben información de su interés. El derecho fundamental a la libertad de prensa (Constitución Política, artículo 20), que incluye "la libertad de fundar medios masivos de comunicación como la libertad de estos medios de funcionar sin interferencias indebidas, de forma tal que puedan cumplir sus cruciales funciones dentro de la sociedad democrática" (Corte Constitucional, 2007). Este derecho se afecta cuando los sitios web o las cuentas de redes sociales o de mensajería bloqueadas se refieren a medios de comunicación.

- El derecho al debido proceso (Constitución Política, artículo 29) que "busca la protección del individuo incurso en una actuación judicial o administrativa, para que durante su trámite se respeten sus derechos y se logre la aplicación correcta de la justicia" (Corte Constitucional, 2014). Este derecho se vulnera cuando el bloqueo ocurre sin notificar al propietario del sitio web, del contenido, de la aplicación o de la cuenta de red social o de mensajería bloqueada. También cuando las personas no entienden la razón del bloqueo cuando tratan de acceder al contenido bloqueado.

- El derecho a la intimidad (Constitución Política, artículo 15) que protege de "todas aquellas divulgaciones ilegítimas de hechos propios de la vida privada o familiar o las investigaciones también ilegítimas de acontecimientos propios de dicha vida" y "el derecho de toda persona de tomar por sí sola decisiones que concierne a la esfera de su vida privada" (Corte Constitucional, 1992). Este derecho se afecta cuando se pide el bloqueo de sitios web o de cuentas personales, porque es posible afectar la reputación de sus dueños. También cuando se bloquean servicios de mensajería privada, ya que puede suponer el control sobre canales de comunicación personal.

Como la afectación más directa de las interrupciones de internet es la libertad de expresión, proponemos su análisis bajo los estándares de ese derecho, así como el test de legalidad, necesidad y proporcionalidad. Para hacer ese examen, la Corte Constitucional ha señalado que, cada vez que se pretenda restringir la libertad de expresión, la autoridad debe demostrar que la restricción:

1. está prevista de manera precisa y taxativa por la ley,
2. persigue el logro de ciertas finalidades imperativas definidas de manera concreta y específica,
3. es necesaria para el logro de dichas finalidades,
4. es posterior y no previa a la expresión,
5. no constituye censura en ninguna de sus formas, lo cual incluye el requisito de guardar neutralidad frente al contenido de la expresión que se limita, y
6. no incide de manera excesiva en el ejercicio de este derecho fundamental, es decir, ser proporcionada (Corte Constitucional, 2007).

La facultad de bloqueo está contenida en la Ley 643 de 2001 (artículo 38, parágrafo 3) cumpliendo, de entrada, el principio de legalidad. Pese a ello, la medida no persigue de forma directa la protección de una finalidad imperativa, puesto que su objetivo directo es la protección del monopolio rentístico estatal y de las marcas de los juegos en línea que han sido autorizados para operar en el país. La Convención Americana de Derechos Humanos ha mencionado como fines, que podrían dar lugar a la restricción, los necesarios para asegurar: a) el respeto a los derechos o a la reputación de los demás, o b) la protección de la seguridad nacional, el orden público, la salud o la moral pública (artículo 13). Así, aunque la restricción resulte útil, razonable u oportuna para un fin estatal, eso no la hace aceptable de cara a la protección de la libertad estatal (Corte Interamericana de Derechos Humanos, 2004). En ese mismo sentido, la medida de bloqueo no es proporcional al interés que la justifica, ni interfiere en la menor medida posible en el goce efectivo del derecho a la libertad de expresión.

A ello se suma que el bloqueo no cumple con los estándares que la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos estableció para que las interrupciones de internet sean compatibles con los derechos humanos:

> que las interrupciones deberían ser lo más limitadas posible en cuanto a duración, alcance geográfico y redes y servicios afectados; que cuenten con la autorización previa de un tribunal u otro órgano judicial independiente, para evitar cualquier influencia política, comercial o de otra índole injustificada; que se comuniquen con antelación a la población y a los proveedores de servicios de telecomunicaciones o de internet, indicando claramente la base jurídica de

> la interrupción y su alcance y duración; y que estén sujetas a mecanismos de reparación efectivos y accesibles para aquellos cuyos derechos se hayan visto afectados por las interrupciones, como procedimientos judiciales en tribunales independientes e imparciales; los procedimientos judiciales deberían llevarse a cabo en el momento oportuno y ofrecer la posibilidad de que una interrupción del acceso a internet producida en contravención de la legislación aplicable se declare ilegal, incluso después de finalizada (2022).

Si bien, desde 2024, se pueden encontrar algunos listados de sitios bloqueados mensualmente, lo cierto es que es difícil hacer seguimiento y control ciudadano de la facultad; debido al formato en PDF, la reducida frecuencia de publicación y a que el archivo no está en un lugar visible y claro en la página web de Coljuegos. De modo que, en el caso de redes sociales y por el impacto que tendría su bloqueo completo en el país, parece que Coljuegos optó por pedir un bloqueo de cuentas por canales distintos a Meta. Sin embargo, ese análisis que podríamos llamar de proporcionalidad solo ocurrió en esa ocasión. No existen pruebas de los análisis que Coljuegos ni su contratista efectúan antes de ordenar el bloqueo. En esa línea, resulta preocupante que sea un contratista privado el que realiza el monitoreo y ordene los bloqueos, así mismo, que tenga una obligación de confidencialidad que va en contra de la protección de la ley de acceso a la información pública. Finalmente, no es claro si Coljuegos o MinTIC realizan alguna verificación sobre el procedimiento mediante el cual los proveedores de servicios materializan el bloqueo.

Para cerrar, destacamos que la misma entidad ha reconocido que “a la fecha, se han emitido cerca de 26.600 órdenes de bloqueo a sitios de apuestas no autorizadas” (2025) y se ha solicitado el bloqueo “de al menos 120 perfiles de redes sociales” (2024a). Además, desde hace un par de años ha contratado mecanismos de monitoreo activo (Coljuegos, 2024d). Ambas situaciones dan cuenta de una función de bloqueo cada vez más robusta, que requiere de atención social urgente que asegure los derechos a la libertad de expresión y de información, la intimidad y el debido proceso.

REFERENCIAS

Asamblea Nacional Constituyente. (1991). Constitución Política de Colombia. Gaceta Constitucional No. 116 de 20 de julio de 1991. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Botero, C. (2018, diciembre 15). Bloqueos de internet por apuestas ilegales. El Espectador. http://www.staging.elespectador.com/opinion/columnistas/carolina-botero-cabrera-sand/bloqueos-de-internet-por-apuestas-ilegales-column-829386/

Comisión Interamericana de Derechos humanos, Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. (2010). Marco jurídico interamericano sobre la libertad de expresión. https://www.oas.org/es/cidh/expresion/docs/publicaciones/MARCO%20JURIDICO%20INTERAMERICANO%20DEL%20DERECHO%20A%20LA%20LIBERTAD%20DE%20EXPRESION%20ESP%20FINAL%20portada.doc.pdf

Coljuegos. (2018a). Contrato 105 de 2018 suscrito entre Coljuegos y MNEMO Colombia SAS. https://www.coljuegos.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=234621

Coljuegos. (2018b). Advertencia Páginas Online Ilegales. https://www.coljuegos.gov.co/publicaciones/301824/advertencia_pampatildeampiexclginas_online_ilegales/

Coljuegos. (2020). Informe de ejecución del Contrato 166 de 2020 suscrito entre Coljuegos e Identian SAS. https://www.coljuegos.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=245804

Coljuegos. (2021). Contrato 092 de 2021 suscrito entre Coljuegos e Identian SAS. https://www.coljuegos.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=251494

Coljuegos. (2022). Respuesta radicado 20221030246312 y 20221030247122 de 2022. Radicado 20225200218161.

Coljuegos. (2024a). Boletín no. 13. Más de 14.000 portales de apuestas ilegales en línea han sido bloqueados en Colombia. https://www.coljuegos.gov.co/publicaciones/306840/mas-de-14000-portales-de-apuestas-ilegales-en-linea-han-sido-bloqueados-en-colombia/

Coljuegos. (2024b). Contrato 169 de 2024 suscrito entre Coljuegos y Kiggu SAS. https://www.coljuegos.gov.co/documentos/213421/169-2024-kiggu-sas/

Coljuegos. (2024c). Respuesta radicado 20241030192662. Radicado 20245200227641. 10 de julio de 2024.

Coljuegos. (2024d). Orden de bloqueo de perfiles (con contenido de publicidad de juegos de suerte y azar de plataformas ilegales, no autorizadas en Colombia). Radicado 20245200361711. https://es.scribd.com/document/802824612/20245200361711-META-PLATFORMS-1733787504976

Coljuegos. (2024e). Boletín No. 090: Así funciona el Centro de Inteligencia Artificial de Coljuegos, la nueva herramienta para vigilar el recaudo y combatir la ilegalidad. https://www.coljuegos.gov.co/publicaciones/307017/asi-funciona-el-centro-de-inteligencia-artificial-de-coljuegos-la-nueva-herramienta-para-vigilar-el-recaudo-y-combatir-la-ilegalidad/index.php

Coljuegos. (2024f). Coljuegos solicitó bloquear 289 perfiles de Facebook e Instagram por operar rifas y promocionar apuestas ilegales. Recuperado el 13 de agosto de 2025, de https://www.coljuegos.gov.co/publicaciones/307065/coljuegos-solicito-bloquear-289-perfiles-de-facebook-e-instagram-por-operar-rifas-y-promocionar-apuestas-ilegales/

Coljuegos. (2024f). Sitios bloqueados en febrero de 2024. https://www.coljuegos.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=287911

Coljuegos. (2024g). Sitios bloqueados en marzo de 2024. https://www.coljuegos.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=288449

Coljuegos. (2024h). Sitios bloqueados en mayo de 2024. https://www.coljuegos.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=289731

Coljuegos. (2025a). Boletín No. 020: Coljuegos intensifica acciones de bloqueo de sitios web de apuestas ilegales. https://www.coljuegos.gov.co/publicaciones/307143/coljuegos-intensifica-acciones-de-bloqueo-de-sitios-web-de-apuestas-ilegales/index.php

Coljuegos. (2025b). Informe Estadístico Diciembre de 2024. https://www.coljuegos.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=295366

Coljuegos. (2025c). Bloqueo del portal Expressen se realizó hace cuatro años por promoción de apuestas ilegales. https://www.coljuegos.gov.co/publicaciones/307237/bloqueo-del-portal-expressen-se-realizo-hace-cuatro-anos-por-promocion-de-apuestas-ilegales/

Coljuegos. (2025d). Contrato 347 de 2025 suscrito entre Coljuegos y Kiggu SAS. https://www.coljuegos.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=300780

Coljuegos. (2025e). Sitios bloqueados en febrero de 2025. https://www.coljuegos.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=295250

Coljuegos. (2025f). Sitios bloqueados en marzo de 2025. https://www.coljuegos.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=295663

Coljuegos. (2025g). Sitios bloqueados en abril de 2025. https://www.coljuegos.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=296863

Coljuegos. (2025h). Sitios bloqueados en mayo de 2025. https://www.coljuegos.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=297097

Convención Americana sobre Derechos Humanos. (2025). Artículo 13. https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=25&lID=2

Corte Constitucional. (1992, junio 16). Sentencia T-534 de 1992. Magistrado Ciro Angarita Barón. https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm

Corte Constitucional. (1994, enero 27). Sentencia C-024 de 1994. Magistrado ponente: Alejandro Martínez Caballero. https://www.corteconstitucional.gov.co/relatoria/1994/c-024-94.htm

Corte Constitucional. (2003, julio 15). Sentencia C-571 de 2003. Magistrado ponente: Jaime Araújo Rentería. https://www.corteconstitucional.gov.co/relatoria/2003/c-571-03.htm

Corte Constitucional. (2007, mayo 22). Sentencia T-391 de 2007. Magistrado ponente: Manuel José Cepeda Espinosa. https://www.corteconstitucional.gov.co/relatoria/2007/t-391-07.htm

Corte Constitucional. (2014, junio 4). Sentencia C-341 de 2014. Magistrado Ponente: Mauricio González Cuervo. https://www.corteconstitucional.gov.co/relatoria/2014/c-341-14.htm

Corte Constitucional. (2018, junio 26). Sentencia T-243 de 2018. Magistrada ponente: Diana Fajardo Rivera. https://www.corteconstitucional.gov.co/relatoria/2018/t-243-18.htm

Corte Constitucional. (2019, abril 2). Sentencia T-145 de 2019. Magistrada ponente: Cristina Pardo Schlesinger. https://www.corteconstitucional.gov.co/relatoria/2019/t-145-19.htm

Corte Interamericana de Derechos Humanos. (2001, febrero 5). Caso Olmedo Bustos y otros Vs. Chile. Fondo, Reparaciones y Costas. Serie C No. 73. https://www.corteidh.or.cr/docs/casos/articulos/seriec_73_esp.pdf

Corte Interamericana de Derechos Humanos. (2004, julio 2). Caso Herrera Ulloa Vs. Costa Rica. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 2 de julio de 2004. Serie C No. 107. https://www.corteidh.or.cr/docs/casos/articulos/seriec_107_esp.pdf.

Decreto 4142 de 2011. Por el cual se crea la Empresa Industrial y Comercial del Estado Administradora del Monopolio Rentístico de los Juegos de Suerte y Azar, COLJUEGOS. Diario Oficial No. 48.242 de 3 de noviembre de 2011. http://www.secretariasenado.gov.co/senado/basedoc/decreto_4142_2011.html

Decreto 1451 de 2015. Por el cual se modifica la estructura de la Empresa Industrial y Comercial del Estado Administradora del Monopolio Rentístico de los Juegos de Suerte y Azar (Coljuegos). http://www.secretariasenado.gov.co/senado/basedoc/decreto_1451_2015.html#2

Enter.co. (2024). Movistar y Claro restablecen el acceso a Reddit tras bloqueo ¿Por qué se restringió la página? https://www.enter.co/colombia/por-que-razon-la-app-y-la-pagina-de-reddit-estuvieron-bloqueadas-por-mas-de-48-horas-en-colombia

Fundación Karisma. (2021). El proyecto de Ley 600 sigue su curso en el Congreso a pesar de las críticas. https://web.karisma.org.co/el-proyecto-de-ley-600-sigue-su-curso-en-el-congreso-a-pesar-de-las-criticas/

Fundación Karisma. (2023). Comentarios PL (Medidas para prevenir, atender, rechazar y sancionar la violencia contra las mujeres). https://web.karisma.org.co/comentarios-sobre-el-proyecto-por-medio-de-la-cual-se-establecen-medidas-para-prevenir-atender-rechazar-y-sancionar-la-violencia-contra-las-mujeres-en-la-vida-politica-y-hacer-efectivo-su-d/

Fundación Karisma. (2024a). Bloqueo de reddit.com por Coljuegos en Colombia. https://obi.karisma.org.co/2024-06-03-colombia-bloqueo-de-reddit-por-coljuegos/

Fundación Karisma. (2024b). Las dudas que quedan tras el bloqueo de Reddit en Colombia. https://web.karisma.org.co/las-dudas-que-quedan-tras-el-bloqueo-de-reddit-en-colombia/

Fundación Karisma. (2024c). Coljuegos en racha: bloqueos a Bitcoin y The Independent. https://web.karisma.org.co/coljuegos-en-racha-bloqueos-a-bitcoin-y-the-independent/

Fundación Karisma. (2024d). Proyecto de ley ofrece nuevas formas de censura impuestas por funcionarios públicos mientras desprotege a víctimas de violencia de género. https://web.karisma.org.co/proyecto-de-ley-ofrece-nuevas-formas-de-censura-impuestas-por-funcionarios-publicos-mientras-desprotege-a-victimas-de-violencia-de-genero/

Fundación Karisma. (2024e). Bloqueo de bitcoin.com e independent.co.uk por Coljuegos en Colombia. https://obi.karisma.org.co/2024-10-28-colombia-bloqueo-bitcoin-e-independent-coljuegos/

Fundación Karisma. (2025). Reporte del bloqueo del sitio web expressen.se. https://obi.karisma.org.co/2025-11-04-reporte-del-bloqueo-del-sitio-web-expressen.se/

Hyperconectado. (2025, noviembre 26). El caso Expressen: improvisación estatal y bloqueos que comprometen la libertad de expresión en Colombia. https://blog.hyperconectado.co/index.php/2025/11/26/el-caso-expressen-improvisacion-estatal-y-bloqueos-que-comprometen-la-libertad-de-expresion-en-colombia/

Ley 65 de 1993. Por la cual se expide el Código Penitenciario y Carcelario. Diario Oficial No. 40.999 de 20 de Agosto de 1993. http://www.secretariasenado.gov.co/senado/basedoc/ley_0065_1993.html

Ley 643 de 2001. Por la cual se fija el régimen propio del monopolio rentístico de juegos de suerte y azar. Diario Oficial No. 44.294, de 17 de enero de 2001. http://www.secretariasenado.gov.co/senado/basedoc/ley_0643_2001.html

Ley 679 de 2001. Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. Diario Oficial No. 44.509 de 4 de agosto de 2001. http://www.secretariasenado.gov.co/senado/basedoc/ley_0679_2001.html

Ley 906 de 2004. Por la cual se expide el Código de Procedimiento Penal. Diario Oficial No. 45.658 de 1 de septiembre de 2004. http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html

Ley 1480 de 2011. Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones. Diario Oficial No. 48.220 de 12 de octubre de 2011. http://www.secretariasenado.gov.co/senado/basedoc/ley_1480_2011.html

Ley 1564 de 2012. Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones. Diario Oficial No. 48.489 de 12 de julio de 2012. http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587 de 18 de octubre de 2012. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Ley 1753 de 2015. Por la cual se expide el Plan Nacional de Desarrollo 2014-2018. Diario Oficial 49.538 de 9 de junio de 2015. http://www.secretariasenado.gov.co/senado/basedoc/ley_1753_2015.html

Machado, M. (10 de enero de 2021). Bloquean página de Tumblr en Colombia por orden de autoridades. https://caracol.com.co/radio/2022/01/10/tecnologia/1641822860_874201.html#:~:text=Hola%2C%20te%20informo%20que%20por,Saludos%20%E2%88%97JP

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2015, julio 18). Ministerio TIC no bloquea aplicaciones sin orden legal, judicial o administrativa. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/11221:Ministerio-TIC-no-bloquea-aplicaciones-sin-orden-legal-judicial-o-administrativa

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2022a). Respuesta a la petición con Radicado MINTIC 221004067 – Solicitud de información bloqueo URL. Radicado: 222018858.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2022b). Respuesta a la petición con Radicado MINTIC 221031423 – Recurso de insistencia. Radicado: 222054211.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2025a). Circular 0017 de 2025. Lineamientos y procedimiento para la solicitud, asignación, seguimiento de credenciales, cargue y bloqueo de los canales, páginas de internet y medios identificados por COLJUEGOS EICE que sirvan a la explotación, operación, venta, pago, publicidad o comercialización de Juegos de Suerte y Azar no autorizados. https://www.mintic.gov.co/portal/715/articles-400515_recurso_1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2025b). Aclaración Circular 0017 del 2025. Aclaración Circular Externa No. 0017 del 23 de abril de 2025. https://www.mintic.gov.co/portal/715/articles-400515_recurso_2.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2025c, diciembre 2). Comunicado de prensa. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/419059:Comunicado-de-prensa

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Coljuegos, Policía Nacional de Colombia, Dirección de Investigación Criminal e Interpol y Federación Colombiana de Empresarios de Juegos de Suerte y Azar. (2020). Orden de bloqueo de sitios web (URL'S y/o dominios) con contenido de juego de suerte y azar ilegal en internet. Versión 2. https://www.coljuegos.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=251486.

Movistar Colombia [@MovistarCo]. (2022, enero 8). Hola es un gusto saludarte, Te informo que por disposición de las Autoridades competentes, la aplicación Tumblr ha sido bloqueada para ser usada en Colombia, no es una decisión de Movistar, te invitamos a continuar disfrutando de tu servicio con normalidad. Saludos. YR. [Tweet]] https://x.com/MovistarCo/status/1479296655820210178

Mundovideo. (2018, julio 19). Skrill en Colombia: bloqueado por Coljuegos?. https://www.mundovideo.com.co/casinos-colombia-noticias/skrill-en-colmbia-bloqueado-por-coljuegos/

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2022). Interrupciones del acceso a Internet: tendencias, causas, implicaciones jurídicas y efectos en una serie de derechos humanos. A/HRC/50/55. https://docs.un.org/es/a/hrc/50/55

OONI Explorer. (2022, enero 31). Web Connectivity Test, www.tumblr.com, AS10620. https://explorer.ooni.org/chart/mat?test_name=web_connectivity&axis_x=measurement_start_day&since=2021-12-01&until=2022-01-31&time_grain=day&probe_cc=CO&probe_asn=AS10620&domain=www.tumblr.com

Policía Nacional de Colombia, Dirección de Investigación Criminal e INTERPOL, Centro Cibernético Policial. (2022). Respuesta petición Consulta bloqueo URL.

ELEMENTOS PARA UNA DOCUMENTACIÓN DE LOS CORTES Y BLOQUEOS DE INTERNET DESDE UNA PERSPECTIVA PSICOSOCIAL

Lorena Peralta

Acompañante psicosocial y defensora de derechos humanos. Es especialista en seguridad y protección de personas defensoras, periodistas y víctimas de la violencia sociopolítica desde un enfoque psicosocial. Ha colaborado con diversas organizaciones en México, como el Centro de Derechos Humanos “Fray Francisco de Vitoria”, la Red Nacional de Organismos Civiles de Derechos Humanos “Todos los Derechos para Todas y Todos” y Aluna Acompañamiento Psicosocial.

Asimismo, ha acompañado a organizaciones de la sociedad civil en México y América Latina en procesos de fortalecimiento institucional, seguridad y acompañamiento psicosocial. Forma parte de la Comunidad de Seguridad de la Información y la Comunicación Latinoamericana (COSIC-Lat).

Este artículo fue posible gracias a las reflexiones conjuntas, aportes, conocimientos y acompañamiento de Jacobo Nájera en el proceso de escritura; y también a la motivación, lectura y observaciones de Pilar Sáenz.

Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

RESUMEN

Esta es una propuesta analítica con la que buscamos aportar elementos para realizar una documentación de cortes y bloqueos de internet desde un enfoque psicosocial. Queremos abonar a las valiosas metodologías que se han desarrollado para la documentación de cortes, bloqueos e interrupciones en la región con otros componentes de índole más subjetivos, pero que también problematizan estos fenómenos para develar no solo lo que está detrás sino lo que es posible desarrollar para afrontarlos.

PALABRAS CLAVE:

Psicosocial, violencia sociopolítica, impactos, afrontamientos.

Este documento fue realizado en el marco del proyecto CADE – Civil Society Alliances for Digital Empowerment. Ver más en https://cadeproject.org/

Esta publicación está cofinanciada por la Unión Europea. Su contenido es responsabilidad exclusiva de Fundación Karisma y no refleja necesariamente las opiniones de la Unión Europea.

INTRODUCCIÓN

Una consideración relevante a la que nos enfrentamos al construir esta propuesta con perspectiva psicosocial para abordar el fenómeno de los cortes y bloqueos de internet es que no basta con considerar la afectación de los derechos a la libertad de expresión y al acceso a la información. Cuando se afectan las vías de comunicación se impacta, en realidad, todo el espectro de derechos a la comunicación. Las personas desarrollamos diversos mecanismos de comunicación e, incluso, algunas nos involucramos en la construcción de las infraestructuras que la soportan. En un sentido profundo, es la comunicación con otras personas y nuestro entorno lo que media el sentido de nuestra vida.

Este artículo parte de una reflexión sobre la importancia de ampliar el campo psicosocial, además del técnico, en la documentación de estos fenómenos. Para ello, es imprescindible acercarnos a la propuesta teórico-metodológica del enfoque psicosocial, allí se expone el concepto y otras teorías que se han nutrido el enfoque psicosocial.

Posteriormente, ofrecemos un contexto internacional relacionado con los bloqueos e interrupciones ocurridas en Rusia, Colombia, Venezuela, Sudán y Guinea Ecuatorial. Esto nos permite introducir la relación entre poder, conflictividad social, intencionalidad y narrativa en el manejo de los cortes y bloqueos. Este marco contextual nos lleva a otra dimensión de análisis que se propone en el enfoque psicosocial: plantea identificar los impactos o daños que podrían generarse, a nivel individual y social, como consecuencia de estos cortes y bloqueos. Así, se expone qué es un impacto, cómo se relaciona con la violencia socio política y cuáles son esas dimensiones de la afectación.

En la siguiente parte presentamos los casos de Brasil, Ecuador y El Salvador, y proponemos algunas posibles explicaciones sobre lo que estaría detrás de la decisión de bloquear o interrumpir la conexión a una población. La intencionalidad, los intereses y los actores que podrían estar participando en este tipo de decisiones, que tienen repercusiones graves en el ejercicio de los derechos humanos.

Esto nos llevó a formular una serie de preguntas que abonen a la metodología de documentación existente desde la mirada psicosocial. Base que más adelante podría convertirse en una ruta de colaboración colectiva.

El artículo finaliza con algunas sugerencias para el acompañamiento digital desde el enfoque psicosocial, que apoyarían la documentación de cortes y bloqueos de internet.

Esta propuesta surge en el marco del encuentro de la red COSIC Lat en 2023, durante una sesión dedicada a explorar qué se entiende y cómo se abordan y registran incidentes de bloqueos de internet en la región. La discusión durante la sesión permitió concluir que la mirada psicosocial era un tema ausente. A partir de ese primer espacio, se mantuvo una conversación que¿{ posteriormente propuso una nueva sesión para el encuentro de esa misma red en 2024, donde, como un primer ejercicio de reflexión, se abordaron los bloqueos y cortes de internet en la región desde un enfoque psicosocial.

¿POR QUÉ HACER UN ANÁLISIS DESDE EL ENFOQUE PSICOSOCIAL?

Reconocemos un avance significativo en la construcción de las metodologías de registro y documentación distribuida sobre las fallas, o la ausencia, de sistemas de telecomunicaciones; principalmente, por cortes, bloqueos o disrupciones, y están enfocados en la arquitectura que permite su funcionamiento. En los países de América Latina, además, encontramos un esfuerzo constante en el desarrollo de metodologías específicas ajustadas a los contextos locales y, particularmente, para registrar los casos donde hay intencionalidad. Sin embargo, creemos necesario ampliar estas aproximaciones hacia las dimensiones sociales del fenómeno.

Nuestra propuesta de Elementos para una documentación de los cortes y bloqueos de internet desde una perspectiva psicosocial busca reconocer los impactos sociales desde dos dimensiones. Por una parte, la afectación que genera la ausencia de telecomunicaciones en las personas, colectividades, organizaciones populares, comunales y barriales para el ejercicio de sus derechos. La segunda, sobre cómo estas colectividades le dan significado y sentido a estas experiencias consumadas o latentes, que no solo incluye los efectos prácticos, visibles o inmediatos, sino cómo entienden las motivaciones, intenciones o simbolismos detrás de los cortes o bloqueos.

MARCO TEÓRICO POLÍTICO DEL ENFOQUE PSICOSOCIAL

Es usual que en momentos claves del contexto nos preguntemos desde dónde queremos abordar una realidad y desde dónde deseamos explicarla. El enfoque psicosocial es una metodología de abordaje para comprender y analizar críticamente la realidad enmarcada en un contexto de violencia sociopolítica. Se centra en analizar esas situaciones de violencia y represión, indagando en los daños y pérdidas, individuales y colectivas, que se originan por esos mismos actos. En sí, es un proceso de pensamiento crítico que lleva a una toma de acción-transformación, es decir, la dirección en la que se intentará resolver o afrontar la problemática y atender los daños. Según Aluna:

> el enfoque psicosocial es una perspectiva crítica de la Psicología Política sobre las relaciones de opresión y violencia de la sociedad y busca fortalecer las estrategias políticas y sociales de resistencia y autonomía de los sujetos políticos para la liberación de esas relaciones de opresión, violencia e injusticia (Aluna, 2017, p.18),

El enfoque se nutre de otros planteamientos teórico-políticos: la psicología de la liberación (Ignacio Martín Baró), la pedagogía crítica (Paulo Freire), la investigación acción participativa (Fals Borda), la epistemología del sur (Boaventura do Santos), la teoría marxista, el marco de derechos humanos y otras voces del sur global como Elizabeth Lira, Javier Giraldo, Isabel Rauber y Carlos Martín Beristain, entre otros. No es un enfoque estático, hay modelos psicosociales que han ido integrando la imbricación de las opresiones o la descolonización del feminismo.

La primera forma de acercarse al enfoque es situarnos contextualmente. Comprender e interpretar lo que está ocurriendo en situaciones donde el poder del Estado se expresa de manera contundente contra quienes se le oponen. Para ello, es necesario integrar el concepto de violencia sociopolítica y represión.

> Se asumirá la violencia sociopolítica como un tipo de violencia premeditada, organizada y sistemática que tiene unos objetivos claros ya sean políticos, económicos, sociales para dominar a través del terror a un grupo de personas organizadas, o no, que por su rol en la sociedad no les es útil (a quienes ejercen dicha violencia) para el modelo de sociedad que pretenden. Una de las estrategias más usadas en la violencia sociopolítica es el terror como mecanismo de guerra para doblegar la voluntad de las personas, siendo el miedo la emoción que impera ante la constante violación de los derechos humanos y el irrespeto por la vida (García, 2010).

A la vez, la violencia usa la represión política. Esta es definida como actos violentos ejercidos por el Estado, o con su anuencia, intencionados que buscan controlar, “corregir” actividades políticas o sociales y generar impactos psicosociales en la población (Correa, 2009). Por tanto, es importante reconocer la violencia sociopolítica y los mecanismos represivos usados por el poder para repensar las estrategias que intentan mantener un estado permanente de despojo, de inmovilidad y acostumbramiento.

Los impactos son como heridas sociales que afectan varios ámbitos de la vida, lo psicoemocional, lo político, lo organizativo, las creencias, lo espiritual, los vínculos, la cotidianidad y los proyectos, tanto personales, políticos y sociales. El acompañamiento psicosocial busca construir herramientas que ayuden a afrontar estas heridas abordando lo psicoemocional, también a fortalecer parte de la vida organizativa y los vínculos, así como a reafirmar o reorientar el rumbo político y a trabajar preventivamente la seguridad.

UBICACIÓN CONTEXTUAL DE LA VIOLENCIA SOCIOPOLÍTICA A TRAVÉS DEL CONTROL DIGITAL

¿Qué momento es el que marca a un país para tomar la decisión de interrumpir o bloquear la señal de internet? Este dependerá del contexto que se esté viviendo, como una forma de controlar lo que a sus ojos podría afectar su gobernanza. Por ejemplo, hay países donde la situación social y política era de mucha confrontación y se tomaron medidas digitales de corte autoritario para inhibir la protesta social.

En 2017, tras una decisión judicial en Rusia, el Servicio Federal para la Supervisión de Comunicaciones, Tecnologías de la Información y Medios Masivos (Roskomnadzor) incluyó la red Tor en su lista de sitios prohibidos. Sin embargo, el bloqueo efectivo del sitio no ocurrió sino hasta finales de 2021 (RuNetEcho, 2021), lo que ha generado mayores obstáculos para que la población acceda a información fuera del control del gobierno ruso. Esta tendencia se ha extendido a otros sitios de noticias desde el inicio de la guerra con Ucrania.

Aunque se trata de contextos distintos, estas formas de restricción también pueden identificarse en otros países que han operado de forma similar en relación con el acceso a la información. En 2021, en Colombia, en el marco de protestas que cuestionaban el gobierno del entonces presidente Iván Duque, se registraron cortes de internet y problemas con las publicaciones en las redes sociales donde se informaba sobre el Paro Nacional y las protestas.

> Algunas historias que referían al paro nacional y a las protestas que utilizaban los hashtags relacionados a la rebelión, fueron eliminadas antes de que se vencieran las 24 horas de circulación y en otros casos aparecían en blanco. En otros casos, los usuarios no podían comentar en Facebook (Bertoldi, 2021).

Si bien hubo dificultades para generar pruebas técnicas de estos cortes y no hay información oficial que permita demostrar que fueron acciones intencionadas, sí se generó un sentimiento de censura. El caso llegó hasta la Corte Constitucional de Colombia, la cual emitió la sentencia T-372 en 2023. En ella se declaró que el Estado vulneró los derechos a la libertad de expresión, de reunión y asociación por la ausencia de información sobre los cortes de internet denunciados y el posible uso de inhibidores de señal durante las protestas (Corte Constitucional de Colombia, 2023).

A inicios de 2025, en Venezuela, varios proveedores de internet bloquearon temporalmente la red social TikTok, la aplicación de mensajería instantánea Telegram y algunas VPN; además se restringió el acceso a DNS; lo que en la práctica inhabilitó el acceso a buscadores y sitios de noticias. En 2024, en el periodo electoral, la red X fue bloqueada con argumentos de incitar al odio y orquestar un golpe de Estado cibernético contra el gobierno de Nicolás Maduro. La organización civil VE Sin Filtro reportó esta serie de bloqueos. Sobre el bloqueo de Telegram añade:

Esta restricción duró algunas horas y no fue la primera vez, ya que en el contexto de las protestas tras las elecciones del 28 de julio de 2024 también se registraron restricciones para el uso de la plataforma. Además, otras aplicaciones similares como Signal también fueron afectadas por este tipo de bloqueos (Tagliafico, 2025).

En Sudán la situación es sumamente crítica, desde que inició el conflicto armado interno, en 2024, el control del servicio de internet se ha convertido en una disputa estratégica. A medida que se controlan territorios, se identifican sitios web susceptibles a ser bloqueados con el fin de controlar el flujo de información donde hay presencia del grupo armado opuesto. En otras zonas, después de confiscar el servicio, este se vende a precios exorbitantes y, en el peor de los casos, hay zonas donde eliminan los dispositivos que hacen posible el servicio. El patrón de interrumpir la señal ya había sido utilizado por el gobierno sudanés durante protestas sociales, antes del actual conflicto. Ahora, es un arma de guerra:

anteriormente, las interrupciones de internet eran principalmente una táctica empleada por el gobierno sudanés para suprimir la disidencia. Ahora, tanto las Fuerzas Armadas Sudanesas como el grupo paramilitar Fuerzas de Apoyo Rápido están utilizando cierres para controlar el flujo de información dentro de los territorios en poder de la parte opuesta (Mohammed, 2025).

Por último, en 2024, parte del territorio Annobón, una isla perteneciente a Guinea Ecuatorial, donde recursos naturales han sido explotados y saqueados con la anuencia del gobierno, varias personas han sido desaparecidas y criminalizadas. Además, a la población le fueron confiscados los celulares y el internet ha sido interrumpido totalmente. En 2013 y 2017 hubo bloqueos de Facebook e interrupción de internet por varios días. Era periodo electoral y había descontento social (Access Now, 2025).

Las situaciones mencionadas tienen en común la disputa con el poder, o por el poder. Los Estados autoritarios y criminales se caracterizan por ejercer acciones violentas contra la población, acompañadas de una confrontación psicológica y mediática que busca generar miedo y terror. Al mismo tiempo, construyen narrativas que señalan un supuesto enemigo para justificar su accionar, sustentándose en la impunidad.

Encontramos una alta carga de violencia asociada al control de la conexión. Los cortes y bloqueos se usan de manera discrecional o como mecanismo para sacar ventaja en contextos de tensión. En Colombia y Venezuela estas acciones parecen asociadas al control de protestas sociales; en Sudán, a la disputa por el poder entre dos grupos armados, con la población como víctima en medio del conflicto; en Guinea Ecuatorial, a la intención de inhibir o manipular la participación electoral, mientras que en la isla de Annobón buscan castigar a la población por oponerse a la actividad minera. La narrativa del poder en estos casos apunta a legitimar medidas extremas como mecanismos necesarios para mantener la gobernabilidad y controlar la disidencia social.

Otro punto que quizá requerirá reflexión es el rol de los intermediarios de internet, especialmente las empresas privadas, en el cumplimiento de los estándares de derechos humanos y los derechos digitales.

IMPACTOS, LAS DIMENSIONES DEL DAÑO

Hasta ahora hemos planteado que la violencia sociopolítica tiene la intención de romper la comunidad y su organización usando el miedo y múltiples estrategias de control, entre ellas el uso de tecnología. Estas estrategias, incluso cuando se declara la razón de su uso, causan daños a nivel individual y colectivo, poniendo en riesgo la salud mental y el desarrollo social y político de una población. ¿Hay conciencia del alcance o de la dimensión del daño que ocasiona un corte o bloqueo de internet? Anteriormente vimos los contextos en los que ocurren violaciones a los derechos humanos y los derechos digitales, a continuación ahondamos sobre los posibles daños generados por dichas situaciones.

El impacto puede entenderse como un daño, una herida, una pérdida o una tensión producto de una vivencia que afecta significativamente a las personas, dejando una huella permanente en ellas y poniendo en riesgo su bienestar físico, emocional y mental. La violencia sociopolítica afecta la cotidianidad, la vida y el bienestar individual y colectivo, limitando con ello las posibilidades de transformación social

Las manifestaciones de estos daños se expresan en varias dimensiones[9]. A continuación, intentamos suponer posibles afectaciones ocasionadas por los cortes y bloqueos de internet, algunas ya fueron mencionadas en los casos anteriores. En las notas periodísticas encontradas se registra el interés generado por la crisis humanitaria ocasionada por la falta de internet, pero hasta el momento se desconoce si se tiene algún tipo de metodología para documentar o identificar daños psicosociales.

Nos parece importante señalar que estos daños son tanto individuales como colectivos y que cada experiencia es única. La intensidad del daño también dependerá de las vivencias, los recursos y redes de apoyo, entre otros elementos, que se tengan para enfrentar la situación.

Dimensión emocional: ansiedad, angustia, incertidumbre, tristeza, depresión, culpa, impotencia, duelos múltiples o desesperanza, entre otros. Hay una emoción que es persistente en cualquier situación de violencia sociopolítica y represión: el miedo. El miedo es una emoción natural, nos permite estar alerta para responder a una situación tensa, cada persona lo experimenta de diferente manera. Hay una alteración de la realidad, nuestro mundo interno lo interpreta de una forma, no hay claridad de dónde está el riesgo. Genera la sensación de vulnerabilidad, desprotección y en la cual no se puede tener control de lo que sucede, no depende de mí. El miedo es una emoción que el poder ha usado para controlar a las sociedades; paraliza, mantiene a la gente en casa, les hace desconfiar o alimenta conflictos, además de retroalimentar el temor.

9. Es una tipología sugerida que bien puede reformularse de acuerdo con la necesidad o pertinencia de quien documenta, acompaña o quién se acompaña.

Access Now ha recogido testimonios en algunos territorios donde ha documentado cortes y bloqueos de internet. Un habitante de Annobón en Guinea Ecuatorial relata:

- Mi padre está en la cárcel en Annobón, aunque ni yo ni el resto de mi familia tenemos claro por qué fue arrestado, ni por qué fue detenido. Es imposible hablar con él, y extremadamente difícil comunicarse con otros familiares en la isla, ya que las llamadas telefónicas regulares son muy costosas. Antes del apagón, podía usar WhatsApp e Imo para llamar a personas en Annobón, y así podía hablar con regularidad con mi familia, incluido mi padre. Pero ahora no sé cómo ayudar. Toda mi familia se siente impotente y desesperanzada ya que no sabemos cuánto tiempo más durará esta pesadilla (Access Now, 2025).

- Dimensión de pensamientos: la realidad es amenazante, pesimismo o auto reproche.

- Dimensión física: palpitaciones, dolor en el pecho, dificultad para respirar, alteraciones del sueño y la alimentación, sudoración, problemas de salud o desgaste.

- Un habitante de Sudán narró: "I've lost contact with my entire family located in areas controlled by the militia. Now, I am taking sedatives just to get some sleep"[10] (Access Now, 2024).

- Dimensión de comportamiento: falta de concentración, aislamiento, irritabilidad, silenciamiento, acostumbramiento, negación, desorganización de la conducta o estado permanente de alerta.

- Dimensión política: cuestionamiento del sentido de lucha, abandono o minimización de las estrategias, ruptura o rigidez de posturas, conformismo, cambio de roles, interrupción de la denuncia digital en tiempo real, se deja de tener o de plantear una contra-narrativa al poder, inhibición para generar contenido, falta de alcance para informar en otras latitudes, suspensión de cuentas, redirección a otros sitios, estigmatización, funa digital[11] o uso de la tecnología para hacer daño (drones de ataque).

- Dimensión organizativa, social y familiar: inhibe o suspende la comunicación, desconexión digital, desconfianza comunitaria, falta de apoyo o participación, parálisis social o pasividad, ruptura de vínculos afectivos y de confianza, estigma, polarización, culpabilizar a otros, falta de acceso a información diversa para verificar violaciones a derechos humanos, imposibilidad para solicitar ayuda médica o algún otro tipo de auxilio, limita la movilidad porque no hay certeza de rutas o sitios seguros, cambio del proyecto de vida, deterioro económico porque no se puede acceder al dinero, alejamiento de círculos familiares y sociales, incremento en los costos del servicio de internet, desplazamiento, hambruna o interrupción de trámites para conseguir papeles vitales para su protección.

10. Traducción: He perdido el contacto con toda mi familia situada en zonas controladas por la milicia. Ahora tomo sedantes para poder dormir.
11. Funar digitalmente se refiere a las acciones que buscan exponer o denunciar en redes sociales a personas o instituciones que se considera han cometido actos inmorales, ilegales o reprensibles socialmente.

MODELOS ANALÍTICOS EN AMÉRICA LATINA: BRASIL, ECUADOR Y EL SALVADOR

Bloqueo de X/Twitter en Brasil

El 31 de agosto de 2024, inició un bloqueo de acceso a X en Brasil debido a una decisión de la Corte Suprema. La orden estuvo justificada porque la empresa incumplió órdenes judiciales luego de que X restableciera cuentas que fueron suspendidas por una orden judicial. El Supremo Tribunal Federal había ordenado la eliminación de siete cuentas de extrema derecha asociadas con el ataque al congreso de 2023, en Brasilia.

La decisión de bloqueo dejó a millones de personas fuera de la red social. Este caso plantea discusiones necesarias: la falta de claridad en la regulación de las redes y también si debe haber límites a la libertad de expresión, o cuáles serían estos límites sin demeritar otros derechos[12].

Sin embargo, la situación también develó cómo Elon Musk usa su poder, a través de las corporaciones bajo su control, para “opinar” y confrontar a gobiernos percibidos como liberales de izquierda, mientras manifiesta su apoyo a actores políticos de derecha como Jair Bolsonaro. Es un ícono del establecimiento que moldea narrativas en la opinión pública y las moviliza a su interés, su empresa X es la plataforma idónea para ello.

Interrupción al servicio de internet en Ecuador

Desde la tercera semana de abril hasta el 1 de mayo de 2024, Ecuador enfrentó interrupciones en el servicio de internet en varias de sus provincias, atribuidas a racionamientos prolongados y recurrentes de energía eléctrica que duraron más de ocho horas diarias, según informaron los proveedores de telecomunicaciones. Desde mediados de septiembre de 2024, la situación se agudizó y todo el territorio ecuatoriano enfrentó apagones de hasta 14 horas diarias. Estos se asociaron a la falta de mantenimiento e inversión en la red hidroeléctrica, a la sequía que redujo la capacidad de generación, y a medidas temporales de dudosa efectividad, como el alquiler de barcazas generadoras a una empresa turca que no alcanzaron a cubrir la demanda.

Ecuador se despertó con una mala noticia: la barcaza contratada para generar 100 MW, en estos momentos de crisis eléctrica, solo está generando 12 MW. Las razones aún son opacas, pues no ha habido un pronunciamiento oficial. Hay hipótesis relacionadas con falta de combustible o inestabilidad de la red de transmisión (Redacción La Fuente, 2024).

12. En 2025, el Tribunal Supremo de Brasil empezó un debate sobre legislar el rol de las redes para difundir noticias falsas y discursos de odio. Uno de los casos que animan es el del bloqueo de X en Brasil en 2024. Disponible en: https://www.pagina12.com.ar/831219-brasil-vuelve-a-debatir-la-regulacion-de-las-redes-sociales

Sin embargo, medios independientes apuntan a otra posible causa: la intención de generar una situación crítica de ineficiencia y abandono para privatizar el servicio eléctrico. Los apagones han sido una manifestación de ese abandono, de ahí que infieran que hay un acto intencionado. La Revista Crisis afirma que:

> la Cámara de Comercio de Quito, en la que se instaba al Gobierno Nacional a "permitir" la iniciativa privada en el sector energético, ya que el Estado resulta "ineficiente e incompetente" para solucionar la crisis. Adicionalmente, la CCQ anunciaba la supuesta dificultad de sostener plazas de empleo bajo condiciones de crisis energética, pretendiendo sacar un doble rédito al argumento en cuestión. Este relato refleja a la perfección la implementación de la doctrina del shock. Desfinanciación, seguida por falta de mantenimiento, adicional a una cruenta campaña de difamación y desprestigio, falla y obsolescencia del servicio público, culminando en la propuesta de una "solución", con la que ya se contaba desde un principio (Revista Crisis, 2024).

Hubo intentos en Ecuador de privatizar el servicio de energía en 2021, con el entonces presidente Guillermo Lasso. También, en 2023, Daniel Noboa propuso reformas a la Ley Orgánica del Servicio Público de Energía Eléctrica y a la Ley Orgánica de Eficiencia Energética, a través de otro proyecto de ley: la Ley Orgánica de Competitividad Energética. Hasta ahora este servicio estratégico sigue en manos del Estado, pero de aprobar este proyecto se abrirían las puertas al mercado privado.

Bloqueo de Telegram en El Salvador

En septiembre de 2024 se registró el bloqueo de Telegram en El Salvador, desde diferentes proveedores de internet, esto a partir de las mediciones del Observatorio Abierto en la Red. Se estima que el bloqueo solamente duró un día y al día siguiente fue posible acceder de nuevo al servicio de Telegram. Organizaciones sociales han pedido transparencia sobre lo ocurrido, porque, además, hay antecedentes de que esta no ha sido la única ocasión en que se bloquea el servicio de Telegram en el país.

En un comunicado firmado por Access Now, Artículo 19, la Red Centroamericana de Periodistas y la Asociación de Periodistas de El Salvador denunciaron:

> Miramos con preocupación los incidentes en El Salvador, sobre todo dadas las condiciones adversas para la libertad de prensa que actualmente subyacen en el país. Durante las elecciones, APES corroboró en conjunto con otras organizaciones de libertad de expresión algunas de estas problemáticas como son la falta de acceso a la información pública, la implementación de sistemas de vigilancia como forma de intimidación y disuasión y el aumento de las campañas de desprestigio solo por mencionar algunas que se han convertido en patrones represivos en la región (Access Now 2024b).

La primera vez, en abril del mismo año, el bloqueo se da en el contexto de las protestas por la segunda posesión de Nayib Bukele, y la amenaza de filtraciones de información en contra de instituciones del Gobierno que ocurrían por medio de Telegram. El bloqueo en septiembre coincidió con reportajes sobre la muerte del exasesor de seguridad nacional Alejandro Muyshondt[13] y el posible espionaje a políticos y periodistas opositores al gobierno.

Los tres casos presentados, ocurridos en 2024, evidencian el control de las comunicaciones y de su infraestructura como mecanismo para concretar agendas de la clase política, que en ocasiones se entrecruzan con intereses corporativos.

Este tipo de situación nos lleva a reflexionar sobre el hecho de que, si bien es vital la documentación técnica de cortes, bloqueos o interrupciones, es necesario ir más allá. Es necesario no quedarnos con la idea de que todo se puede cuantificar o cualificar desde lo técnico; también es necesario documentar el contexto. La tendencia a medir sin contextualizar es un método que hay que descolonizar. La sociedad, politizada o no, tiene un significado en relación con todo lo demás. Es decir, hay que sumar a la ausencia de medios de comunicación producto del corte mismo, además de la afectación al derecho a la libre expresión y el acceso a la información, la cascada de otras violaciones a derechos humanos que pueden derivarse o percibirse de estas acciones, decisiones y circunstancias.

Además, queremos resaltar cómo se va construyendo el imaginario político del enemigo y cómo la clase política en el poder encuentra mecanismos para desactivarlo, inmovilizarlo o silenciarlo. Y en ello, cómo se alimenta la polarización social a través de una narrativa que no posibilita el diálogo, que no tiene sustento argumentativo y que, en algunos casos, apela o exacerba ciertas emociones como el odio. Encontramos un vínculo entre lo psicosocial y lo político, que trasciende la dimensión política de lo virtual al espacio físico y que deriva en una guerra psicológica hacia ciertos procesos de ideologización, de inoculación del miedo y, por tanto, de alienación de las sociedades. A su vez, los poderosos combinan otras herramientas, digitales y análogas, para hacer más efectivo el control.

De igual manera, las corporaciones se fortalecen al querer mantener la ambigüedad legal sobre el uso y operación de plataformas, al igual que por la falta de auditoría social sobre ellas y el gran poder que concentran al controlar la comunicación, las narrativas y la difusión de información.

Por otro lado, en estas y otras situaciones, no es posible soslayar la responsabilidad del Estado para atenuar la magnitud de la afectación y al responder a las emergencias de una manera inmediata, adecuada y empática con la población, sobre todo cuando los actos no son claramente intencionados y tienen que ver más con fallas técnicas.

13. Fallecido en un hospital bajo custodia por neumonía, aunque su defensa declaró haber sido torturado. Fue acusado de ser doble agente del expresidente Mauricio Funes. Muyshondt previamente había acusado a funcionarios cercanos a Bukele y a un miembro del congreso de tener nexos con crimen organizado (Espinoza, 2024).

Parte de la responsabilidad ética del Estado y las corporaciones es comunicar clara y transparentemente por qué ocurrió y qué se está haciendo. Brindar información permite salir del estado de confusión que generan los cortes, bloqueos o interrupciones, brindando tranquilidad mental al no alimentar el miedo social.

Reiteramos que documentar la falla técnica con la intención, contexto, actores involucrados y daños generados en todas sus dimensiones nos ayudará a comprender y recordar la evolución de las formas de control. También es útil para construir las formas de afrontarlo con la posibilidad de reconectar, considerando esta acción en su sentido más amplio. Para así, seguir existiendo desde las luchas de transformación, o recuperando otras formas de comunicación no digitales, para mantener el bienestar físico, mental y vivir dignamente.

¿CÓMO SE PODRÍA DOCUMENTAR UN CORTE O BLOQUEO DESDE UN ENFOQUE PSICOSOCIAL?

A partir de lo anterior, proponemos pensar y abonar a la metodología de documentación de cortes y bloqueos ya existentes desde una perspectiva psicosocial. Podemos iniciar cuestionandonos: ¿qué preguntas podríamos hacernos para tener información que sume al análisis de la situación desde un enfoque psicosocial?

- ¿Sabe o se imagina por qué está ocurriendo el corte, bloqueo o interrupción?
- ¿Tiene conocimiento del alcance geográfico de la afectación?
- ¿Sabe si hubo otro grupo de la población que haya sido más afectado?, ¿De qué manera?
- ¿Conoce si alguna autoridad o empresa ha informado sobre lo ocurrido y sobre las medidas que está haciendo para resolver el problema?
- ¿Ubica alguna otra información sobre lo ocurrido que no sea institucional?
- ¿Qué ideas o pensamientos le provocaron el corte, bloqueo o interrupción?
- ¿Cómo lo vivió, qué sintió en el cuerpo y sus emociones?
- ¿Qué hizo para enfrentar la situación o qué medidas tuvo a su alcance que le proporcionaron tranquilidad?
- ¿Este corte, bloqueo o interrupción cómo afecta su cotidianidad, trabajo, su relaciones comunitarias, integración social y luchas? ¿Identifica otra afectación personal?
- ¿Cómo afecta a su comunidad y a la sociedad?

Este no es un listado exhaustivo de preguntas, pero algunas de ellas podrían utilizarse para iniciar un diálogo empático, cuidadoso, respetuoso y con pertinencia cultural y diversa. Las preguntas son una orientación, pero no deben ser usadas de manera extractiva, reduciéndolas a una dinámica de pregunta-respuesta.

ORIENTACIONES PARA EL ACOMPAÑAMIENTO PSICOSOCIAL COMO UNA FORMA DE SEGUIR DEFENDIENDO LOS DERECHOS DIGITALES

La comunicación inicia no hablando, sino escuchando. Es fundamental generar confianza y empatía, identificar los códigos culturales y contextuales, dialogar sobre las experiencias y visualizar todas sus dimensiones. Ese es el primer auxilio. Cada situación se experimenta de manera única y en ocasiones será prioritario empezar por la parte subjetiva (psicoemocional) para posteriormente atender la parte técnica-política. Priorizar ayuda a tomar decisiones y, a veces, será posible realizar los acompañamientos en paralelo. El camino no es único, desde esta perspectiva, vamos construyendo y adecuando.

El acompañamiento ayuda a transitar de un estado de confusión a uno de claridad y de posible toma de acción. En situaciones de violencia sociopolítica es imprescindible nombrar lo que está ocurriendo, reconocer lo que nos pasa y validar lo que se siente. Buscamos fortalecer a las personas a identificar todo aquello que permite enfrentar situaciones que causan algún tipo de sufrimiento. Paralelamente, también es importante ser conscientes de los límites del acompañamiento. La idea es avanzar hacia la autonomía.

Los afrontamientos son el némesis de los impactos. Así como es importante identificar los daños, es vital identificar aquello que nos puede mantener en pie, que nos dignifica aún en la adversidad más acuciante. Las siguientes son algunas formas de afrontamiento:

- Afirmar el sentido, los sueños, la utopía política y compartirla con otras personas.
- Buscar o fortalecer nuestras redes de apoyo: familia, colectiva, comunidad y amistades, entre otras.
- Reconocer y resignificar el momento histórico en que vivimos y aportamos.
- Validar, visibilizar y compartir los impactos, daños, pérdidas o tensiones.
- Intencionar espacios de confianza para socializar emociones, pensamientos y hablar del miedo.
- Buscar espacios para fortalecer el espíritu o mantener prácticas, rituales o celebraciones que nos brinden bienestar.
- Organizarnos comunitariamente (en el barrio, la colonia o el edificio, entre otros).

- Reforzar el sentido de la vida, de los vínculos y los proyectos de vida personal y familiar.
- Tener una mirada estratégica de la situación y de las rutas para abordarla.
- Identificar y fortalecer otras formas de comunicación analógicas o recuperar algunas en desuso, pero efectivas.
- Elaborar otras formas información que contrarresten la desinformación.
- Desarrollar estrategias digitales y territoriales (en las calles, en los barrios, las colonias o las comunidades).

REFERENCIAS

Access Now. (2024a). #KeepItOn: Las autoridades de Guinea Ecuatorial deben poner fin al bloqueo de internet y otros abusos a los derechos humanos en Annobón. https://www.accessnow.org/press-release/keepiton-las-autoridades-de-guinea-ecuatorial-deben-poner-fin-al-bloqueo-de-internet-en-annobon/

Access Now. (2024b). El conflicto de Sudán: Cómo los cierres de internet profundizan una crisis humanitaria. https://www.accessnow.org/the-sudan-conflict-how-internet-shutdowns-deepen-a-humanitarian-crisis/

Access Now. (2025). ¿Por qué el apagón de internet en Annobón debería importarle a todo el mundo? https://www.accessnow.org/historias-apagon-annobon/

Agencia Lupa. (2024, septiembre 2). Bloqueo de X en Brasil: Te explicamos lo que está pasando contra la pelea legal entre Alexandre de Moraes y Elon Musk. Chequeado. https://chequeado.com/el-explicador/bloqueo-de-x-en-brasil-te-explicamos-lo-que-esta-pasando-con-la-pelea-legal-entre-alexandre-de-moraes-y-elon-musk/

Aluna Acompañamiento Psicosocial. (2017). Modelo de acompañamiento psicosocial

Aluna. Aluna Acompañamiento Psicosocial y Pan Para el Mundo.

Artículo 19. (2024, septiembre 24). Comunicado conjunto de Access Now, Artículo 19, la Red Centroamericana de Periodistas y la Asociación de Periodistas de El Salvador: Sociedad civil y periodistas exigen transparencia sobre la interrupción de la plataforma de mensajería Telegram. https://articulo19.org/sociedad-civil-y-periodistas-exigen-transparencia-sobre-la-interrupcion-de-la-plataforma-de-mensajeria-telegram/

Beltrán Luna, J. (2024). Las denuncias que llevaron a Alejandro Muyshondt a la cárcel… y a la muerte. ElSalvador.com. https://www.elsalvador.com/noticias/nacional/denuncias-llevaron-alejandro-muyshondt-caracel-muerte/1122483/2024/

Bertoldi, V. (2021). Censura en Colombia: Bloquean el acceso a internet y eliminan contenido de redes sociales. Izquierda Web. https://izquierdaweb.com/censura-en-colombia-bloquean-el-acceso-a-internet-y-eliminan-contenido-de-redes-sociales/

Correa, C. (2009). En J. E. González Ruíz (Coord.), Balance de los derechos humanos en el "sexenio del cambio". Universidad Autónoma de la Ciudad de México.

Corte Constitucional de Colombia. (2023). Sentencia T-372 de 2023. https://www.corteconstitucional.gov.co/relatoria/2023/t-372-23.htm#_ftnref1

Dávalos, P. (2024). Ecuador: Hacia la privatización del sector energético ecuatoriano. Resumen Latinoamericano. https://www.resumenlatinoamericano.org/2024/01/08/ecuador-hacia-la-privatizacion-del-sector-energetico-ecuatoriano/

Editorial Revista Crisis. (2024, octubre 14). Noboa apaga la luz para privatizarla. Revista Crisis. https://www.revistacrisis.com/editorial/noboa-apaga-la-luz-para-privatizarla

Espinoza, C. (2024). La muerte de Alejandro fue un homicidio, inducido y controlado para callarlo. La Prensa Gráfica. https://www.laprensagrafica.com/elsalvador/La-muerte-de-Alejandro-fue-un-homicidio-inducido-y-controlado-para-callarlo-20240216-0089.html

García Méndez, H. L. (2010). La violencia sociopolítica, una realidad colombiana: Abordaje desde la psicología jurídica. Comisión Intereclesial de Justicia y Paz. https://www.justiciaypazcolombia.com/la-violencia-sociopolitica-una-realidad-colombiana-abordaje-desde-la-psicologia-juridica/

Janosch, D. y Knight, B. (2024). Elon Musk, más poderoso que nunca. Deutsche Welle. https://www.dw.com/es/elon-musk-domina-cada-vez-m%C3%A1s-la-tecnolog%C3%ADa-y-la-pol%C3%ADtica/a-70608595

La Fuente. (2024, septiembre 25). Barcaza baja su producción eléctrica a 12 MW, en medio de la crisis de apagones. https://periodismodeinvestigacion.com/2024/09/25/apagones-barcaza-karpowership/

Mohamed, E. (2025). Campo de batalla digital de Sudán: La militarización de los cierres de internet en el conflicto. LSE Middle East Centre Blog. https://blogs.lse.ac.uk/mec/2025/03/31/sudans-digital-battleground-the-weaponisation-of-internet-shutdowns-in-conflict/

Página 12. (2025, junio 4). Brasil vuelve a debatir la regulación de las redes sociales. https://www.pagina12.com.ar/831219-brasil-vuelve-a-debatir-la-regulacion-de-las-redes-sociales

RuNetEcho. (2021). Rusia bloquea el acceso al sitio del navegador TOR (R. Navarro, Trad.). Global Voices. https://es.globalvoices.org/2021/12/12/rusia-bloquea-acceso-al-sitio-del-navegador-tor/

Tagliafico, F. (2025). #Te explicamos: ¿Cuáles son las páginas y redes sociales que han sido bloqueadas en Venezuela? El Diario. https://eldiario.com/2025/01/17/cuales-son-paginas-redes-sociales-bloqueadas-venezuela/


Fundación
Karisma
karisma.org.co
fundacion karisma
karismacol
@karisma