¿CÓMO EVITAR LA CENSURA EN TIEMPOS DE CONMOCIÓN SOCIAL?

En los últimos días el mundo ha sido testigo de las grandes manifestaciones en Colombia y la brutal represión que se ha desatado con el fin de apagar la protesta legítima de millones de ciudadanos. ¿Pero qué detonó el estallido social? Si bien la causa inmediata fue la oposición a la Reforma Tributaria presentada por el ejecutivo, es imperativo subrayar que la situación del pueblo colombiano ha estado atravesada desde hace mucho por gravísimas desigualdades que se han visto acrecentadas por la crisis sanitaria global en combinación con medidas de corte antipopular, como la reforma a la salud en tiempos de pandemia y la falta de cumplimiento con los ofrecimientos tras la firma del acuerdo de paz por parte del gobierno, que no han hecho más que acrecentar el descontento ciudadano y detonar el legítimo deseo de exigir un país mejor y más justo a la clase gobernante.

A lo largo y ancho de la región y a nivel global, la receta para controlar y apagar la protesta social es casi siempre la misma: el despliegue de la fuerza pública para el sometimiento de los manifestantes y la protección de bienes públicos y privados; pero además de ello, con el auge de las tecnologías de la información y la comunicación en la actualidad, la censura en entornos digitales es una tendencia peligrosa que cada vez gana más fuerza y se diversifica en dependencia de las circunstancias.

En el marco de las manifestaciones por el Paro Nacional en Colombia, existen numerosos reportes que dan cuenta de apagones de internet, como en el caso de Cali en donde el fenómeno ha sido atribuido a supuestas fallas en los cables subamarinos Arcos y Maya[1]. Llama la atención que sea precisamente Cali, uno de los lugares en donde se han reportado gran parte de los casos de abuso por parte de la fuerza pública en contra de los manifestantes y es de ahí, precisamente, de donde provenían los reportes ciudadanos y denuncias que no tardaron en viralizarse en el mundo entero.

Asimismo, existen numerosas denuncias que hacen referencia al bloqueo de transmisiones en vivo desde la primera línea por parte de determinados proveedores de redes sociales por supuestas infracciones a sus condiciones de uso[2], o incluso la desaparición de historias en plataformas como Instagram, aduciendo fallas a nivel mundial, aún cuando curiosamente, las historias desaparecidas tenían contenido relacionado al Paro Nacional en Colombia.[3]

En este punto es importante que nos preguntemos: ¿Cuál es el objetivo de la censura?

La respuesta puede ser bastante obvia, sin embargo es importante resaltar que la censura no se aplica de igual manera en todas las circunstancias y en todos los lugares, mas si

1 https://www.eltiempo.com/archivo/documento/MAM-2537421
2 https://heraldodemexico.com.mx/tendencias/2021/5/5/facebook-instagram-bloquean-transmisiones-en-vivo-desde-colombia-denuncian-usuarios-292588.html
3 https://www.eltiempo.com/tecnosfera/apps/instagram-esta-borrando-las-stories-sobre-el-paro-nacional-586471

tuviéramos que mencionar algunos de los objetivos de la censura, podemos citar los siguientes:

- Dado que existen numerosas denuncias relacionadas con uso desmedido de la fuerza, ejecuciones extrajudiciales, desapariciones forzadas, delitos sexuales y demás violaciones a los derechos humanos perpetradas por las fuerzas estatales, el objetivo de impedir que la información sea difundida, especialmente hacia el exterior, se vuelve imperante con el fin de evitar la judicialización y condena.
- Ante manifestaciones populares multitudinarias, por ningún motivo conviene permitir que las agrupaciones sociales y ciudadanos en general se organicen, por tanto urge reducir toda posibilidad de comunicación que pueda fortalecer a la resistencia, haciendo así, menos efectiva a la protesta.
- Impedir la fuga de información que visibilice los altos niveles de violencia y violaciones a derechos humanos no es únicamente algo que se haga hacia el exterior, sino que la censura de información sucede también al interior del territorio de la nación, pues ciudadanos que no conozcan lo que está sucediendo en las diferentes localidades de su país, probablemente no tendrán motivos para levantarse y sumarse a la protesta popular.
- Frente a los problemas, es natural que se presenten soluciones y el caso de la censura no es diferente, por lo cual, los bloqueos de información, apagones de internet o censura en redes sociales cumplen el firme objetivo de impedir que los ciudadanos accedan a herramientas o medidas que permitan superar o al menos mitigar de algún modo los efectos de la censura.

Pero, ¿qué es lo que nos dice la legislación internacional acerca del derecho a la protesta?

En el año 2019, la Comisión Interamericana de Derechos Humanos definió al derecho a la protesta como:

"[U]na forma de acción individual o colectiva dirigida a expresar ideas, visiones o valores de disenso, oposición, denuncia o reivindicación, a modo de ejemplos, pueden mencionarse la expresión de opiniones, visiones o perspectivas políticas, sociales o culturales; la vocalización de apoyo o crítica relativas a la denuncia de un problema público; la afirmación de la identidad o visibilización de la situación de discriminación y marginalización de un grupo."[4]

Dicha definición recoge en sí misma la relevancia de la protesta social dentro de los procesos democráticos de las naciones y, a su vez, las legislaciones locales de los distintos países del continente contemplan el legítimo derecho a manifestarse para sus ciudadanos; sin embargo, en muchas ocasiones este derecho puede ser limitado, por ejemplo, con el decreto de estados de excepción que limitan la libre movilidad de lxs ciudadanxs..

4CIDH (2019). *Protesta y Derechos Humanos: Estándares sobre los derechos involucrados en la protesta social y las obligaciones que deben guiar la respuesta estatal*, OEA/Ser.L/V/II CIDH/RELE/INF.22/19, Septiembre 2019. Disponible en:

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

Y es precisamente en este último caso cuando ciertas prácticas entran en una zona gris en la cual el Estado aprovecha la falta de normativa explícita y específica para censurar contenidos que considera controversiales y lesivos mediante distintos mecanismos.

Se puede decir que la censura en internet puede suceder principalmente en las siguientes formas:

- A través de "blocklists": En general, este tipo de bloqueos es una práctica integrada en los sistemas regulares de los proveedores de internet. En principio, los gobiernos se valen de este tipo de censura con fines positivos, como en el caso de la restricción de contenido considerado ilegal en el país; sin embargo, también puede ser utilizado con el fin de bloquear listas de sitios web o direcciones IP bajo pedido.
- Apagones de internet que consisten en la interrupción deliberada del servicio de internet en un área geográfica en particular. Puede darse mediante la exigencia de los gobiernos a los proveedores de internet o a través de intervención manual a la infraestructura física.
- Mediante interceptaciones de comunicaciones y tráfico de internet que, en lugar de buscar bloquear el flujo normal de la información, busca recopilar la mayor cantidad de datos acerca de los ciudadanos con diversos fines, como podrían ser el perfilamiento, criminalización y procesamiento de los individuos que ante la mirada de los gobiernos, resulten incómodos. Pese a que la mayoría del tráfico de internet en estos días se encuentra cifrado, los gobiernos podrían intentar forzar el retiro de dicha protección con el propósito de recopilar el contenido de la comunicación. Independientemente de esto, el gobierno recolectará los metadatos y así podrá determinar qué sitios web fueron accedidos y quiénes se comunicaron entre sí.

Una vez que hemos hablado de algunos de los objetivos de la censura estatal, sin duda vale la pena hacer lo propio en el caso de quienes recurren a medios digitales en momentos de gran conmoción social, como lo son las manifestaciones populares.

Cuando el Estado falla en su obligación de garantizar el derecho a la protesta social pacífica, es natural que se susciten excesos por parte de la fuerza pública en su afán de contener la movilización popular. Ya lo han vivido Haití, Ecuador, Chile, Brasil y ahora Colombia, entre otros a lo largo del último año con episodios de violencia extrema y violaciones sistemáticas a los derechos humanos que, de no ser por el registro multimedia y difusión inmediata que nos permiten las tecnologías actuales, pasarían inadvertidos. Cabe resaltar aquí que el caso colombiano genera gran preocupación por los niveles elevados de violencia conque las fuerzas del orden han reprimido a los manifestantes en comparación con otros países de la región.

Quienes luchan ven en el registro y difusión de las manifestaciones, una forma de rebasar fronteras y contar al mundo lo que está sucediendo. Asimismo, acciones de organización, apoyo y solidaridad se generan gracias a las redes. Pero quizás uno de los objetivos que cobra mayor relevancia en el ámbito de la protesta popular es el de recolectar evidencia que permita establecer responsabilidades cuando la vida de los manifestantes se ve vulnerada por los aparatos represivos del poder, tarea que normalmente debería ser realizada por entidades gubernamentales como la Defensoría del Pueblo.

Frente a la inminente censura impuesta por los gobiernos, es natural querer encontrar herramientas o mecanismos que permitan impedir que el normal flujo de información sea

intervenido, sin embargo, es importante considerar que no todas la recomendaciones que lleguen a nosotros deben ser aplicadas ciegamente, pues no todas las personas y no todos los lugares están sujetos a censuras de la misma naturaleza y, además de ello, es preciso entender que la aplicación de diversas herramientas y mecanismos para evitar la censura pueden traer consigo riesgos, entre los que podemos mencionar: el riesgo de identificación y ubicación, la interceptación del contenido que compartes para ser usado posteriormente en tu contra o incluso, la gente con la que te comunicas también puede ser identificada y perfilada.

Otro aspecto a ser tomado en cuenta es que las legislaciones de los diferentes países regulan de manera distinta el uso de ciertas tecnologías, como lo son el cifrado o las redes de anonimato, por tanto, si bien el uso de dichas tecnologías podría contribuir a superar la censura impuesta por el gobierno y proteger derechos fundamentales como lo son la privacidad y el anonimato, al mismo tiempo se estaría incurriendo en un delito por el sólo hecho de utilizarlas.

Además, existe evidencia de sobra que demuestra cómo los gobiernos muchas veces catalogan como ilegal el uso de ciertas tecnologías en dependencia del nivel de conmoción social y a partir de ahí deciden qué tipo de restricción que imponen sobre los ciudadanos.

Respecto a esto, cabe mencionar el criterio del desarrollador de software y experto en seguridad informática, Ola Bini, quien sostiene que: “No importa lo que diga la ley, el uso de este tipo de técnicas en ocasiones se puede utilizar para identificar a las personas y convertirlas en objetivos. Las diferentes técnicas traen consigo diferentes riesgos, pero ninguna es completamente segura, especialmente en un país que experimenta malestar generalizado de algún tipo. Conocer los derechos y las leyes es útil, pero es posible que aún así no estés protegido”.

Respecto a las diversas recomendaciones circulando en las redes respecto a tecnologías para evitar la censura, podemos referirnos a las siguientes:

- **VPN (Virtual Private Network/Redes Privadas Virtuales):** Hablando del contexto latinoamericano, más en concreto en el caso de Colombia, la mayoría de ciudadanos probablemente no tenga acceso a VPN propias, pero existirán casos en donde se pueda acceder a ellas a través de los empleadores/compañías medianas en donde esta tecnología es comúnmente utilizada para acceder a recursos internos. Sin embargo, se puede acceder a una VPN de manera doméstica o internacionalmente. Para el primer caso, imaginemos que una determinada localidad en Colombia se encuentra bajo condiciones de censura y la sede de la compañía para la cual trabajamos se encuentra en Bogotá en donde existen condiciones de censura diferentes, si tratamos de acceder a recursos o enviar información y esto no funciona, lo podemos hacer utilizando la VPN de nuestro empleador y así, todo el tráfico que normalmente hubiera salido de nuestro computador en la localidad mencionada inicialmente, ahora saldrá desde Bogotá.

  Ahora, las compañías internacionales también utilizan VPN. Para esto, imaginemos que trabajamos para una empresa radicada en Chicago con una VPN en esa misma ciudad. En este caso, también podríamos utilizar esta VPN y acceder a recursos y enviar información desde Chicago en lugar de Bogotá.

Cabe mencionar que podrían existir ciertas restricciones impuestas por las compañías respecto al tipo de búsqueda que se puede ser desde la VPN, por tanto ello implica que existe algún tipo de censura en la empresa. Por otro lado, si vamos a hacer algo potencialmente peligroso, esto podría ser atribuido a la compañía a través de su VPN, por tanto existe un riesgo implícito que es mejor evitar. Probablemente el mejor uso para una VPN en estos casos es para evitar la censura y la interceptación, pues la gran mayoría de VPN están completamente cifradas, haciendo que la intervención cercana a nuestras comunicaciones sea imposible y también, considerando que las condiciones de la censura cambian en función de dónde se encuentra radicada la VPN.

Existen proveedores de servicios como *Riseup* que ponen a disposición de activistas VPN, sin costo alguno. Esto no conlleva los mismos riesgos que existirían al utilizar la VPN de una compañía privada o tu empleador.

Finalmente, cabe destacar que las VPN muy probablemente no servirán en casos de apagones de internet, pues en estas circunstancias, todo el tráfico de internet se ve comprometido, incluso aquel que nos permitiría conectarnos a la VPN.

- **Proxies:** Son similares a las VPN en el sentido que a través de nuestro computador o teléfono podemos conectarnos a otro computador, de modo que todo el tráfico y conexiones que queramos hacer saldrán a través de este otro computador en lugar de nuestro dispositivo. Imaginemos que tenemos un proxy en Amsterdam e intentamos conectarnos a él desde Bogotá, todo el tráfico de internet saltará al proxy. Por ejemplo, si intentamos acceder a un sitio web censurado en Colombia, podemos conectarnos al proxy y empezar a navegar en el sitio pues la censura no afectará al computador en Amsterdam. Esto es posible cuando nos conectamos a un proxy internacional que existe en un país fuera de donde rige la restricción y en donde en general, no se aplica la censura a gran escala.

  Un proxy es algo que está más al alcance de individuos privados. Si bien existen compañías que proveen de libre acceso a proxies, usualmente estos son bastante lentos. Sin embargo, por una pequeña suma de dinero, se puede adquirir el acceso a proxies en todo el mundo que podrían ser configuradas tanto para nuestro computador como, para nuestro teléfono. Existen compañías proveedoras de proxies que aceptan pagos en criptomonedas, tales como Bitcoin por el servicio, haciendo posible que accedas a un proxy de manera completamente anónima. Dos de las mejores son *Mullvad* y *ProtonVPN*.

  Un proxy va a tener una conexión cifrada entre nuestro computador y el computador proxy como tal, lo que significa que no existe lugar para la interceptación. Del mismo modo que con las VPN, el objetivo principal de un proxy es evitar la censura y asimismo, en el caso de apagones de internet, la conexión con el proxy no será posible. En algunos casos, ciertos regímenes de censura van a bloquear la conexión con servicios reconocidos de proxies; sin embargo, existen suficientes proveedores de proxies y es poco posible que todas las conexiones con ellos sean censuradas. De la misma manera, en ocasiones estos proveedores también poseen una gran cantidad de servidores en distintas partes del mundo a los cuales podemos conectarnos. En muchas ocasiones, estas compañías internacionales de proxies

también sirven de protección frente a gobiernos que buscan determinar tu identidad.

Los proxies no experimentan los mismos riesgos que las VPN, pues en general los proveedores de proxies son compañías legalmente constituidas y por tanto gozan de ciertas protecciones.

Finalmente, muchas de estas compañías también proveen proxies especialmente dedicados a personas en situaciones de riesgo y conmoción social e incluso tienen servidores proxy que ni siquiera aparecen en listas públicas. Para poder acceder a ellos, por lo general basta con enviar un correo electrónico solicitando este servicio especial, haciendo de este modo mucho más difícil que la censura afecte estas conexiones proxy. Para el caso particular de Colombia, hay que mencionar que en ocasiones, las personas ofrecen computadores a manera de proxies sin ningún costo de manera solidaria. A menudo, es posible encontrar estos servicios haciendo una búsqueda de internet.

Cabe mencionar que los proxies presentan un problema y este es que todo tu tráfico va a fluir a través de un sólo punto y esto implica que quien administra el proxy podría interceptar dicho tráfico. En la coyuntura colombiana actual, quizás este no es un gran inconveniente; sin embargo, en un sentido general este es un riesgo que muchos encuentran inaceptable y para ello, la red Tor es una manera de evitarlo.

- **Tor (The Onion Router/ El Ruteador Cebolla):** Podemos considerar a la red Tor como un gran número de proxies que funcionan gracias a voluntarios alrededor del mundo pero, en lugar de dirigir tu tráfico únicamente por un sólo proxy, la red Tor utiliza 3 proxies diferentes y cifra el tráfico entre ellos de tal modo que ninguna de las personas que opera estos proxies puede tener acceso al contenido. Tor te ayuda a evitar la censura, así como también la interceptación de información.

  Sin embargo, la red Tor suele ser censurada en países que atraviesan momentos de conmoción social de distintos tipos; en estos casos, la censura no afecta únicamente a los servidores proxy, sino también al sitio del cual se quiere descargar el software. Hay que mencionar asimismo que existen soluciones a estos dos problemas. La primera solución son los denominados “puentes”, computadoras desconocidas que pueden ser configuradas en Tor para conectarse a través de ellas en lugar de la red Tor conocida, haciendo así más fácil evitar la censura. Supongamos en el caso particular de Colombia, que el gobierno no sabrá acerca de la existencia de dichos “puentes”. La segunda solución para el caso en que el sitio para descargar Tor esté bloqueado, es enviar un correo electrónico a la dirección gettor@torproject.org, diciendo, por ejemplo: “windows es” (sistema operativo/idioma) para recibir enlaces para descargar Tor desde sitios que no se encuentren bloqueados.

  Asimismo, Tor tiene la posibilidad de ocultar el tráfico de modo que este no se vea como tráfico de Tor haciendo más difícil que el gobierno pueda censurarlo.

  Siendo Tor una herramienta conocida, existe el riesgo de que el sólo hecho de usarla te convierta en un objetivo, pues según algunos gobiernos y sus aparatos represivos, el hacerlo lleva implícita la intención de cometer actividades ilegales, aun cuando aquello no sea cierto. Vale aclarar que no existe ningún riesgo legal al intentar

acceder sitios web a través de la red Tor, pues no existe modo de rastrear el tráfico de vuelta hacia ti, es decir, nadie puede saber quién está usando la red Tor y lo que se está haciendo con ella.

Del mismo modo que sucede con las VPN y los proxies, Tor no te protege en casos de apagones de internet, pues para poder acceder a la red anónima, necesariamente debes tener algún tipo de conexión de internet.

- **Redes Descentralizadas:** Cuando no tienes acceso a una conexión de internet, la situación se vuelve compleja, ya que naturalmente tendrás la necesidad de comunicarte con otras personas y acceder a información para organizarte. Es aquí en donde las redes descentralizadas cobran relevancia. La idea de este tipo de redes es que tú puedes configurar una red sin ningún tipo de intermediario, sin un proveedor de servicio de internet, sin entrar al internet para poder conectarte a otras personas. Para esto, tu teléfono o tu dispositivo electrónico puede utilizar su antena o radio dentro de sí para conectarse directamente con otras personas. Esto significa que puedes intercambiar mensajes directamente entre tus compañerxs y tú para poder comunicarse, suponiendo que estén lo suficientemente cerca.

  Existen distintas versiones de este tipo de protocolos. Por ejemplo, la aplicación *Briar* para teléfonos móviles puede servir para este fin. Asimismo, existe una red de enrutadores (routers) bastante común en Hamburgo en donde tienes una serie de ruteadores que, incluso sin estar conectados al internet, pueden reconocer y conectarse automáticamente a otros enrutadores cercanos generándose de esta manera, una red descentralizada, de modo que la gente conectada a esos ruteadores pueda comunicarse entre sí. Un dato interesante acerca de este tipo de redes es que no sólo resultan útiles para facilitar la comunicación entre individuos cuando no existe conexión a internet, sino que también en muchos casos, si alguien dentro de una red descentralizada tiene conexión a internet, las otras personas dentro de la misma red pueden utilizar esa conexión para enviar y recibir información y es precisamente esto lo que vuelve a esta tecnología tan poderosa, pues permite el flujo de la información dentro y fuera de una región que se encuentra bajo bloqueo, asumiendo que exista algún tipo de brecha en el mismo.

  Una red descentralizada es más util cuando tienes un apagón de intenet a gran escala, pues puede servir para evitar la censura pero, al ser una solución un tanto lenta, no necesariamente va a ser la más efectiva.

  La mayoría de estos protocolos están cifrados, por lo tanto te protegerán de la interceptación de información.

  En cuanto a los posibles riesgos de utilizar este tipo de tecnología, estos son considerablemente bajos, pues se trata de métodos aplicados de manera local, por lo que si alguien quiere identificarte/encontrarte, debería estar lo suficientemente cerca a ti y darse cuenta que estás usando este tipo de método y en muchos casos, eso puede ser ocultado.

- **Teléfonos Satelitales:** Cuando es complicado o prácticamente imposible acceder a internet por canales regulares, puede resultar útil recurrir a los teléfonos satelitales. Como lo indica su nombre, estos dispositivos se comunican con redes satelitales en

lugar de utilizar conexiones locales. Lastimosamente, se trata de equipos un tanto costosos, pero si tienes a alguien cercano a ti con acceso a uno de ellos, este se puede convertir en una herramienta bastante útil en circunstancias complicadas, pues, del mismo modo que harías con un teléfono regular, usualmente puedes utilizar una conexión de datos con el beneficio de que dicha conexión no irá a través de un proveedor de internet local, sino que irá a través del satélite y quien sea que esté a cargo de dicho satélite, por ello, si existe algún tipo de restricción de acceso al internet, dependerá enteramente de quien es el propietario de dicho satélite.

Hay que reconocer que este tipo de dispositivo, a más de costoso, es difícil de conseguir y además pueden ser lentos, pues usualmente el ancho de banda con el que funcionan no es muy grande, pero si tienes que enviar información fuera del lugar donde te encuentras, un teléfono satelital puede ayudar, considerando que, por lo general, la censura se aplica localmente, permitiéndote evadirla, lo mismo cuando existen apagones de internet. Especialmente si lo utilizas en combinación con las otras técnicas, como las redes descentralizadas, puede resultar beneficioso para muchas personas con el fin de enviar información hacia el exterior.

- **Conexión de módem a un número internacional:** En algunos casos, los apagones de internet afectarán únicamente a las conexiones de datos y no a las conexiones telefónicas. Si ese es el caso, puede ser posible utilizar una conexión via módem. En medio de situaciones de estallido social, algunas organizaciones de la sociedad civil en otros países suelen crear portales de internet conectados a números internacionales sin ningún costo, por lo que, si tienes un módem disponible (hoy por hoy, la mayoría de teléfonos móviles y sistemas operativos de computadores tienen implementada la funcionalidad de módem) y te es posible encontrar información acerca de este tipo de recursos, podrás acceder a internet a través de una de conexión de acceso telefónico. Este método fue utilizado con éxito en algunas de las revueltas en Egipto, donde existieron apagones de internet, así como también en Irán y Siria.

  Es importante mencionar que, habitualmente, este tipo de métodos no está disponible de manera pública y permanente, sino que suelen aparecer cuando existen situaciones de alta conmoción social y alguien decide montar el servicio en el exterior y lo difunde con personas que se encuentran en la zona de conflicto para su uso. De modo que difícilmente existirán “proveedores” que aparezcan en motores de búsqueda de forma abierta.

  Lo bueno de esta técnica es que no existen posibilidades de censura en el país de origen. Las únicas personas que podrían hacerlo son las personas que en principio establezcan la llamada telefónica con el número internacional. El inconveniente es que la conexión es bastante lenta, únicamente es posible la conexión de un dispositivo con un número internacional (salvo opciones más sofisticadas) y en ocasiones es posible que las conexiones telefónicas internacionales también hayan sido bloqueadas. Esta técnica puede ser usada para evitar la censura, pero es mucho más útil cuando existen apagones completos de internet. A esto hay que agregar que no existe un nivel de protección absoluto, pues si la conexión telefónica que estás usando es interceptada de algún modo, hay una posibilidad real de que quien sea que esté recopilando esa información, pueda almacenarla.

Las conexiones de acceso telefónico modernas utilizan un cierto tipo de cifrado, pero usualmente este no es muy fuerte y en muchos casos no garantiza protección real. Eso significa que quien esté interviniendo la conexión telefónica y recopilando datos, podrá reconstruir la información a partir de ello. Al utilizar una conexión telefónica de cierto tipo, ya sea esta fija o móvil, también existe una gran posibilidad de que esto pueda servir para identificarte en el acto. Por tanto, recomendamos considerar los riesgos asociados a este método.

- **Transmisiones en vivo:** Esta técnica en particular, en realidad no tiene el fin de evitar la censura o los apagones de internet, pero puede ser realmente útil al momento de documentar abusos de diferente tipo, además de asegurar que la comunidad internacional fije su atención en lo que está sucediendo en un lugar en particular. Para hacerlo, se requiere una cámara, usualmente de tu teléfono, conectada a una cuenta en alguna red social como Twitter, YouTube, Facebook, entre otros, que transmita directamente lo que está sucediendo, de modo que la visualización se da de manera casi inmediata.

  Esto puede ser muy útil al momento de proteger a las personas, pues la idea es que la policía y otras fuerzas del orden piensen dos veces antes de cometer algún acto indebido al conocer que están siendo observados, pero por otro lado, al hacerlo te pones potencialmente en riesgo, ya que este tipo de transmisión te hará muy fácil de ser identificado, tanto en el momento de la transmisión, como después de ella, por lo cual no se descartaría la posibilidad de ser arrestadx o incluso algo peor en situaciones altamente conflictivas; sin embargo, es importante tener conocimiento acerca de este tipo de herramienta sin ignorar las posibles consecuencias de su uso. En ocasiones, te puedes proteger mediante el uso de un proxy o Tor para canalizar estas transmisiones a través de algo más, reduciendo significativamente las posibilidades de ser identificado.

  Más concretamente, te podríamos recomendar:

a) Etiquetar un bot de Telegram que haga copia automática de la transmisión en otro servidor. Sin embargo, te recomendamos que no utilices Telegram para tus comunicaciones si estas son sensibles de algún modo, puesto que la aplicación contiene algunas vulnerabilidades en lo que respecta a seguridad y tanto tú como los tuyos podrían quedar expuestos.

b) Identificar plataformas alternativas de streaming en vivo, pues existen reportes de que las redes sociales asociadas a Facebook, pueden borrar las transmisiones en vivo.

- **OONI Probe:** Cuando queremos comprender qué tipo de interferencia se está dando en una red, en ocasiones es útil recopilar ese tipo de información para publicarla y centralizarla de algún modo después. Existen algunas herramientas que nos pueden ayudar a hacer esto, sin embargo, puede ser potencialmente peligroso utilizarlas si no estás seguro de lo que estás haciendo. El problema es que estas herramientas analizan tu conexión de internet en distintos modos, entre ellos, tratando de hacer ciertas cosas que a menudo están prohibidas. Desde luego, si lo estás haciendo en un país en donde esto no es permitido, estas acciones pueden de hecho convertirte en un objetivo.

Al utilizar una herramienta como OONI Probe, podrás saber qué tipo de censura está teniendo lugar en tu zona y la comunidad internacional podrá entender qué es lo que está sucediendo y documentarlo para el futuro, sin embargo, si no tienes el conocimiento técnico para comprender qué exactamente está pasando y no puedes determinar cómo puedes protegerte, no es recomendable utilizar este tipo de herramienta. Pero si en cambio, posees conocimiento técnico, el hacerlo puede resultar bastante útil para que la comunidad técnica pueda recolectar esa información y centralizarla en las bases de datos acerca de manipulación, censura y apagones de internet.

IDEAS FINALES

La mayoría de las veces, los apagones de internet no serán totales, pues es riesgoso desde un punto de vista económico, bloquear la conexión en todo un país. Podríamos comparar a un apagón de internet con una sierra eléctrica, mientras que la censura podría actuar como un escalpelo. En ocasiones necesitas una sierra eléctrica, pero en otros momentos es más conveniente usar el escalpelo.

La mayoría de veces, los gobiernos aplicarán los apagones de internet en las regiones de un país bajo mayor conflicto, pues es necesario controlar la situación con mayor efectividad; sin embargo, esto puede cambiar y los apagones podrían ser trasladados/extendidos a distintas regiones en dependencia de la gravedad del conflicto, de forma temporal o por tan sólo unos cuantos días, mientras que la censura en su forma habitual se valdrá de mecanismos persistentes que están ahí todo el tiempo, como en el caso de las “blocklists”.

En el caso de los apagones, estos suelen afectar con más frecuencia al acceso a internet de los consumidores, dejando ciertas partes del internet abiertas para distintos operadores. En el caso de Egipto, esto sucedió cuando la mayoría del internet había sido bloqueado, con excepción de ciertas conexiones relacionadas a los negocios y mercados de bolsas, por lo que, si entre tus compañerxs existe alguien con las habilidades técnicas para encontrar estas conexiones abiertas en medio del bloqueo, te será posible tener tráfico de internet hacia el exterior de tu región para que se sepa qué es lo que está sucediendo en tu zona.

En general, son los gobiernos quienes darán las órdenes para que sucedan los apagones o la censura, pero en ocasiones, quienes en realidad se encargan de que esto en efecto se dé, son los proveedores de internet o la infraestructura física en que estos convergen antes de conectarse al internet (Internet Exchange Point/Punto Neutro). En vista de que por lo general estas compañías son internacionales, vale la pena llamarlas por su nombre y condenarlas ante la comunidad internacional por lo inaceptable de sus acciones al seguir las órdenes de los gobiernos, impidiendo de este modo, el libre flujo de información en situaciones de conmoción social.

A manera de cierre podemos decir que todo método para mitigar la censura, trae consigo ciertos costos, por lo cual es importante que pensemos y consideremos el tipo de amenaza a la cual nos estamos enfrentando antes de decidir qué método o tecnología aplicar. Muchas veces es posible reforzar nuestra protección sin agregar más complejidad a cómo nos comunicamos.

Cabe resaltar que, incluso si no tienes conexión a internet, siempre es útil recolectar evidencia de lo que está sucediendo a tu alrededor, pues incluso si no puedes compartir esa información de forma inmediata, ¡quizás lo puedas hacer luego![5]

Recuerda que no existen medidas rápidas que protejan efectivamente tus comunicaciones. Si una herramienta promete protegerte de manera completa e inmediata, lo más probable es que esto no suceda y expongas tu seguridad y la de tus compañerxs en algún modo. La aplicación de toda tecnología o método requiere cierta preparación con el fin de poder minimizar al máximo los riesgos implícitos en su uso, además de los que la censura y el bloqueo traen consigo. Es natural querer protegerte cuanto antes en situaciones de conflicto intenso y fuerte represión gubernamental, pero es importante considerar que decisiones tomadas apresuradamente, pueden traer consecuencias negativas.

Por último, es vital que recordemos siempre que la seguridad operacional (OPSEC) no funciona de manera retroactiva, por lo cual es importante que seamos conscientes de los posibles riesgos que el uso de ciertas tecnologías traen consigo, sobretodo en situaciones de conflicto.

Este documento contiene mucha información, por lo que queremos compartir contigo enlaces que te puedan ayudar a aprender más y sobretodo entender cómo usar de forma segura las herramientas que te hemos propuesto. Algunos de los enlaces estarán en español, sin embargo, parte de la información sólo está disponible en inglés.

Para saber más acerca de la Red Tor y software asociado con ella, el mejor lugar para empezar es este: https://tb-manual.torproject.org/es/

Muchos de los siguientes links también hablan de Tor además de otras técnicas y herramientas como los proxies y las VPN, entre otros: https://securityinabox.org/es/guide/anonymity-and-circumvention/

Para una mirada un poco más técnica, el siguiente link contiene una guía que cubre material similar al mencionado arriba: https://ssd.eff.org/en/module/understanding-and-circumventing-network-censorship

Cuando hablamos de redes descentralizadas, en ocasiones conocidas como redes en malla/mesh networking, existen muchas herramientas que puedes utilizar. Briar y Bridgefy son un buen punto de inicio. Puedes encontrar más información sobre Briar aquí: https://briarproject.org/how-it-works/

https://www.cibertip.com/tutoriales/briar-la-aplicacion-de-mensajeria-movil-que-funciona-sin-internet-o-mediante-la-red-tor-comunicacion-libre-de-cualquier-vigilancia/

Para saber más acerca de Bridgefy, te recomendamos: https://bridgefy.me/ y https://dl.autonomia.digital/bridgefy/

5 https://twitter.com/TembloresOng/status/1390875676010598400?s=20

Además de los enlaces anteriores, también puedes visitar: https://www.elespanol.com/omicrono/software/20171003/aplicaciones-mensajeria-cifrada-segura-usadas/251476130_0.html

Sobre los teléfonos satelitales y herramientas relacionadas te recomendamos:
https://www.dezeen.com/2020/03/13/internet-shutdown-fallback-portal-device-technology/
https://www.yifanhsieh.com/fallback
https://www.starlink.com/ (proveedor principal de esta tecnología)

Cuando se trata de conexiones de acceso telefónico a través de líneas telefónicas internacionales, no hay tantos recursos disponibles. Lamentablemente, esta es principalmente una técnica desconocida, a pesar de que se utilizó con éxito en Egipto y otros lugares. El siguiente artículo describe algunos de estos eventos:

https://www.pcworld.com/article/218179/egyptians_find_new_routes_to_the_web.html

https://www.pcworld.com/article/218927/

dialup_connections_for_when_disaster_strikes.html

https://web.archive.org/web/20110208091758/http://manalaa.net/dialup

https://twitter.com/xs4all/status/1186195563018162177?lang=en

Si te encuentras fuera de un apagón de Internet, ya sea en otras partes del país o fuera de este, puedes ayudar a las personas en la zona de conflicto configurando un servidor que les ayude a eludir la situación de censura. Puedes encontrar una guía sobre cómo hacer esto con el sistema operativo Linux aquí:

https://www.howtoforge.com/linux_dialin_server

En el caso de la herramienta OONI Probe, puedes visitar este enlace que contiene una guía de uso: https://www.derechosdigitales.org/13931/manual-rapido-de-ooni-probe-para-monitorear-bloqueos-de-sitios-y-servicios-usando-telefonos-android/

Sin embargo, te recomendamos que te informes de los posibles riesgos que conlleva el uso de esta herramienta aquí: https://ooni.org/es/about/risks

Si quieres conocer más consejos para enfrentar los apagones de internet les recomendamos visitar los siguientes enlaces:

https://citizenevidence.org/2020/11/16/shutdown-toolkit/

https://www.accessnow.org/internet-shutdowns-and-elections-handbook/

https://es.witness.org/2020/02/intercambio-de-archivos-y-comunicacion-durante-un-apagon-de-internet/

https://es.witness.org/2020/02/configurar-un-telefono-para-documentar-cuando-no-haya-internet/

https://es.witness.org/recursos/video-como-evidencia/

https://cpj.org/es/2021/04/seguridad-digital-bloqueos-de-la-internet/

Por último, te invitamos a leer un par de artículos que hablan de experiencias en países que han enfrentado situaciones de censura y apagones de internet, aquí:

https://www.forbes.com/sites/johnkoetsier/2019/09/02/hong-kong-protestors-using-mesh-messaging-app-china-cant-block-usage-up-3685/?sh=a5d6ed4135a5

https://www.apc.org/es/news/disrupciones-de-internet-en-ecuador-como-ocurrieron-y-como-eludirlas