DERECHO Y POLITICAS HUMANITARIAS

Sin conexión y en peligro: las consecuencias humanitarias de las interrupciones de la conectividad

julio 14, 2025, Análisis / Comunicaciones / Nuevas tecnologías

15 mins read

Cléa Thouin
Asesora sobre Protección en la Era Digital en la Delegación del CICR para el Ciberespacio y el Centro Cibernético Global

Mientras que en todo el mundo las personas dependen más y más de las redes digitales y de telecomunicaciones para acceder a servicios esenciales, ponerse en contacto con sus seres queridos y buscar ayuda, las interrupciones cada vez más frecuentes de los servicios de conectividad en los conflictos armados son un motivo de creciente preocupación por la seguridad y la dignidad de la población.

En el presente artículo, la especialista en protección del CICR, Cléa Thouin, reflexiona sobre las consecuencias humanitarias que traen aparejadas esas interrupciones —situaciones en las que se pierde parcial o totalmente el acceso a las redes digitales o de telecomunicaciones— y sobre la necesidad de abordar las causas y mitigar los efectos, especialmente en contextos en los que la conectividad puede marcar la diferencia entre la vida y la muerte.

ICRC Humanitarian Law & Policy Blog · Offline and in danger: the humanitarian consequences of connectivity disruptions

¿Hasta qué punto depende su vida de la conectividad? Debido a que las sociedades están cada vez más digitalizadas, la conectividad —y en particular el acceso a internet— desempeña un papel cada vez más importante en la vida cotidiana de muchas personas, ya sea en cuestiones más mundanas como las plataformas que nos brindan entretenimiento o en tareas más esenciales como mantenernos en contacto con nuestros seres queridos, comunicarnos en el ámbito laboral, concertar citas médicas y realizar transacciones financieras. Por eso, cuando se interrumpe la conectividad en tiempos de conflicto armado o crisis, es posible que haya mucho en juego. En esos momentos, la conectividad ya no es solo una cuestión de comodidad: es un recurso que salva vidas.

Sin conectividad, cuando comienzan las operaciones militares, puede resultar casi imposible obtener información precisa y vital sobre rutas de evacuación seguras o sobre las zonas afectadas por las hostilidades. Quienes intentan cruzar una frontera internacional en busca de protección tal vez no puedan obtener documentación esencial almacenada en línea ni acceder a ella. Es posible que quienes habitan las zonas afectadas por las interrupciones se queden sin recursos financieros para adquirir bienes esenciales cuando los servicios de dinero móvil dejan de funcionar, y los familiares tal vez se queden sin noticias sobre lo que les ha ocurrido a sus seres queridos.

En los últimos años, muchas organizaciones –entre ellas *Access Now*, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (*ACNUDH*), la organización Global System for Mobile Communications Association (*GSMA*) y el *CICR* han puesto de relieve los efectos devastadores que producen las interrupciones de la conectividad en las personas y comunidades afectadas por conflictos armados. Ante su creciente incidencia, es fundamental que el sector humanitario comprenda y aborde mejor las causas y consecuencias de las interrupciones de la conectividad para poder ofrecer una respuesta humanitaria eficaz a las poblaciones afectadas.

En situaciones de conflicto armado, la interrupción de la conectividad puede producirse por varios motivos. A menudo, puede tratarse de un efecto incidental de las hostilidades, como cuando los equipos de mantenimiento no logran llegar de forma segura a las zonas afectadas por el conflicto armado para reparar o mantener la infraestructura física que permite la conectividad o cuando escasean los insumos necesarios para la conectividad –en particular la electricidad o el combustible– o bien como consecuencia de interrupciones en la cadena de suministro.

En situaciones de conflicto armado, se observan *cada vez más* restricciones deliberadas de la conectividad, en las que las interrupciones son el resultado de medidas intencionales o selectivas*[1]*, con actores que atentan contra la conectividad tanto en zonas bajo su control como en zonas bajo el control de otros. Por ejemplo, las autoridades y otros actores pueden llevar a cabo interrupciones técnicas, específicamente dando la orden a los proveedores de servicios de internet de que interrumpan la conectividad a internet o bien presionándolos para que lo hagan. Los ciberataques contra los proveedores de servicios de internet o las empresas de telecomunicaciones, así como los actos físicos de sabotaje, también pueden ocasionar interrupciones en la conectividad. Las operaciones militares pueden dañar o destruir deliberadamente la infraestructura física necesaria para la conectividad, como las torres de telefonía móvil o los cables de fibra óptica. También pueden utilizarse medidas electromagnéticas como la interferencia para afectar la conectividad, ya sea mientras duren las operaciones militares o de forma más permanente.

Una amenaza adicional a la vida, la seguridad y la dignidad de las personas

En *Etiopía*, *Gaza*, *Myanmar*, *Sudán* y otros lugares, las interrupciones de la conectividad han tenido efectos enormemente perjudiciales para las personas afectadas por conflictos armados. Como suele ocurrir, los más afectados son los niños, las mujeres, los ancianos, las personas con discapacidad, así como las personas desplazadas o migrantes.

Cuando se interrumpe la conectividad, las comunidades cuentan con menos posibilidades de buscar y recibir *información* vital sobre las hostilidades en curso, las rutas de evacuación seguras, así como la disponibilidad y ubicación de refugios, servicios esenciales y asistencia médica o humanitaria. Esta falta de visibilidad aumenta el riesgo de que se expongan a situaciones de violencia y a daños físicos, o de que no puedan recibir tratamiento en caso de que sufran lesiones o enfermedades. También aumenta el *riesgo* de desinformación y de que se difunda información errónea, ya que los hechos comunicados no pueden cotejarse fácilmente con fuentes confiables, por lo que la población queda expuesta a más peligros o alejada de la protección y la asistencia.

Sin acceso a internet, las comunidades también cuentan con menos recursos para *organizar* sus propias respuestas y comunicar sus necesidades a las autoridades y los actores humanitarios, lo cual reduce su capacidad de resiliencia ante situaciones de crisis e incluso puede privarlas de obtener la asistencia que tanto necesitan durante períodos prolongados. En muchos lugares, y sobre todo en zonas rurales o de difícil acceso, las comunidades suelen depender de la conectividad para *ponerse en contacto con servicios de emergencia* como ambulancias o servicios de rescate; por ende, sin conectividad, aumenta el riesgo de que se produzcan muertes evitables y los habitantes se exponen a un mayor peligro al tener que ocuparse de buscar ayuda en otro lugar. La falta de conectividad también incide en la capacidad de las personas para recuperar o tratar de obtener documentación y certificados importantes antes de evacuar zonas afectadas por conflictos armados, por lo que se les dificulta aún más cruzar las líneas del frente o las fronteras internacionales en busca de seguridad o protección internacional.

La prestación de servicios esenciales quizá se vea interrumpida o se torne poco confiable ya que, en la actualidad, la infraestructura crítica que permite el funcionamiento de los servicios públicos esenciales generalmente utiliza la conectividad y depende de ella para funcionar. Es posible que la *infraestructura* de agua, aguas residuales y electricidad no funcione con normalidad o incluso quede inutilizada, lo que supone importantes riesgos para la salud pública. Los hospitales y los proveedores de servicios de salud, ya sobrecargados de trabajo, tal vez no puedan acceder a los archivos de los pacientes, programar cirugías u ofrecer *atención médica especializada de guardia* sin una conectividad confiable. En zonas alejadas, donde la *telemedicina* aporta una ayuda indispensable, es posible que las comunidades se queden sin acceso a la asistencia de salud. Los sistemas de alerta y notificación nacionales o locales, entre los que se incluyen los relativos a catástrofes naturales, también pueden verse afectados por la falta de conectividad, lo cual deja a la población sin la preparación necesaria para hacer frente a las emergencias.

La interrupción de la conectividad imposibilita el contacto entre familiares que han quedado separados a ambos lados de una línea del frente o de una frontera internacional, muchas veces en los momentos de mayor intensidad de las hostilidades, de modo que les impide confirmar qué ha ocurrido con sus familiares y aumenta el riesgo de que desaparezcan personas. Esta situación puede generar una importante carga psicológica, que se suma al estrés, la ansiedad y los traumas de vivir en contextos de conflicto armado.

En lugares donde las herramientas de aprendizaje digital han surgido como *soluciones esenciales*, el acceso a la educación suele verse comprometido cuando se interrumpe la conectividad, ya que los estudiantes no pueden inscribirse en la universidad, asistir a clase o presentarse a exámenes. También se ha informado profusamente que las restricciones a la conectividad repercuten en los medios de subsistencia de la población y en su acceso a oportunidades económicas. En muchos países afectados por conflictos armados, una gran cantidad de personas depende cada vez más de los servicios financieros digitales, como *el dinero móvil* y las remesas del extranjero, que se han visto muy afectadas por las restricciones a la conectividad. Además, muchos hogares de zonas afectadas por situaciones de violencia dependen de actividades comerciales en línea para subsistir, lo que significa que las interrupciones de los servicios de internet pueden *dejarlos* sin fuente de ingresos. En esas circunstancias, es posible que surjan 'mercados negros' de conectividad en torno a fuentes de conectividad alternativas, que con frecuencia *benefician* a grupos armados o delictivos, alimentan la dinámica del conflicto y generan riesgos adicionales de protección para las personas afectadas por el conflicto armado que buscan fuentes de conectividad alternativas.

Si bien las consecuencias humanitarias que genera la falta de conectividad pueden ser considerables, es importante tener presente que la conectividad en sí misma también puede poner en riesgo a las personas. A veces, las autoridades, las partes beligerantes y otros grupos la utilizan para vigilar, perseguir e identificar como objetivo a determinadas personas, y las comunidades marginadas también pueden llegar a enfrentarse a más obstáculos y a exponerse a la discriminación a través de la conectividad. Además, en virtud del derecho de los derechos humanos, los Estados pueden restringir el acceso a las redes de comunicación cuando existen razones de seguridad legítimas y proporcionadas que lo justifiquen. Estas cuestiones plantean '*dilemas digitales*' para los actores humanitarios, quienes deben *analizar* las oportunidades y los riesgos que supone la conectividad para las personas afectadas por conflictos armados, de modo que '*no causen daños digitales*' en las actividades de promoción y asistencia que realizan. Pero el hecho de que las personas y las sociedades dependan cada vez más de la conectividad implica que el costo de las interrupciones nunca ha sido tan alto.

Interrupción de un facilitador esencial de la acción humanitaria

Las organizaciones humanitarias también dependen cada vez más de la conectividad para ofrecer una respuesta a la velocidad y la escala que se necesitan en situaciones de emergencia. La interrupción de los servicios de conectividad obstaculiza su capacidad de operar y prestar *asistencia*.

Con frecuencia, las organizaciones humanitarias recurren a la conectividad para identificar necesidades humanitarias, por ejemplo, cuando recopilan de forma remota información de los hospitales relativa al número de víctimas durante una emergencia o cuando se ponen en contacto con las poblaciones afectadas para llevar a cabo un seguimiento individual. También la utilizan para documentar posibles violaciones del derecho internacional de forma remota (incluso a través de inteligencia de fuentes abiertas [OSINT] y de *tecnologías remotas*) y para llevar a cabo intervenciones vitales en tiempo real. Asimismo, necesitan conectividad para su *coordinación* interna y para gestionar cadenas logísticas y de suministro. La seguridad también puede verse afectada: en una época en la que los trabajadores humanitarios *nunca* se han enfrentado a tantas amenazas contra su vida, la interrupción de la conectividad puede poner en peligro su capacidad de obtener garantías de seguridad esenciales para los equipos en el terreno o simplemente para llegar a las partes interesadas pertinentes en momentos de necesidad. Si bien existen tecnologías alternativas como la *conexión satelital*, en comparación, esas opciones resultan costosas, no siempre están permitidas por la legislación nacional y, en algunos casos, conllevan riesgos políticos y de vigilancia, con lo cual no siempre es fácil ampliar su uso.

Durante las interrupciones en la conectividad, los trabajadores humanitarios también pueden estar sujetos a una mayor vigilancia a fin de que no pasen por alto restricciones. Al mismo tiempo, pueden verse sometidos a otras presiones para que faciliten información sobre lo que ven en el terreno, con el fin de llenar el vacío de información sobre posibles violaciones del derecho internacional humanitario y el derecho internacional de los derechos humanos. Está en juego la capacidad de los trabajadores humanitarios para preservar tanto su independencia como la confidencialidad de la información sensible que necesitan para proteger a las personas. Sin embargo, mantener un enfoque basado en principios no es opcional, sino que se trata de un requisito funcional.

Construir un futuro mejor

En la XXXIV Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, los Estados y los componentes del Movimiento aprobaron por consenso una *resolución* para proteger mejor a la población civil ante el posible costo humano de las actividades relacionadas con las tecnologías de la información y las comunicaciones durante los conflictos armados. En ella se reconoce explícitamente la importancia de la conectividad para la protección de las personas civiles y la acción humanitaria basada en principios, y se insta a "proteger... la infraestructura técnica esencial para la disponibilidad general o la integridad de internet". Esta resolución es un logro importante si se tiene en cuenta el debate, a veces polarizado, que existe sobre estos temas y, lo que es más importante, establece una base concreta para que los Estados y otras partes interesadas debatan y busquen soluciones para mitigar las consecuencias humanitarias de la interrupción de la conectividad en el futuro.

Existen diferentes formas de contribuir a estructurar y orientar los esfuerzos jurídicos, políticos, de protección y operacionales para que las interrupciones de la conectividad no causen daño ni se cobren vidas humanas. La diplomacia humanitaria y la defensa de los principios humanitarios, así como el diálogo sobre protección con las partes beligerantes, deberían hacer hincapié en las consecuencias de las interrupciones de la conectividad e incluir llamamientos a un mayor respeto, en particular del derecho internacional humanitario y el derecho internacional de los derechos humanos. También es necesario centrar los esfuerzos en diseñar la infraestructura de conectividad de modo que facilite la distinción entre activos y datos digitales civiles, por un lado, y activos y datos militares, por el otro; y en buscar la manera de reforzar la solidez y resiliencia de los sistemas conectados, tanto desde el punto de vista técnico como *sociopolítico*. En cuanto a sus propias operaciones, las organizaciones humanitarias deberían idear formas de ofrecer soluciones humanitarias eficaces en entornos de conectividad baja o nula, así como reflexionar sobre los *riesgos, ventajas y matices* de proporcionar conectividad como ayuda. En forma paralela, las autoridades deberían analizar de qué modo podría preservarse la capacidad de los trabajadores humanitarios para utilizar la conectividad en operaciones de emergencia y destinadas a salvar vidas, concediéndoles los privilegios e inmunidades adecuados en materia de protección o conectividad.

Nunca hemos tenido tantos medios tecnológicos y sofisticados a nuestro alcance para garantizar nuestra capacidad de comunicación cuando están en juego la vida, la seguridad y la dignidad de las poblaciones afectadas. Los Estados, los grupos armados no estatales, el sector privado y otros actores que tienen el poder de provocar interrupciones en la conectividad deben analizar las consecuencias humanitarias de sus decisiones y tomar medidas para evitar que haya muertos, heridos y sufrimiento entre la población civil.

Referencias

[1] Este tipo de interrupciones suelen denominarse 'cortes de internet', término que popularizó la organización de defensa de los derechos digitales *Access Now* y lo definió como "interrupciones intencionales de internet o de las comunicaciones electrónicas, que las vuelven inaccesibles o efectivamente inutilizables para una población específica o dentro de un lugar concreto, generalmente con el fin de controlar el flujo de información".

Tags: civiles, Conflicto armado, conflicto armado, métodos modernos de guerra, Protección de la población civil

De la "guerra total" a la "defensa total": el trilema de la participación civil en los conflictos armados

19 mins read

Análisis / Comunicaciones / Nuevas tecnologías Ruben Stewart

Cuando los Estados adoptan estrategias de "defensa total" que movilizan a poblaciones enteras en la preparación de un conflicto armado, la línea divisoria …

Reanimar la protección específica para hospitales según el DIH

19 mins read

Análisis / Comunicaciones / Nuevas tecnologías

Supriya Rao & Alexander Breitegger

En los conflictos armados de hoy en día, crecen los ataques contra hospitales y su uso indebido con fines militares. Estas acciones socavan …