PISTOLAS contra CELULARES

Fundación Karisma

PISTOLAS contra CELULARES

Bogotá, Colombia
Septiembre de 2021

Autores:
Juan Pablo Parra
Carolina Botero

Revisiones:
Pilar Saenz
Andrés Velásquez
Juan Diego Castañeda
Joan López
Lucia Camacho
Diseño Editorial:
Hugo A. Vásquez

Ilustración:
Don Repollo

En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos. Más información sobre el tema en http://www.documentoaccesible.com/#que-es

Fundación Karisma

CONTENIDO

INTRODUCCIÓN

El 28 de abril de 2021, luego de que el presidente Iván Duque radicó ante el Congreso de la República el proyecto de ley de la Reforma Tributaria, se dio lugar a un movimiento masivo de protesta ciudadana en Colombia conocido como el paro nacional. Desde entonces y hasta el 15 de junio, de forma oficial, se convocaron marchas y actividades en distintas ciudades de todo el país.

En medio de este panorama de agitación social y democrática, las concentraciones y marchas fueron escenarios de enfrentamientos entre las personas manifestantes y la fuerza pública, incluso con personas armadas que apoyaban a la Policía. De forma simultánea, en algunas redes sociales como Facebook, Instagram, Twitter y Tik Tok, las personas comenzaron a publicar denuncias y vídeos sobre presuntas violaciones a los derechos humanos de quienes se manifestaban. Se viralizaron publicaciones donde se documentaron los excesos en el uso de la fuerza por parte de la fuerza pública contra las personas que se manifestaban o los ataques de la ciudadanía a la fuerza pública y a la infraestructura local.

Con el aumento de la intensidad de los enfrentamientos en las calles y las personas saliendo a marchar con sus celulares en las manos, como mecanismo de denuncia y defensa contra los abusos, también surgieron reportes sobre posibles actuaciones por parte de representantes del Estado que limitaban de forma desproporcionada derechos fundamentales que ejerce la ciudadanía a través de la tecnología, tales como: la libertad de expresión, de acceso a la información, de reunión y el derecho a la intimidad.

La falta de información clara sobre qué pasa con los derechos en el entorno digital en medio de la protesta, así como la ausencia de investigaciones de parte de las autoridades colombianas, y la proliferación de casos en los que desaparecían, se disminuía el alcance de publicaciones o se bloqueaban cuentas, generó un sentimiento de censura general por parte del Estado a la ciudadanía y cuestionamientos sobre el rol de las empresas privadas intermediarias de internet en lo sucedido. En este informe analizaremos la afectación que sufrió el entorno digital colombiano a partir de los casos de posibles vulneraciones a los derechos humanos ejercidos en espacios digitales por parte de la ciudadanía y que fueron recopilados por la Fundación Karisma durante el primer mes del paro, entre el 28 de abril y el 28 de mayo de 2021.

Algunos de los riesgos que aquí explicamos fueron informados, de forma conjunta con otras organizaciones de la sociedad civil, a la Comisión Interamerica de Derecho Humanos (CIDH) previo a su visita de trabajo a Colombia con la intención de que las considerara en su documento de recomendaciones al gobierno nacional[1]. Dicho escrito de observaciones y recomendaciones fue publicado la primera semana de julio e incluyó un capítulo dedicado al internet como espacio de protesta[2]. Allí la CIDH llamó la atención al Estado sobre temas como el ciberpatrullaje de la fuerza pública, las interrupciones al servicio de internet, las órdenes de bloqueo de direcciones IP e incluyeron recomendaciones para adecuar o limitar dichas actividades al marco interamericano[3].

Para mayor claridad, este informe se organiza así: primero, se abordarán los casos en los que se acusa al Estado de haber interferido internet mediante bloqueos o presuntos cortes; en seguida, se explicarán los riesgos para la ciudadanía que generan las campañas de criminalización de la protesta digital y los señalamientos de noticias falsas llevadas a cabo desde el Ministerio de Defensa; en un tercer momento, se tratará el uso de tecnologías para el control de la protesta social y las requisas a celulares; ya terminando, haremos unos breves comentarios sobre el papel que desempeñaron las empresas privadas intermediarias del servicio de internet durante el paro y; finalmente, se presentarán algunas conclusiones y recomendaciones.

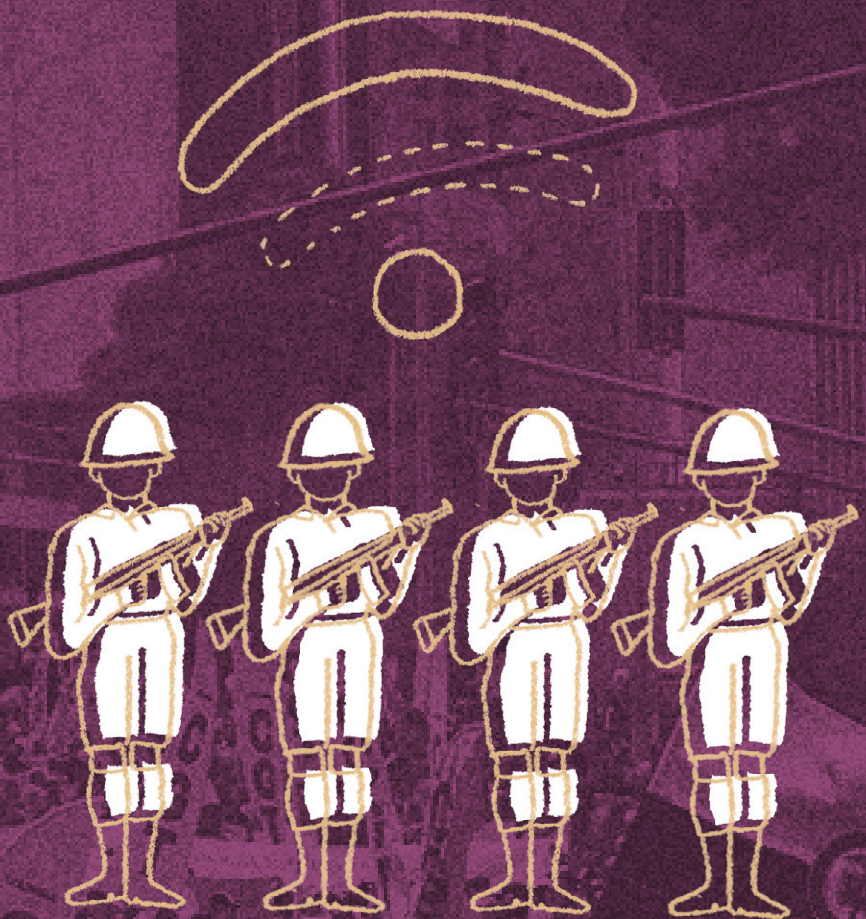
---

1 Fundación Karisma. Pedimos incorporar y analizar las violencias digitales en la protesta durante su visita. Disponible en: https://web.karisma.org.co/una-peticion-para-incorporar-y-analizar-las-violencias-digitales-en-la-protesta/

2 Fundación Karisma cuenta oficial Twitter. HIlo del 7 de julio de 2021: https://twitter.com/Karisma/status/1412839454595760130

3 CIDH. CIDH culmina visita de trabajo a Colombia y presenta sus observaciones y recomendaciones. Disponible en: https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/167.asp

UNO.
EL ESTADO LE METE MANO A INTERNET: CORTES Y BLOQUEOS SELECTIVOS DURANTE EL PARO NACIONAL



Uno de los principales temores de la ciudadanía respecto de los derechos digitales durante el paro nacional, era la posibilidad de que el Estado interfiriera internet para limitar los mensajes de protesta o como mecanismo para impedir que se informe sobre los presuntos abusos de la fuerza pública en las calles. Este temor a la censura, se hizo patente con la avalancha de publicaciones en redes sociales que denunciaban cortes a internet durante el paro. Pero el problema va más allá, pues, normativamente, varias entidades estatales tienen facultades para intervenir internet, sin que esté claro si han usado dichos poderes o quién ejerce control al respecto.

En este capítulo abordaremos los casos en que el Estado le metió mano a internet durante el paro nacional. En concreto, nos referiremos a los presuntos cortes a internet en Cali, a las facultades discrecionales de los organismos de seguridad para usar dispositivos que bloquean señales y a las órdenes dadas por la Superintendencia de Industria y Comercio de bloquear algunas direcciones IP específicas. En suma, analizaremos cómo el Estado colombiano tiene capacidad tecnológica instalada para restringir el acceso a internet o bloquear contenidos en línea y sí el marco jurídico aplicable establece un diseño institucional que ofrezca garantías de derechos humanos y/o evite abusos por parte de las autoridades.

1.1 Aclaraciones iniciales. Cortes a internet un tema complejo

Antes de abordar los casos en concreto es necesario hacer algunas aclaraciones. En primer lugar, en Colombia no se ha presentado un apagón de internet, ni antes ni durante el paro nacional. Es decir, no se ha dado un corte en la prestación del servicio por orden del Estado, como son el caso de Birmania[4] y el de Venezuela en las elecciones de 2013[5], o por lo menos no hay prueba de ello. Sin embargo, desde que comenzó el paro, los reportes ciudadanos de cortes de internet han sido una constante.

Estas denuncias no son un tema menor. Durante las manifestaciones de 2021 se hizo habitual que la ciudadanía acudiera de forma masiva a internet para expresar su descontento y para documentar en vivo, o retransmitiendo, lo que sucedía en las calles, en especial las irregularidades vinculadas con la fuerza pública. Este uso activo de internet y de las redes sociales como medio para ejercer derechos del calado de la libertad de expresión, de acceso a la información y de participación política, hacen que sean especialmente preocupante los reportes ciudadanos de posibles bloqueos de internet. Las interferencias estatales a la prestación del servicio de internet atentan contra el núcleo fundamental de los citados derechos, ya que impide de plano a la ciudadanía expresarse, participar o informarse sobre el contexto nacional y obstruye la denuncia o documentación de violaciones a los derechos humanos que se produjeron durante el paro nacional.

La importancia del internet para ejercer y disfrutar los derechos humanos, nos lleva a la segunda aclaración: Colombia, como Estado parte de la Convención Americana de Derechos Humanos, está obligada a proteger internet y tiene prohibido bloquearla o apagarla. Al respecto, los relatores de libertad de expresión de diferentes organismos internacionales de derechos humanos, entre ellos la Organización de los Estados Americanos (OEA) y la Organización de las Naciones Unidas (ONU), señalaron en 2011 que: "la interrupción del acceso a Internet, o a parte de este, aplicada a poblaciones enteras o a determinados segmentos del

4 RTVE.es. La ONU denuncia los cortes de Internet en Birmania, ya que socavan "los principios democráticos fundamentales" Disponible en: https://www.rtve.es/noticias/20210215/onu-denuncia-cortes-internet-birmania-socavan-principios-democraticos-fundamentales/2075803.shtml

5 Instituto prensa y sociedad Venezuela. Gobierno nacional interrumpió temporalmente servicio de internet y bloqueó acceso desde el exterior a página web del Consejo Nacional Electoral. Disponible en: https://ipysvenezuela.org/alerta/gobierno-nacional-interrumpio-temporalmente-servicio-de-internet-y-bloqueo-acceso-desde-el-exterior-a-pagina-web-del-consejo-nacional-electoral/

público (cancelación de internet) no puede estar justificada en ningún caso, ni siquiera por razones de orden público o seguridad nacional"[6].

Y en ese mismo sentido, se pronunció la Comisión Interamericana de Derechos Humanos (CIDH) al referirse a los cortes de internet en época de protesta y señalar que "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"[7].

El tercer factor que debe tenerse en cuenta en el caso colombiano, es la débil infraestructura con la que cuenta el país para prestar servicios públicos como internet o electricidad. Según datos de septiembre de 2020, Colombia es uno de los países que tiene peor acceso a la web[8], contando con solo 24,3 millones de accesos a internet reportados para más de 50 millones de personas. Además, existen distintos niveles de acceso y calidad del servicio, según la región, siendo las zonas excluidas las que tienen servicios más deficientes[9]. Algo similar sucede con el servicio de luz, ya que al menos 1710 poblados en Colombia aún se alumbran con velas[10]. Y si bien este panorama no es tan drástico en la ciudades, sí es cierto que hay poblaciones y zonas marginadas donde el acceso es de menor calidad.

Siendo así, cuando hablamos de cortes o interrupciones de internet no solo debemos tener en cuenta las posibles acciones ilegales por parte del Estado, sino que la falta de acceso a la conectividad de calidad, eventos masivos que sobrecarguen la red (como marchas o conciertos), daños físicos a la infraestructura, procesos de mantenimiento de la red de prestación del servicio, cortes de luz y problemas a nivel de plataforma o aplicación, son factores que explican de forma plausible las fallas en la prestación del servicio. Es por esto que establecer el origen y naturaleza de las interferencias es central para garantizar los derechos de las personas. El contexto socio político o las complejidades técnicas no justifican las interrupciones al servicio de internet, ni eximen al Estado de obligar a investigar y aclarar lo sucedido.

1.2 Interrupciones y cortes selectivos e ilegales de internet. Cali, una noche sin internet y con la fuerza pública en las calles

El primer caso sonado y relevante sobre cortes de internet en el país fue el de Cali durante la tarde y noche del día 4 de mayo de 2021 (aproximadamente desde las 4:30 pm) hasta la madrugada del día siguiente. Problemas con el servicio de internet que confirmó Netblocks, organización inglesa dedicada al monitoreo de

6 La Declaración Conjunta sobre Libertad de Expresión e Internet, 2011, puede consultarse en https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849

7 Relatoría Especial para la Libertad de Expresión. Comisión Interamericana de Derechos Humanos. Protesta y Derechos Humanos.Estándares sobre los derechos involucrados en la protesta social y las obligaciones que deben guiar la respuesta estatal. Párrafo 298. Disponible en:http://www.oas.org/es/cidh/expresion/publicaciones/ProtestayDerechosHumanos.pdf

8 El Tiempo. Colombia, uno de los países con más dificultades de acceso a internet. Disponible en ; https://www.eltiempo.com/tecnosfera/novedades-tecnologia/internet-calidad-de-conexion-en-colombia-con-mas-dificultades-en-el-mundo-529850#:~:text=Seg%C3%BAn%20el%20Ministerio%20de%20las,y%20no%20tienen%20este%20beneficio y MinTIC. ¿Cómo está el país en conexión de internet? Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/MinTIC-en-los-medios/151654:Como-esta-el-pais-en-conexiones-de-internet

9 MinTIC. Boletín trimestral del sector TIC - Cifras cuarto trimestre de 2020. Disponible en: https://colombiatic.mintic.gov.co/679/w3-article-172261.html

10 El Tiempo. Los 1710 poblados que aún se alumbran con velas en el país. Disponible en: https://www.eltiempo.com/colombia/otras-ciudades/los-poblados-que-aun-no-tienen-energia-electrica-en-colombia-324980

internet, en su comunicado *Internet disrupted in Colombia amid anti-government protests*[11] del 5 de mayo. Esta denuncia tuvo especial relevancia nacional debido a la fuerte presencia militar que copó la ciudad y a la crudeza de los enfrentamientos que allí se presentaron. La noche del 4 de mayo, la violencia policial presuntamente dejó como saldo tres jóvenes asesinados con arma de fuego en el distrito de Siloé, lugar donde también se denunciaron cortes de internet.

Desde el inicio de las protestas, el 28 de abril hasta la fecha de las denuncias del corte de internet, Cali había sido el epicentro del paro nacional. En la ciudad, la tercera más importante del país, se presentaron fuertes enfrentamientos entre la ciudadanía y la policía, con denuncias en redes y prensa nacional sobre muertos e incendios en la ciudad, especialmente en los distritos de Agua Blanca y Siloé[12]. Ante dicho panorama, se decretó toque de queda a partir del 28 de abril hasta el 2 de mayo[13] y se anunció la llegada de más militares a la ciudad[14].

Fue en este contexto de alta presencia militar y de violencia, que se conocieron las denuncias de cortes a internet en Cali entre el 4 y 5 de mayo. Los primeros reportes de problemas se dieron a través de Twitter donde se indicaba que los Live, transmisiones en vivo de las marchas y los enfrentamientos, se caían, que los planes de datos de las personas no funcionaban de forma correcta y que era muy difícil conectarse a redes sociales[15], [16].

Algunas de las denuncias ciudadanas reportaban que también había cortes de energía eléctrica en Siloé. Además, algunos testigos señalan que los cortes o bloqueos de internet impedían de cualquier forma subir contenido a redes o incluso acceder. "Digamos que ahorita se ha calmado porque ya hay una mirada nacional e internacional, pero cuando apenas empezó, se daba que se perdiera la red total. Siloé estuvo un día apagado cinco horas, cinco horas en que no entraba ni salía nada. Osea yo estaba por walkie talkie con la gente de derechos humanos y no sabíamos si estaban vivos o muertos... sencillamente no había señal... Yo vi la motorizada con un equipo grande con una antena, yo no tengo foto... Mucho de lo que compartí fue atemporal porque allí no había señal", narra al respecto, Jahfrann, fotógrafo freelance colombiano en un testimonio inédito recogido por la Fundación para la Libertad de Prensa (FLIP).

---

11 Network. Internet disrupted in Colombia amid anti-government protests. Disponible en: https://netblocks.org/reports/internet-disrupted-in-colombia-amid-anti-government-protests-YAEvMvB3

12 El Tiempo. A siete sube sufra de muertos en el paro en Cali: https://www.eltiempo.com/colombia/cali/cali-tuvo-una-noche-de-terror-tras-orden-de-militarizacion-de-duque-592136

13 Infobae.Ministerio de Defensa confirmó la militarización en Cali: llegan 450 soldados. Disponible en: https://www.infobae.com/america/colombia/2021/04/28/ministerio-de-defensa-confirmo-la-militarizacion-en-cali-llegan-450-soldados/

14 Gobernación del Valle del Cauca. Consejo extraordinario de seguridad confirma la llegada de más personal del Esmad y el Ejército al departamento. Disponible en: https://www.valledelcauca.gov.co/publicaciones/70630/consejo-extraordinario-de-seguridad-confirma-la-llegada-de-mas-personal-del-esmad-y-el-ejercito-al-departamento/ y El Tiempo. Paro Nacional Cali: Toque de queda. Disponible en: https://www.eltiempo.com/colombia/cali/paro-nacional-cali-toque-de-queda-y-militarizacion-por-desordenes-584340

15 Blue Radio. ¿Qué pasó con el internet en Cali durante las protestas del pasado martes?. Disponible en: https://www.bluradio.com/blu360/pacifico/que-paso-con-el-internet-en-cali-durante-las-protestas-del-pasado-martes

16 Denuncias en Twitter sobre la noche del 4 y la madrugada del 5 de mayo: https://twitter.com/DefenderLiberta/status/1392601992292405251?s=20, https://twitter.com/julioclondono/status/1389941025775439876?s=20, https://twitter.com/Mariaisa1990/status/1389841875830546434?s=20 , https://twitter.com/chef_alv/status/1389856559874912257?s=20, https://twitter.com/MarceHolguinh/status/1389912481401868291?s=20 https://twitter.com/MULATACARAMELO1/status/1389826205294202880?s=20 https://twitter.com/juanmiguel94/status/1390498845839212544?s=20 https://twitter.com/juansitx/status/1389826124843266048?s=20 https://twitter.com/cranvodk/status/1389810050370318337?s=20 https://twitter.com/diegop4z/status/1390066216866357248?s=20 https://twitter.com/male_juri/status/1389814647868506113?s=20 https://twitter.com/JENNJGP/status/1389941927106260996?s=20

Este tipo de problemas por presuntos cortes a las telecomunicaciones también lo experimentaron miembros de Red Alterna Popayán, medio de comunicación alternativo que cubrió el paro. En una entrevista inédita realizada por la FLIP, señalaron que: "Aquí en el campamento no había señal, ni radio. Por ejemplo, unos compañeros estaban transmitiendo y nos tocó grabar, porque no funcionaba, [las transmisiones en vivo] se caían muy fácilmente. De lo que yo he solventado, hemos podido por medio de VPN. Porque al inicio era un ataque más que nada, dirigido a las direcciones de conexión. Pero ya cuando llega el ministro Molano a acompañar, no había señal, no forma total de conectar a VPN. Principalmente, cuando las confrontaciones se ponen más fuertes es cuando ¡fuf! desaparece la conexión".

El revuelo por el posible corte del servicio se materializó cuando el 5 de mayo, Netblocks afirmó que había problemas de acceso a internet y manifestó que era el segundo incidente durante el paro nacional. Según los datos, publicados por el observatorio inglés se habrían presentado dos caídas que disminuyeron la conectividad hasta en un 25% en Cali.

El informe de Netblocks no permite saber el origen o naturaleza de las interrupciones que reporta[17]y debe ser tomado como un dato más para informarnos sobre posibles interferencias a internet. Sin embargo, respecto de interrupciones a internet en el caso de Cali, además de que el informe coincidió con un importante ruido en redes sociales sobre posibles interrupciones a internet en sectores de Cali y la empresa prestadora del servicio sobre la cual Netblocks reportó las fallas, Colombia Telecomunicaciones S.A., más conocida como Movistar, también señaló que tuvo problemas de conexión en la red fija de internet durante la madrugada del 5 mayo en el distrito de Aguablanca. Indicó que esto se debió al hurto de un cable de fibra óptica y a problemas para reconectar al servicio debido a la situación de orden público. Movistar no se refirió a las fallas en el servicio en el sector de Siloé ni a los problemas con los dispositivos móviles que se reportaron en Twitter. Por su parte, Emcali, la otra empresa mencionada en el informe de Netblocks sobre interrupciones en el servicio como referente de comparación con Movistar, señaló que había prestado el servicio con normalidad y que no se había realizado ningún tipo de interrupción voluntaria del servicio[18], tal como lo había dicho en su momento el informe de NetBlocks.

Al respecto, en entrevista con el periódico El Espectador, Sergio Martínez, director de la Comisión de Regulación de Comunicaciones (CRC) -máxima autoridad en temas de internet en Colombia- señaló que el único reporte que habían recibido el 4 de mayo era por daños a la infraestructura. Y agregó que, "en ningún momento vamos a avalar ni a disponer ni indicar que se bloquee o se cierre internet [...] por parte de la CRC, nunca vamos a expedir un mandato de este tipo, porque eso atenta contra la libertad y la democracia en Colombia"[19].

Por su lado, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) se limitó a hacer un informe con lo dicho por las empresas, pero señalando sin pruebas, que el daño se produjo no por un robo,

17 Existen cuestionamientos sobre la metodología y datos de los informes que hace Netblocks, ya que en distintos casos sus reportes sobre caídas o cortes de internet han sido refutados y considerados poco fiables. Este problema se ha visto agravado por la negativas de Netblocks a ser más transparente con la información y metodología que maneja. Este problema ha descrito en artículos como ***How the internet censorship world turned on NetBlocks*** en Wired (Disponible en: https://www.wired.co.uk/article/netblocks-internet-shutdow). En todo caso, los cuestionamientos a Netblocks ponen de manifiesto que la falta de información fiable sobre los cortes a internet es un problema en sí mismo.

18 Emcali. Reportamos normalidad en el servicio de telefonía fija, internet, teléfono móvil en toda la ciudad. Disponible en: https://twitter.com/search?lang=es&q=(from%3AEMCALIoficial)%20until%3A2021-05-06%20since%3A2021-05-04&src=typed_query

19 El Espectador. ¿Por qué se cayó internet en algunas partes de Cali durante el 4 de mayo?. Disponible en: https://www.elespectador.com/tecnologia/por-que-se-cayo-internet-en-algunas-partes-de-cali-durante-el-4-de-mayo/

sino por “actos vandálicos” que no se podían reparar por culpa de las manifestaciones. Declaraciones que implican dejar de lado el lenguaje neutro con que se habían pronunciado las empresas privadas sobre los hechos y pasar a señalar de forma velada a los manifestantes.

A la fecha, aún no se sabe con certeza qué pasó en Cali entre el 4 y el 5 de mayo. Las explicaciones del Estado sobre los cortes de internet en Cali son insuficientes, por no decir nulas. Y las declaraciones de los prestadores del servicio, aunque bienintencionadas, tampoco permiten establecer qué sucedió. Por ejemplo, si bien el reporte de Netblocks no permite determinar en qué zonas de Cali se presentaron las interferencias al servicio de internet, por las denuncias en redes y medios está claro que el epicentro fue Siloé, afectando de forma especial la conexión de teléfonos móviles. Siendo así, la respuesta de Movistar es razonable para comprender el problema detectado en el informe de Netblocks en relación con la ciudad de Cali, pero resulta insuficiente para explicar los problemas con acceso a internet desde líneas fijas y móviles que se presentaron en Siloé.

Además, no debe olvidarse que tanto en Cali, como en Barranquilla, en el municipio de Caldas (Antioquia) y en el Portal de las Américas en Bogotá, también se reportaron cortes de internet y se habló de cortes de energía eléctrica en simultáneo cuando las manifestaciones se tornaron violentas por enfrentamientos con la policía. Tal y como sucede con internet, las fallas de la energía podrían explicarse por problemas de infraestructura. Pero lo cierto es que no hay información que sustente la versión sobre problemas de infraestructura localizados en lugares de protesta, como tampoco hay pruebas de cortes intencionados como se han dado, por ejemplo, en Venezuela[20]. Esta falta de información, fruto de la opacidad estatal y la poca transparencia de los privados involucrados, marca una tendencia respecto de las posibles vulneraciones a los derechos en el entorno digital durante las manifestaciones. Asunto sobre el cual, desde ya, llamamos la atención.

Contrario a lo que sucede en Colombia, la disponibilidad de información respecto a las interrupciones de internet o energía debería ser tal que permita el escrutinio público sobre todos los aspectos de conectividad implicados. Así sucedió, por ejemplo, en Washington en junio de 2020 en medio de las protestas contra el presidente Donald Trump. En ese caso, gracias a la gran cantidad de información disponible sobre lo sucedido, las denuncias sobre posibles interrupciones de internet fueron desmentidas por los periodistas de la agencia Reuters que lograron reconstruir lo sucedido durante las protestas[21].

En todo caso, conforme lo explicamos en el acápite anterior, corresponde al Estado colombiano, fruto de sus obligaciones internacionales de protección de los derechos humanos en el entorno digital, realizar las investigaciones para determinar causas y responsables de los cortes de internet ocurridos en Cali. Pero no ha sido así, el Estado se ha rehusado a dar respuesta o siquiera a buscarlas, en parte debido a que en su diseño institucional, como lo explicaremos más adelante. Este fenómeno político e institucional ha dejado en el ambiente una sensación de censura y dudas sobre si la fuerza pública, que estaba presente en las zonas donde se reportaron problemas de acceso a internet, está usando dispositivos que tiene en su poder para bloquear la señal[22].

---

20 Derechos Digitales. Políticas Públicas de Acceso a Internet en Venezuela. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/CPI_venezuela.pdf

21 Reuters. Fact check: Washington, D.C. did not have a city-wide blackout at 1 a.m. on June 1, 2020. Disponible en: https://www.reuters.com/article/uk-factcheck-dc-blackout-protests/factcheckwashington-dcdid-not-have-a-city-wide-blackoutat-1-amon-june-1-2020-idUSKBN2383OK

22 El País. La interrupción de internet durante las protestas enardece a los manifestantes en Colombia. Disponible en: https://elpais.com/internacional/2021-05-06/la-interrupcion-de-internet-durante-las-protestas-agita-a-los-manifestantes-en-colombia.html

1.3 Censura a discreción. Los inhibidores de señal de la fuerza pública

Uno de los factores que genera más dudas sobre lo que pasó en Cali entre el 4 y el 5 de mayo, es la fuerte presencia de militares y policías en la ciudad y su posible interferencia en la prestación del servicio. Debe señalarse para empezar, que no hay pruebas de que el ejército o la policía hayan utilizado dispositivos para interrumpir la señal durante el paro nacional. Sin embargo, es una realidad que los organismos de seguridad tienen y utilizan de forma habitual dichos dispositivos para bloquear señal. Ejemplo de ello son los mecanismos de bloqueo de telecomunicaciones que son usados en los cárceles[23]. O los seis "inhibidores de frecuencias" comprados por la Dirección de Investigación Criminal e Interpol (DIJIN) en 2016, a la empresa Robotec Colombia S.A.S, y catalogados como equipo militar y de inteligencia[24].

Además, la fuerza pública está avalada normativamente para hacer uso de dispositivos que bloquean las señales, y lo más preocupante, para hacerlo sin que exista un control sobre sus acciones. Dicha facultad fue entregada mediante la Resolución 2774 de 2013[25] del MinTIC. Norma en la que se autoriza a la fuerza pública a adquirir y usar inhibidores, bloqueadores y amplificadores de señales radioeléctricas por "razones de seguridad e interés general", siendo los únicos requisitos justificar de forma interna el uso del inhibidor y aportar estudios técnicos sobre el mismo.

La situación se volvió aún más preocupante en 2018 cuando el MinTIC cambió su regulación original mediante la Resolución 1823[26] y estableció que hay "autorizaciones especiales" que facultan a "los organismos de seguridad del Estado" a instalar inhibidores de señal en sitios abiertos en casos "relacionados con la seguridad pública", sin necesidad de una autorización del MinTIC ni control judicial.

Hay varias cuestiones que preocupan de esta facultad discrecional y sin contrapeso de la fuerza pública para usar inhibidores y bloqueadores de señal. En primer lugar, porque se trata del uso de tecnologías que impiden el acceso a internet, lo cual implica una restricción desproporcionada a derechos como la libertad de expresión e información no consagrada en una ley y que no supera el test de legalidad, necesidad y proporcionalidad de la Convención Americana. Como lo ha señalado la Relatoría para la Libertad de Expresión de la CIDH, no basta con hacer menciones abstractas a seguridad nacional para restringir derechos[27].

En segundo lugar, porque tal como lo apunta la Resolución 1823 de 2018 los permisos especiales para usar tecnología que bloqueen señales o internet están exentos de mecanismos de supervisión, a pesar de que debido al alcance de la autorización, ésta solo la debió haber entregado mediante autoridad judicial y de que el resto de las facultades reguladas por la resolución requieren permiso previo del MinTIC. Finalmente, la justificación genérica de "seguridad nacional", que reiteramos ha sido calificada previamente de insuficiente por la CIDH, aumenta la

23 Caracol Radio. Por demandas y multas apagamos bloqueadores de señal: Inpec. Disponible en: https://caracol.com.co/radio/2019/09/12/judicial/1568304853_201434.html y W Radio. Extorsiones carcelarias: ¿Están de adorno los bloqueadores de señal de celulares?. Disponible en: https://www.wradio.com.co/noticias/actualidad/extorsiones-carcelarias-estan-de-adorno-los-bloqueadores-de-senal-de-celulares/20210212/nota/4109297.aspx

24 Policía Nacional, Ministerio de Defensa Nacional. Contrato de compraventa PN DIJIN No. 03-2-1005018. Aprobado el 5 de julio de 2016.

25 MinTIC. Resolución 2774 de 2013 . Disponible en : https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_2774_2013.htm

26 MinTIC. Resolución 1823 de 2018 . Disponible enhttps://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_1823_2018.htm

27 Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. Párrafo 157. Disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

opacidad, pues dificulta acceder a información que confirme el uso de estos dispositivos, probablemente al consultar el Ministerio de Defensa o la fuerza pública se negarían a entregar la información con esta excusa.

También preocupa que no haya ninguna entidad estatal técnica e independiente del ejecutivo que ejerza control en caso de interferencia con internet. La CRC, entidad creada en 2019, para ejercer como regulador convergente, no cuenta con la capacidad para proteger a la ciudadanía de la intromisión a su derecho de acceso a las comunicaciones electrónicas, pues no cuenta con facultades de vigilancia y sanción en temas de Internet, funciones que se encuentran en cabeza del MinTIC. Por diseño legal, debería ser la CRC, el organismo que cuenta con el conocimiento y las capacidades técnicas para procesar datos e investigar a los prestadores del servicio de internet, e incluso a las actuaciones de otras entidades del Estado, pero no es así. Además, la CRC también debería proteger e informar a las personas usuarias de los servicios de telecomunicaciones sobre el origen y naturaleza de los cortes de internet, así como sancionar a los responsables, pero, de nuevo, en la práctica no tiene ninguna de estas facultades.

Por otro lado, la Agencia Nacional del Espectro (ANE), el órgano técnico que apoya al MinTIC en sus funciones de vigilancia y control del espectro electromagnético, es entidad llamada a investigar las interferencias con las señales de celulares, asunto bajo su control, pero no lo ha hecho y, de hacerlo, su adscripción al MinTIC no ofrece la confianza e independencia suficiente para vigilar al gobierno del que hace parte.

Siendo así, el actual diseño legal ha dejado en manos del MinTIC, entidad que es parte del poder ejecutivo, la vigilancia y sanción del sector, y no solamente de la definición de la política pública. De esta forma, el gobierno colombiano termina vigilando algo sobre lo que él debe ser vigilado. Y su labor, en efecto, se ha limitado a dar partes de tranquilidad respecto a la prestación del servicio de internet por las empresas privadas, usando un lenguaje que descalifica a los manifestantes, a pesar de la persistencia de denuncias en redes sociales que muestran otro tipo de amenazas. Vale la pena indicar que en situaciones similares los reguladores en Tailandia[28] o Estados Unidos[29] han adelantado investigaciones, pues tienen facultades autónomas y son los encargados de proteger los derechos de quienes usan los servicios de telecomunicaciones.

La falta de una institucionalidad que garantice el derecho al acceso a internet y que investigue las intromisiones a tal derecho, sumado a las dudas que existen sobre el uso que la fuerza pública da a sus facultades para inhibir las señales y a su presencia reiterada en zonas donde se han presentado bloqueos e interrupciones, deja en el aire una sensación de desprotección y falta de garantías para los derechos humanos en entornos digitales en el marco del paro nacional. Ante esta situación, muchas organizaciones civiles le han pedido al Estado que cumpla sus obligaciones internacionales de investigar, sancionar y garantizar la no repetición de violaciones a los derechos humanos, como lo es un bloqueo a internet[30]. Así como que se creen mecanismos de información periódica, técnica e independiente que permita el escrutinio público sobre la salud de la infraestructura en Colombia, tal como lo recomendó la CIDH en su documento de Observaciones y Recomendaciones. Pero hasta el momento han sido ignoradas.

---

28 Khaosod English. Cop admits signal jammers were deployed at protest. Disponible en: https://www.khaosodenglish.com/news/crimecourtscalamity/2020/08/24/cop-admits-signal-jammers-were-deployed-at-protest/

29 CBSN. FCC Investigates BART Cell Service Shutdown. Disponible en: https://sanfrancisco.cbslocal.com/2011/08/16/fcc-investigates-bart-cell-service-shutdown/ y Wetmachine. Are Police Jamming Cell Phones At Standing Rock Protest? The FCC Should Investigate. Disponible en: https://wetmachine.com/tales-of-the-sausage-factory/are-police-jamming-cell-phones-at-standing-rock-protest-the-fcc-should-investigate/

30 Comité Derechos Humanos ONU.Observación general núm. 37 (2020), relativa al derecho de reunión pacífica (artículo 21)*. Disponible en: https://www.hchr.org.co/files/observacion-general-37.pdf

1.4 Neutralidad de la red en peligro. Una internet desequilibrada.

El Estado colombiano ha reconocido el Principio de neutralidad de la red[31] a través de la ley[32] y en sus regulaciones internas[33]. Según este principio, que es una de las bases de internet tal cual la conocemos hoy en día, "[e]l tratamiento de los datos y el tráfico de Internet no debe ser objeto de ningún tipo de discriminación en función de factores como dispositivos, contenido, autor, origen y/o destino del material, servicio o aplicación"[34]. Y según las interpretaciones de la CIDH[35] y de la Corte Constitucional[36], los Estados parte de la Convención Americana están obligados a proteger la neutralidad de la red, pues la idea básica de la misma se vincula de forma directa con los derechos a la libertad de expresión y de acceso a la información, pilares de la sociedades democráticas.

Siendo así, en Colombia no solo las empresas que prestan el servicio, también el Estado está obligado a no usar su poder para discriminar, restringir, bloquear o interferir "en la transmisión del tráfico de Internet, a menos que sea estrictamente necesario y proporcional para preservar la integridad y seguridad de la red; para prevenir la transmisión de contenidos no deseados por expresa solicitud –libre y no incentivada– del usuario; y para gestionar temporal y excepcionalmente la congestión de la red"[37]. Para todos estos casos se aplican los parámetros interamericanos sobre libertad de expresión y acceso a la información, siendo la excepción a la regla, lo regulado en la Ley 1336 de 2009, según la cual el MinTIC puede bloquear páginas con contenido relacionado con el abuso sexual a menores (la mal llamada pornografía infantil) o, de forma más reciente, para evitar las apuestas ilegales en línea.

Según la CIDH, el "bloqueo o suspensión obligatoria de sitios web enteros o generalizados, plataformas, conductos, direcciones IP, extensiones de nombres de dominio, puertos, protocolos de red o cualquier tipo de aplicación, así como medidas encaminadas a eliminar enlaces (links), datos y sitios web del servidor en los que están alojados", constituyen una restricción que sólo es admisible para discursos abiertamente ilícitos y no resguardados por el derecho a la libertad de expresión conforme con el artículo 13 de la Convención Americana[38].

Bajo este marco normativo, el Estado colombiano encaró el Paro Nacional. El 4 de mayo de 2021, Anonymous, presuntamente, publicó nombre, número de documento de identidad, correo electrónico de algunos integran-

31 Fundación Karisma. ¿Qué es la neutralidad de la red? Disponible en: https://web.karisma.org.co/que-es-la-neutralidad-de-la-red/
32 Ley 1450 de 2011, artículo 56.
33 Comisión de Regulación de Comunicaciones, artículo 3 de la Resolución 3502 de 2011: "Por la cual se establecen las condiciones relativas a la neutralidad en Internet, en cumplimiento de lo establecido en el artículo 56 de la Ley 1450 de 2011". Disponible en internet desde: https://www.crcom.gov.co/resoluciones/00003502.pdf
34 Relator Especial de las Naciones Unidas (ONU) sobre la Promoción y Protección del derecho a la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión, y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP). 1 de junio de 2011. Declaración conjunta sobre libertad de expresión e Internet. Punto 5 (a).
35 Relatoría para la Libertad de Expresión CIDH. Libertad de expresión e internet. Párrafo 25. Disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf
36 Corte Constitucional. Sentencia T-179 de 2019. Disponible en: https://www.corteconstitucional.gov.co/relatoria/2019/T-179-19.htm y Sentencia SU-420 de 2019. Disponible en: https://www.corteconstitucional.gov.co/relatoria/2019/SU420-19.htm
37 Relatoría para la Libertad de Expresión CIDH. Libertad de expresión e internet. Párrafo 30. Disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf
38 Relatoría Especial para la Libertad de Expresión. Comisión Interamericana de Derechos Humanos. Protesta y Derechos Humanos. Párrafo 84. Disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

tes de la fuerza pública y otros funcionarios del gobierno, luego de que en la madrugada del mismo día atacaran la página oficial del ejército como respuesta a los asesinatos que se habían presentado en el marco de las protestas y en las que supuestamente estarían involucrados militares y policías[39].

Para contrarrestar la acción de Anonymous, el Viceministro de Conectividad del MinTIC remitió el 21 de mayo a los proveedores de internet en Colombia una orden de bloquear dos URL específicas, en aplicación de una resolución de la Superintendencia de Industria y Comercio (SIC)[40]. El comunicado mediante el cual MinTIC notificada la decisión no incluía copia de la resolución de la SIC.

Se puede discutir la legitimidad de la decisión, pero por el contexto de la misma es innegable que fue desproporcionada y pudo haber algunas irregularidades. Para empezar, la resolución de la SIC no es pública, lo que impide calificar la legalidad, proporcionalidad y necesidad del acto administrativo[41]. Para el momento de los hechos, la última decisión publicada en la página de la entidad era de abril de 2021 y no corresponde a la orden de bloqueo[42]. De otra parte, según fue informado a Karisma, la resolución que contiene la orden no fue oportunamente allegada a las empresas proveedoras de internet cuando les fue puesta en conocimiento la misma a través de la comunicación del Viceministro de las TIC. Es decir, ni las empresas proveedoras podían evaluar la legalidad, necesidad y proporcionalidad de la medida o si la misma se había emitido según lo exige la ley. Tampoco se les permitió defenderse de forma eficiente respecto a las mismas.

Hablamos entonces de una decisión que limita derechos fundamentales con carácter reservado, lo que contraría el ordenamiento jurídico y vulnera derechos fundamentales como el de defensa, debido proceso y acceso a la información. Sin importar si la SIC actuó en uso de sus facultades administrativas o judiciales, debía haber aplicado el principio de publicidad o de contradicción, según el caso.

El segundo problema, es que partiendo de lo que se conoce de la resolución[43] y suponiendo que la razón para "hacer seguimiento de la medida" sea la del conocimiento técnico del MinTIC, parece que el Viceministro de Conectividad, quien firmó la comunicación entregada a los proveedores de internet, no sabe cómo funciona la web. Es imposible cumplir con la orden de bloquear una URL específica dentro del dominio archive.org o ghostbin.co sin bloquear por completo esos sitios web. Es decir que ni la SIC ni MinTIC tuvieron en cuenta que esa orden bloquearía todo los contenidos de los sitios web, sin importar si lo que se alojaba en las dos páginas web estaba relacionado con el contenido de la resolución o no. Esto es más grave aún teniendo en cuenta que archive.org aloja además contenido material probatorio en medio de protestas sociales.

La directora de la Fundación Karisma, Carolina Botero, lo explicó así: "Cuando entramos a una página en internet o cuando una aplicación intenta conectarse con sus servidores que usen el protocolo HTTPS, los proveedores de internet solo pueden saber a qué dominio o IP (por ejemplo archive.org) nos estamos conectando, de

39 Publimetro. Anonymous publica números de tarjetas de crédito de altos mandos militares colombianos. Disponible en: https://www.publimetro.co/co/noticias/2021/05/04/anonymous-publica-numeros-de-tarjetas-de-credito-de-altos-mandos-militares-colombianos.html

40 Fundación Karisma. Trino del 21 de mayo de 2021: https://twitter.com/Karisma/status/1395849533586825225/photo/1

41 Carta de Karisma, El veinte, La FLIP e ISUR a la Comisión Interamericana. Pedimos incorporar y analizar las violencias digitales en la protesta durante su visita. Disponible en: https://web.karisma.org.co/wp-content/uploads/2021/06/Carta_visita_CIDH.pdf

42 El Espectador. La peligrosa y torpe orden de bloquear páginas web. Disponible en: https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/la-peligrosa-y-torpe-orden-de-bloquear-paginas-web/

43 Fundación Karisma. Trino del 21 de mayo de 2021: https://twitter.com/Karisma/status/1395849533586825225/photo/1

ahí en adelante la conexión está cifrada, la empresa no puede ver qué recurso o ruta dentro del servidor está siendo accedida. Por esto una orden de bloquear una URL específica tendría que dirigirse no al proveedor de Internet sino a quien administre la página en cuestión (por ejemplo archive.org). Si la empresa proveedora de internet intenta cumplir con la orden, lo que hará será bloquear el sitio completo y por tanto impedirá el acceso a todos los recursos del mismo"[44]

El tercer problema, es que la orden, que es claramente desproporcionada pues bloqueaba otros contenidos no relacionados con la resolución de la SIC, fue ejecutada por algunas de las empresas intermediarias sin tener en cuenta el impacto en los derechos humanos de las personas usuarias de sus servicios. Ese parece ser el caso de Emcali y Avantel, respecto de los cuales hay reportes de varias personas que aseguran que al usar sus servicios no pudieron ingresar a los sitios de archive.org y a ghostbin.co, problemas que fueron confirmados por el Observatorio Abierto de Interferencias en Redes (OONI, por su siglas en inglés), al respecto, recomendamos leer la columna en El Espectador, *La peligrosa y torpe orden de bloquear páginas web d*onde se explica el tema a detalle. Vale la pena destacar que esto no parece haber sucedido con el resto de los proveedores, lo que podría indicar que el problema no fue mayor gracias a que algunas de las empresas intermediarias no acataron una orden expedida por la SIC que era desproporcionadamente restrictiva con los derechos fundamentales de la ciudadanía.

Ahora bien, volviendo a revisar esta actuación desde la óptica de la neutralidad, es claro que esta norma protege es a los contenidos legítimos. Es decir, no se puede hablar de violación a la neutralidad si se bloquea material abusivo contra niños, niñas y adolescentes, tampoco si se actúa para evitar la circulación de contenido que viola las normas de protección de datos, por ejemplo. Sin embargo, cuando la orden de la autoridad es ilegal o no se ajusta a los estándares -porque es desproporcionada, por ejemplo-, entonces ahí sí hay una relación entre esos bloqueos y la neutralidad. La mala implementación tiene el efecto de impedir acceder a contenidos legítimos, eso pasa si se bloquea toda una página intentando evitar que las personas accedan a una determinada url.

Finalmente, vale la pena destacar que, la propia SIC, después de recibir una carta de algunas de las empresas intermediarias de internet en la que le explicaban por qué no era viable técnicamente cumplir su orden y que la misma ponía en riesgo derechos fundamentales, decidió modificar su decisión de bloquear las url específicas, cambiando como destinatario de la orden de bloqueo a las empresas intermediarias por los administradores de los dominios archive.org y a ghostbin.co[45]. Además, no debe olvidarse que la CIDH en su documento de observaciones y recomendaciones tras la visita de trabajo a Colombia reafirmó que bloquear contenidos o servicios es el último recurso que, precisamente, no se justifica sino en casos extremos (como la protección de menores por explotación sexual), por tanto, como cualquier restricción al ejercicio de la libertad de expresión, esta debe ser consagrada legalmente, ser necesaria y proporcional.

44 El Espectador. La peligrosa y torpe orden de bloquear páginas web. Disponible en:https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/la-peligrosa-y-torpe-orden-de-bloquear-paginas-web/

45 Superintendencia de Industria y Comercio. Resolución Número 37070 de 2021. Disponible en: https://www.sic.gov.co/sites/default/files/documentos/062021/Resolucion37070del17deJunioDe2021_PorLaCualSeModificaElResuelvDeLaResolucion29323del14DeMayoDe2021.pdf

DOS, ESTÁN CONMIGO O CONTRA MÍ. LA NARRATIVA ESTATAL QUE CRIMINALIZA LA PROTESTA DIGITAL

La criminalización de la protesta social ha sido una constante en Colombia durante las últimas décadas[46]. No obstante, con la irrupción de las tecnologías de las telecomunicaciones, surgió la protesta digital y el panorama cambió. Los movimientos políticos y sociales, así como las organizaciones de defensa de la sociedad civil, tuvieron a su alcance una herramienta con el poder de comunicar directamente sus contenidos y de hacerlos virales. Ante esta nueva expresión de participación política digital, el Estado colombiano ha seguido con su respuesta de manual, es decir, estigmatizar, criminalizar y perseguir.

Internet es un espacio que propicia e impulsa el ejercicio de la protesta. Ya sea mediante cadenas de correos, peticiones en línea, manifestaciones o campañas en redes sociales, la red permite ejercer de forma plena y democrática la libertad de expresión e información, el derecho a asociarse y a participar en la vida política. Es por esta razón que el Estado debe garantizar no solo el acceso a internet de la ciudadanía, sino condiciones que no amedrentan, estigmaticen o violenten a las personas que protestan en la web[47]. Obligación que parece no haber cumplido el gobierno colombiano durante el paro nacional, tal como lo explicamos a continuación.

2.1 De qué hablamos cuando hablamos de ciberpatrullaje

Cuando hablamos de ciberpatrullaje parece que nos referimos a muchas cosas. A ciencia cierta, no se sabe en qué consiste el patrullaje digital que la fuerza pública ha desarrollado activamente durante el paro nacional, lo que ya implica un problema. Así que para entender este tema, antes de abordar lo sucedido durante el paro nacional, haremos algunas precisiones semánticas sobre qué es o en qué parece consistir el ciberpatrullaje en Colombia.

En 2015 con la expedición de la Resolución 5839 de la Policía Nacional[48], el ciberpatrullaje hace su aparición dentro del ordenamiento jurídico. Dicha norma habilitó al Centro Cibernético Policial a "realizar ciberpatrullajes 24/7 en la web" con el propósito de identificar amenazas contra la "ciberseguridad ciudadana", con origen nacional o internacional. Así como a "desarrollar la capacidad de identificación y detección de factores comunes en los incidentes de su conocimiento"[49]. Sin embargo, la resolución no especifica de forma clara en qué consiste el ciberpatrullaje, sino que directamente habilita a la policía para hacerlo sin establecer procedimientos, herramientas permitidas o prohibidas, ni límites. Vale la pena precisar que una resolución no tiene el rango de una ley estatutaria y, por lo tanto, no cumple con el requisito de legalidad del artículo 13.2 de la Convención Americana, según el cual toda limitación a derechos como la libertad de expresión, asociación e información debe estar expresa de forma clara en una norma de rango legal, que haya sido resultado de un debate democrático.

Ante la ausencia de una definición normativa, hay que buscar otras fuentes que permitan entender qué entienden los organismos de seguridad colombianos por ciberpatrullaje. El *Informe del Sector Defensa. Garantías a la manifestación pacífica y control de acciones violentas, período 28 de abril al 4 de junio de 2021*[50] del Ministerio de Defensa (MinDefensa) da algunas luces sobre lo que puede ser el ciberpatrullaje, y lo hace en al menos tres dimensiones: investigar y prevenir amenazas cibernéticas, desinformación y perfilamiento.

---

46 Revista 070. La criminalización de la protesta en Colombia es histórica. Disponible en: https://cerosetenta.uniandes.edu.co/la-criminalizacion-de-la-protesta-social-en-colombia-es-historica1/#:~:text=La%20Corte%20Suprema%20de%20Justicia,frente%20a%20la%20protesta%20social.

47 Relatoría Especial para la Libertad de Expresión. Comisión Interamericana de Derechos Humanos. Protesta y Derechos Humanos. Disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

48 Policía Nacional. Resolución 5829 de 2015. Disponible en: https://www.policia.gov.co/file/32305/download?token=OA0OIAOJ

49 Policía Nacional. Resolución 5829 de 2015. Artículo 15, numeral 12.

50 MinDefensa. Informe del Sector Defensa. Garantías a la manifestación pacífica y control de acciones violentas, período 28 de abril al 4 de junio de 2021. Disponible en: https://www.mindefensa.gov.co/irj/go/km/docs/pccshrcontent/Recursos%20MDN/Plantillas%20Documentos/Ministerio/CentroDocumentos/Generales/Recursos/INFORME_DEFENSA_GarantiasManifestacion.pdf

2.1.1. Patrullar la web para investigar y prevenir amenazas cibernéticas

En línea con ejemplos internacionales, como es el caso de España[51], en Colombia parece que se adelantan, bajo el nombre de ciberpatrullaje, actividades de investigación judicial sobre la posible comisión, o para la prevención, de cibercrímenes o delitos cometidos en o a través de internet.

El informe ya mencionado de MinDefensa indica que gracias al ciberpatrullaje se detectaron "104 eventos cibernéticos, así; 41% (43 eventos), corresponde a defacements (modificaciones de código web), 32% (33 eventos), corresponde a los ataques de filtración de información, 20% (21 eventos) de denegación de servicios, 7% vulneración sitios web (7 eventos)"[52]. Es decir, que de acuerdo con el informe, el ciberpatrullaje en Colombia implica pesquisas e indagaciones judiciales sobre delitos que se cometen a través de internet, así como el bloqueo de sitios web en los que presuntamente se llevan a cabo estos delitos. Por ejemplo, en el último reporte de MinDefensa sobre el paro nacional, publicado el 2 de julio, se señala que durante las actividades de ciberpatrullaje se han registrado: 2.295.194 Direcciones IP con comportamientos maliciosos, 147.281 alertas preventivas generales, 1986 campañas maliciosas y 4 dominios identificados en campañas maliciosas[53].

Sin embargo, MinDefensa ha hecho pública muy poca información sobre sus actividades de monitoreo en internet en el marco de actividades de lucha contra el cibercrimen. Por ejemplo, no se indica cuáles sitios web han sido catalogados como maliciosos, qué tipo de ataques se han registrado, contra quién, qué acciones se tomaron contra las direcciones IP, qué pasa con las alertas que generan o con los dominios que identifican, cómo se relacionan con la protesta o qué significa "campaña maliciosa".

Si bien es importante que la Policía tenga la capacidad de proteger a las personas de ser víctimas de ciberdelitos, las herramientas que usen deben estar reguladas por un marco legal proporcional y razonable que los faculte para ello. Dentro de una democracia ningún poder debe ser absoluto o arbitrario, sino que debe contar con controles y contrapesos adecuados, y esto se aplica igual dentro y fuera de la web. La forma como la policía colombiana actúa en estos casos no es clara ni transparente, lo que impide el escrutinio público y por tanto no se construye confianza en la autoridad, elemento central de una política de ciberseguridad.

Sabemos muy poco sobre la forma como se adelantó esta dimensión del cibertaprullaje durante el paro, o si se sigue haciendo, pero, si de una alerta por amenaza cibernética el resultado es un bloqueo de un nombre de dominio o de una URL, debemos tener garantías para que esto se haga en debida forma como lo mencionamos en el aparte sobre neutralidad de la red.

2.1.2. Patrullar la web para combatir la desinformación

Tal como se infiere de los *Balances generales del paro nacional* que fueron publicados durante los meses de mayo y junio en la cuenta oficial en Twitter del MinDefensa[54], otra forma de entender o posible dimensión del

51 RTVE España. ¿Qué es el ciberpatrullaje? Disponible en: https://www.rtve.es/play/audios/cooperacion-publica-en-el-mundo-fiapp/cooperacion-publica-mundo-fiiapp-ciberpatrullaje-01-07-20/5614376/

52 MinDefensa. Informe del Sector Defensa. Garantías a la manifestación pacífica y control de acciones violentas, período 28 de abril al 4 de junio de 2021. Disponible en: https://www.mindefensa.gov.co/irj/go/km/docs/pccshrcontent/Recursos%20MDN/Plantillas%20Documentos/Ministerio/CentroDocumentos/Generales/Recursos/INFORME_DEFENSA_GarantiasManifestacion.pdf

53 MinDefensa. Trino del 2 de julio: https://twitter.com/mindefensa/status/1410958233058037761

54 MinDefensa cuenta oficial Twitter. Publicación del 2 de julio de 2021. Disponible en: https://twitter.com/mindefensa/status/1410958233058037761

ciberpatrullaje es como el monitoreo de páginas, perfiles y redes sociales con el fin de rastrear noticias falsas. Como también ha sucedido en Argentina.[55]

El antecedente colombiano inmediato del ciberpatrullaje para identificar contenido en línea que presuntamente generaba desinformación, lo realizó la policía en 2020. En el marco de la pandemia del Covid-19, la policía creó un reporte periódico de las noticias falsas detectadas por el Comando de Atención Inmediata Virtual[56]. Actividad que en su momento, fue identificada por la CIDH como un riesgo a las libertades fundamentales de la ciudadanía, pues "podría retrotraer a la región a una lógica de criminalizar expresiones sobre funcionarios o asuntos de interés público y establecer una herramienta con un fuerte efecto inhibitorio de la difusión de ideas, críticas e información"[57].

A pesar de lo dicho por la CIDH, el ciberpatrullaje entendido como rastreo de supuestas "noticias falsas" parece haber hecho carrera en la fuerza pública. Así lo deja claro el *Informe del Sector Defensa* ya mencionado. En dicho documento se señala que durante el paro nacional se llevaron a cabo, solo hasta el 9 de junio, 21.675 horas de ciberpatrullaje, en las cuales "se identificaron campañas de desinformación con el fin de generar contenido de caos y odio hacia las instituciones del Estado. Se han identificado y validado 154 noticias falsas de las cuales 91 están orientadas a desdibujar con hechos que no corresponden a la verdad y que han afectado la imagen de la Policía Nacional"[58].

La policía está dedicando un porcentaje considerable de recursos y tiempo a rastrear y etiquetar publicaciones en redes sociales como falsas, en una auto atribución, sin sustento legal, de la facultad para actuar como "policía de la verdad". Esto denota una percepción generalizada de culpabilidad de la ciudadanía y un desconocimiento y estigmatización del disenso político y de las denuncias de violaciones a derechos humanos. Además, contraría los estándares interamericanos de derechos humanos, pues la actitud del gobierno desincentiva la denuncia y genera autocensura.

2.1.3. Patrullar la web para perfilar actividades y personas sospechosas

En Colombia, existen precedentes nefastos e impunes de interceptaciones y perfilamientos realizados por la fuerza pública, como son los casos de las chuzadas del DAS[59] y las carpetas del ejército a inicios de 2020[60]. En este último caso, el ejército colombiano recolectó de forma masiva e indiscriminada, a través de herramientas informáticas, información sobre diferentes personas que consideraban peligrosas. Una actividad a todas luces violatoria de los derechos humanos.

De nuevo, el *Informe del Sector Defensa*, muestra que el ciberpatrullaje también sirvió para controlar la protesta en el mundo físico. En lo que entendemos como una tercera forma o dimensión del ciberpatrullaje. El informe habla de que se realizaron 3.420 alertas preventivas anticipando actos de vandalismo, que analizaron 3.723 vi-

---

55 https://observatoriolegislativocele.com/ciberpatrullaje-o-inteligencia/

56 Índice coronavirus y derechos digitales. Ciberpatrullaje de la Policía Nacional para identificar desinformación. Disponible en: https://cv19.karisma.org.co/docs/CiberpatrullajeDesinformacion/ y Policía Nacional. Reporte de noticias falsas detectadas por CAI Virtual. Disponible en: https://www.policia.gov.co/reporte-fakenews

57 CIDH y su RELE expresan preocupación por las restricciones a la libertad de expresión y el acceso a la información en la respuesta de Estados a la pandemia del COVID-19. Disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1173&lID=2

58 Ibidem.

59 Revista Semana. Así fueron las Chuzadas del DAS a la Corte Suprema de Justicia. Disponible en: https://www.semana.com/nacion/articulo/asi-fue-la-conspiracion/121785-3/

60 Revista Semana. Las carpeta Secretas. Disponible en: https://especiales.semana.com/espionaje-desde-el-ejercito-nacional-las-carpetas-secretas-investigacion/index.html

deos para identificar e individualizar responsables y que gracias a esto se abrieron 9 procesos de investigación. Estas cifras confirman que el monitoreo de la red es amplio y que incluye acciones de "inteligencia de fuentes abiertas" que lleva a la individualización de personas, es decir, hay una vigilancia activa de las comunicaciones de las personas para criminalizarlas. ¿Cómo operan en estos casos las garantías de derechos humanos? la información que hay pública no provee datos sobre esto. Otro aspecto del ciberpatrullaje del que sabemos poco y que preocupa teniendo en cuenta los antecedentes de chuzadas y perfilamientos en Colombia[61].

Prueba de ello, es el "sistema de ciberinteligencia basado en inteligencia artificial" que la policía intentó adquirir en 2020 y finalmente adquirió en julio de 2021[62] con el fin de realizar monitorear sitios web, redes sociales, TOR, I2p, Freenet y sistemas de mensajería instantánea como Telegram[63]. A pesar de que el proceso de contratación fue declarado desierto en dos ocasiones, es muy diciente que la Policía adquiera un sistema automatizado que le permita realizar perfilamientos a partir de las publicaciones de redes sociales de la ciudadanía. La amplitud de los criterios de "peligroso" que pueda usar la Policía, pone en riesgo la libertad de expresión e información de la ciudadanía, pues es posible que se den retaliaciones a partir de los perfilamientos por el comportamiento en redes o que la ciudadanía se autocensure, deje de participar en debates o de seguir grupos o famosos para evitar ser señalado.

Ahora bien, respecto del ciberpatrullaje, la CIDH en su documento de *Observaciones y Recomendaciones. Visita de trabajo en Colombia* no habló de la primera dimensión, se ocupó esencialmente de la segunda dimensión, y algo dijo de la tercera. La Comisión señaló que el ciberpatrullaje estaba orientado a "un monitoreo proactivo de contenidos presuntamente falsos sobre el desarrollo de las protestas, desprestigio de la imagen de las fuerzas públicas, así como la instigación al odio público"[64] y que dicho actuar del Estado colombiano, donde las fuerzas de seguridad se abrogan la facultad de chequeo y catalogación como verdadero o falso de denuncias en internet, resulta "especialmente preocupante" ya que se categoriza información sobre las actuaciones de las mismas fuerzas de seguridad. Y que tal comportamiento promueve la censura.

2.2 La ofensiva de la fuerza pública por copar la narrativa en el espacio público digital

Durante el paro nacional, la fuerza pública quedó mal parada a nivel nacional e internacional cuando en las primeras semanas de protestas, internet se inundó de denuncias y videos sobre presunto uso excesivo de la fuerza o posibles violaciones a los derechos humanos. Ante esta andanada de reclamos e indignación, el MinDefensa no reaccionó con sanciones a los implicados en presuntos excesos o delitos, sino poniendo en marcha, lo que parece ser, una estrategia para adueñarse de la narrativa sobre el paro nacional y las actuaciones de los organismos de seguridad en el espacio público digital. Esta fue la dimensión del ciberpatrullaje de la que más se habló y vimos durante el paro nacional.

Hay algunos indicios claros de que el ciberpatrullaje se usó como herramienta para controlar la narrativa en el espacio público digital. Para empezar, como ya fue explicado, la puesta en marcha de la policía de la verdad

61 Fundación Karisma. El ciberbolillo que nos espera. Disponible en: https://web.karisma.org.co/el-ciberbolillo-que-nos-espera/
62 Fundación Karisma. Nuevo Contrato de la DIPOL para perfilar y rastrear a las personas en internet. Disponible en: https://web.karisma.org.co/nuevo-contrato-de-la-dipol-para-perfilar-y-rastrear-a-las-personas-en-internet/
63 Fundación Karisma con colaboración de Temblores ONG. Dime a quién sigues y te diré qué tan peligrosos eres. Disponible en: https://web.karisma.org.co/dime-a-quien-sigues-y-te-dire-que-tan-peligroso-eres/
64 Comisión Interamericana de Derechos Humanos. Observaciones y Recomendaciones. Visita de trabajo en Colombia. Disponible en: https://www.oas.org/es/cidh/informes/pdfs/ObservacionesVisita_CIDH_Colombia_SPA.pdf

que cataloga como falsas o ciertas sus propias actuaciones denota un interés del MinDefensa por cuidar su propia imagen y no tanto por cuidar la seguridad de la ciudadanía. La atribución de la fuerza pública para verificar con sus propias fuentes reservadas qué de lo publicado en internet por la ciudadanía es falso, además de no tener sustento legal y que la CIDH lo ha catalogado en varias ocasiones como una amenaza a la libertad de expresión e información, surge del interés por contrarrestar las denuncias en contra de la fuerza pública.

Así quedó ejemplificado, el 5 de mayo de 2021, cuando a través de las redes sociales oficiales de todas las ramas de la fuerzas armadas y del Ministerio de Defensa se lanzó la campaña #ColombiaEsMiVerdad, con la cual se intentó acabar a la "desinformación" tratando de noticias falsas o terrorismo digital a publicaciones que no beneficiaban la imagen del ejercio o la policía[65].

Hacen parte de dicha campaña de imagen, el Boletín de Fake News de la Policía Nacional[66] o las publicaciones hechas el 13 de mayo por la policía[67] y el 19 de mayo por el ejército[68] en sus redes, bajo los numerales: #ColomabiaEsMiVerdad, #RompaLaCadena, #MeInformoMejor, en las que se invita a no compartir noticias que señalan como falsas con el objetivo de "romper la cadena de desinformación".

Sin embargo, conforme el paro ha avanzado y la intensidad de los enfrentamientos ha disminuido, al menos durante el mes de junio, el numeral #ColombiaEsMiVerdad comenzó a ser usado, por miembros de la fuerza pública y desde las redes oficiales de las mismas para difundir información que legitima al ejército o que ayuda a difundir una imagen positiva del mismo[69]. Mientras tanto, el #RompaLaCadena sigue siendo usado de forma activa para luchar contra la "desinformación" y haciendo un llamado "para no seguir el juego de las noticias falsas a través de las redes sociales"[70]. Finalmente, el #MeInformoMejor ha sido usado desde cuentas oficiales de la Presidencia y Vicepresidencia para señalar denuncias públicas como falsas y solicitar que no sean compartidas[71].

La campaña contra la supuesta desinformación adelantada por la fuerza pública evidencia la intención por controlar lo que se dice en el espacio público digital sobre lo que estaba aconteciendo en Colombia. Para empezar, se catalogó, sin sustento legal, de falsas o verdaderas denuncias sobre posibles violaciones a derechos humanos y los contenidos que no eran afines a los organismos de seguridad. Además, desde la Presidencia se promovió que no se compartieran algunas publicaciones previamente catalogadas y, en cambio, desde las cuentas pertenecientes a entidades adscritas al Ministerio de Defensa se publicaron y compartieron noticias favorables a su imagen. Comportamientos que evidencian una intención por controlar cuándo, cómo y qué se decía sobre el paro y la fuerza pública en redes sociales, el espacio de debate de mayor importancia y alcance de la actualidad.

Sumado a esto, fueron muchos los casos en que funcionarios de gobiernos locales o del nacional se han referido de forma estigmatizante a la ciudadanía que de una u otra forma hace parte activa del paro nacional. El mismo día en que iniciaron las manifestaciones, el 28 de abril de 2021, la Consejera Presidencial para los Derechos Humanos, Nancy Patricia Gutierrez, señalaba que había "vándalos que se camuflan entre los mani-

65 El Tiempo. Ministerio de Defensa Lanza Campaña contra Noticias Falsas en el Paro. Disponible en: https://www.eltiempo.com/justicia/servicios/ministerio-de-defensa-lanza-campana-contra-noticias-falsas-en-el-paro-586659?utm_medium=Social&utm_source=Twitter#Echobox=1620400394

66 Policía Nacional. Fake News en el marco del Paro Nacional 28a, 29a y 30a. Disponible en: https://oas.policia.gov.co/sites/default/files/documento_10_fake_news_manifestaciones.pdf

67 Unidad de Operaciones Especiales en Emergencia. Trino del 13 de mayo: https://twitter.com/GrupoPONALSAR/status/1392910787904147457?s=20

68 Dirección de Ampliación de Normas de Transparencia del Ejercito.Trino de 19 de mayo: https://twitter.com/YoSoyDanteEJC/status/1395116046860836867?s=20

69 Hashtags #ColomabiaEsMiVerdad en Twitter: https://twitter.com/search?q=%23ColombiaesMIvERDAD&src=typed_query

70 Hashtags#RompaLaCadena en twitter: https://twitter.com/search?q=%23RompaLaCadena&src=typed_query

71 Hashtags #MeInformoMejor en twitter: https://twitter.com/search?q=%23MeInformoMejor&src=typed_query

festantes", y que merecían "sanción penal más dura"[72]. A medida que el paro se intensificó y las redes sociales comenzaron a inundarse de contenido sobre enfrentamientos entre manifestantes y fuerza pública o de denuncias de abusos en el uso de la fuerza por parte de la policía, la campaña de criminalización de la protesta también se digitalizó.

El 3 de mayo, el ministro de defensa, Diego Molano, señaló en un trino que "los terroristas están operando con convocatorias a través de WhatsApp y Telegram y han sido sistemáticos su accionar en principales ciudades"[73]. De igual forma, Mindefensa lanzó a través de sus redes sociales la citada campaña #ColombiaEsMiVerdad, con el objetivo de tachar de falsas las acusaciones contra la policía y en respuesta al activismo de las fanáticas -en su mayoría mujeres jóvenes- del K-pop, quienes se habían apoderado de *hashtags* como*: #ApoyoAMiFuerzaPublica, #NoMasParo #ParoDestructorSOS, #UribeTieneLaRazon y #YoApoyoAlEsmad,* para difundir información sobre su bandas y canciones favoritas, aplacando así la tendencia iniciada por el político colombiano, Alvaro Uribe Velez, en defensa del uso de las armas por parte de la fuerza pública y en contra de las personas que se manifestaban[74].

Otro ejemplo de la campaña de deslegitimación de la protesta por parte del Ministerio de Defensa es el video publicado el 6 de mayo de 2021 en la cuentas oficiales de Facebook y Twitter del ministro Molano[75]. La publicación en la que, literalmente, tachó de falsa las denuncias sobre la fuerza pública y se refiririó a las denuncias como "terrorismo digital"[76].

El 7 de mayo, fue el Comandante General de las Fuerzas Armadas quien se refirió a las protestas de las fanáticas del K pop como noticias falsas mediante un comunicado[77]. Y ese mismo día, el director de la policía, se pronunció a través de un video desmintiendo las acusaciones de abuso del ESMAD y la policía, y señalando que dichas denuncias eran parte de una campaña de desinformación y terrorismo digital[78].

El presidente Duque también ha participado de la campaña de criminalización del activismo en redes durante el paro. El 28 de mayo de 2021, cuando se cumplía el primer mes de manifestaciones, y tras una jornada marcada por la violencia en las calles y por las denuncias en redes sobre civiles armados trabajando en conjunto con la policía, el presidente se refirió a lo ocurrido al dar un discurso en Cali señalando la existencia de "islas de anarquia" y una campaña "terrorismo digital urbano de baja intensidad"[79].

Respecto de los señalamientos de falsedad y terrorismo digital, se pronunció la CIDH en sus *Observaciones y recomendaciones. Visita de trabajo en Colombia.* La Comisión hizo un llamado para que la fuerza pública dejará

---

72 Presidencia de la República de Colombia. "Vándalos son criminales que merecen la sanción penal más dura": Consejera Nancy Patricia Gutiérrez. Disponible en: http://www.derechoshumanos.gov.co/Prensa/2021/Paginas/280421-Vandalos-son-criminales-que-merecen-la-sancion-penal-mas-dura-Consejera-Nancy-Patricia-Gutierrez.aspx

73 MinDefensa. Trino de 3 de mayo de 2021: https://twitter.com/mindefensa/status/1389232357354389505?s=20

74 Semana. Fans del K-pop "spamean" hashtags uribistas. Disponible en: https://www.semana.com/cultura/articulo/fans-del-k-pop-spamean-hashtags-uribistas/202132/

75 Ministro de Defensa, Diego Molano. Trino 6 de mayo de 2021: https://twitter.com/Diego_Molano/status/1390311574800375809?s=20

76 Ministro de Defensa, Diego Molano. Publicación en Facebook del 6 de mayo de 2021: https://www.facebook.com/DiegoMolanoAponte/videos/2861421874131466/

77 https://www.cgfm.mil.co/es/blog/colombia-es-mi-verdad-campana-que-busca-terminar-con-las-noticias-falsas

78 Semana. "Es falso que la policía ataca la manifestación pública y pacífica": general Jorge Vargas, director de la institución. Disponible en: https://www.semana.com/nacion/articulo/es-falso-que-la-policia-ataca-la-manifestacion-publica-y-pacifica-general-jorge-vargas-director-de-la-institucion/202144/

79 Presidencia de la República de Colombia. Declaración del Presidente de la República, Iván Duque Márquez - 28 de mayo de 2021. Disponible en: https://www.youtube.com/watch?v=uAZj0kKxejA

de calificar los contenidos, evitando incurrir en censura y recomendó al Estado aportar más información sobre el tema al debate público. Además, señaló que había "recibió denuncias por parte de las autoridades respecto de personas que publican información que contienen, que en su criterio, mensajes de "odio" o de "incitación a la violencia"[80], es decir, que se estaba publicando contenido fuera de los límites del derecho a la libertad de expresión y que puede ser intervenido por una autoridad judicial, respetando el debido proceso. Respecto a este tema, la CIDH instó al gobierno colombiano a que haga las respectivas denuncias, pero de nuevo que se abstenga, cómo es su deber, de calificar o censurar.

Siendo así, la estrategia del Estado Colombiano para capturar la narrativa sobre el paro y la fuerza pública en internet, el espacio contemporáneo de debate público de mayor alcance e importancia, tenía cuatro pasos: 1) señalar como falsas las denuncias sobre excesos de la fuerzas de seguridad, invitar a no compartir y promover contenido que beneficie su imagen, 2) señalar como vandálicas y, por tanto, de terroristas las actuaciones organizadas de la ciudadanía en pro del paro, 3) hacer uso de las categorías de la Convención Americana, que ponen límites a la libertad de expresión -incitación al odio y la violencia- para señalar los contenidos de la ciudadanía y así animar a que sean bloqueados por las plataformas y 4) llevar la estigmatización de la protesta y de quienes protestan hacia la criminalización usando el marco excepcional del terrorismo con el propósito de desincentivar la participación en las manifestaciones. Todo esto, presuntamente, con el objetivo de hacer mutar la narrativa en internet de un movimiento de protesta legítima con denuncias de excesos en el uso de la fuerza por parte del Estado a episodios de vandalismo y terrorismo, físico y digital, donde se promovieron discursos falsos o que incitaban al odio.

80 https://www.oas.org/es/cidh/informes/pdfs/ObservacionesVisita_CIDH_Colombia_SPA.pdf

TRES. LA TECNOLOGÍA AL SERVICIO DE LA VIGILANCIA O CÓMO ABUSAR DE LA HERRAMIENTA PARA CONTROLAR LA PROTESTA Y AMENAZAR LOS DERECHOS DE LAS PERSONAS

La falta de regulación sobre el uso de armas no letales, fue reconocida por el ex Relator de Ejecuciones Extrajudiciales de ONU, Christof Heyns, como un riesgo para los derechos humanos desde 2014[81]. A pesar de ello, actualmente la variedad de armas no letales o menos letales, no ha hecho más que aumentar debido a los avances tecnológicos y, en muchos casos, se ha perdido la línea que diferencia lo letal, de lo no letal[82].

Algo similar sucede con la tecnología. Los avances tecnológicos también se han traducido en la incorporación de diversos tipos de tecnología para controlar y vigilar las manifestaciones sociales o las multitudes por parte del Estado. Y aunque es de suponerse que con la aparición de nuevas tecnologías, se aumentaría la regulación que tiene el Estado de las mismas de modo que no sean abusadas y puedan convertirse en una amenaza, ese no parece ser el caso colombiano.

En este acápite abordaremos el caso de los dispositivos de reconocimiento facial y el acceso a los celulares de las personas por parte del Estado en el contexto del paro nacional, exponiendo los riesgos que estos implican para los derechos fundamentales de la ciudadanía.

3.1. Uso de tecnología de vigilancia en el marco de protestas ciudadanas

En 2020, la Alta Comisionada de las Naciones Unidas para los Derechos Humanos, Michelle Bachelet publicó un informe sobre tecnologías que vulneran el derecho a la protesta pacífica. En el informe, se señalaba que "la vigilancia por medios tecnológicos ha sido un factor importante en la reducción del espacio cívico ocurrida en numerosos países", ya que "las autoridades usan esos medios para vigilar directamente a quienes participan en las protestas"[83]. Esto a su vez genera que las personas pierdan el interés por manifestar públicamente sus ideas "por temor a ser identificadas y sufrir luego consecuencias adversas"[84].

En consecuencia, la alta comisionada recomendó a los Estados "que se abstengan de utilizar la tecnología de reconocimiento facial para identificar a quienes participan en reuniones pacíficas y que no realicen grabaciones de los manifestantes"[85]. Una recomendación a la que el Estado colombiano hace caso omiso.

3.1.1 Qué es el reconocimiento facial

Antes de abordar los posibles usos que le da el Estado colombiano a la tecnología de reconocimiento facial, es necesaria una pequeña introducción. El reconocimiento facial es "un método a través del cual se busca identificar o verificar la identidad de una persona utilizando capturas de su rostro, a través del uso de fotografías, videos guardados o cámaras que captan imágenes en tiempo real"[86]. Con esta tecnología se busca lograr autenticar la identidad de una persona, es decir, verificar si la persona es quien dice ser, o, identificar a un individuo, en otras palabras, establecer quién es o cuál es su identidad[87].

---

81 ONU, Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias, Nota del Secretario General, A/69/265, 6 Agosto 2014 párr.73.
82 Relatoría Especial para la Libertad de Expresión. Protesta y Derechos Humanos. Párrafos 119 y 120. Disponible en: http://www.oas.org/es/cidh/expresion/publicaciones/ProtestayDerechosHumanos.pdf
83 Oficina del Alto Comisionado de Naciones Unidas para los Derechos Humanos. Las nuevas tecnologías deben reforzar el derecho a la protesta pacífica, no impedirlo. Disponible en: https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=S
84 Ibidem.
85 Ibidem.
86 Fundación Karisma. Qué es y Cómo funciona el reconocimiento facial. Disponible en: https://digitalid.karisma.org.co/2021/07/01/que-es-reconocimiento-facial/
87 Ibidem.

Ahora bien, tanto para identificar como para autenticar la identidad de una persona se requiere: 1) capturar un rostro a partir de diferentes sensores, como cámaras, videos o imágenes y 2) una base de datos que contenga los registros de los rostros de diversas personas para comparar con la imagen previamente capturada.

De forma resumida, el proceso de reconocimiento facial es el siguiente: primero se captura una imagen de consulta, es decir, la imagen del rostro de una persona; en seguida, el sistema detecta y determina la posición de los ojos y, a partir de allí, se convierte la imagen de consulta en una "huella facial", es decir, en una representación numérica y digital de esta cara. Una vez creada la huella facial se compara con todas las huellas faciales que se encuentran almacenadas en la base de datos. Para una explicación detallada sobre este procedimiento recomendamos ID Colombia, *Qué es y Cómo funciona el reconocimiento facial*.

3.1.2 Sistema de reconocimiento facial en poder del Estado colombiano

Se sabe con certeza que al menos tres entidades del Estado colombiano cuentan con sistemas capaces de identificar rostros de forma masiva en cualquier formato de video o imagen: Migración Colombia, la Policía Nacional y la Registraduría Nacional [88]. Aquí nos referiremos de forma breve a las dos últimas entidades, pues su actuar puede estar relacionado con lo sucedido durante el paro nacional.

La Registraduría administra el Sistema Nacional de Identidad (SNI) en cual cuenta con tecnología de reconocimiento facial y contiene los datos de todos los mayores de 7 años que hayan tramitado documentos de identidad. Dicho sistema tiene como objetivo la identificación legal de las personas a partir de características únicas, en este caso a través de algoritmos que identifican la biometría facial. En concreto, desde 2018, la Registraduría incluyó el reconocimiento facial al SNI y lo ofrece como un servicio a terceros, incluidas la Fuerza Pública, sin que esté claro qué marco jurídico o garantías con el derecho a la intimidad está aplicando[89].

Por el lado de la Policía Nacional se ha establecido que en 2019 contrató un sistema biométrico facial, palmar y dactilar para "individualizar el crimen" a través de la identificación de personas en videos e imágenes[90]. Además, según informó la Dirección de Investigación Criminal e Interpol de la Policía Nacional a Fundación Karisma en 2021, el sistema ABIS de la Policía estaría usando para comparar imágenes de consulta las bases de datos de la Registraduría. Y al igual que en el caso de la Registraduría esta tecnología se está usando sin el control de un marco legal, e incluso es posible que en contextos políticos como manifestaciones y protestas. Este sistema está a cargo de la DIJIN, Policía Judicial, así que idealmente debería usarse en investigaciones criminales y con la autorización judicial previa. Sin embargo, no podemos descartar que el sistema se pueda utilizar en los contextos de protesta porque el sistema ABIS está en manos de las autoridades policiales y podrían utilizarlo fuera del contexto de investigaciones penales.

3.1.3 Uso inadecuado de tecnología para el control de la protesta social durante el paro nacional

En 2019, la Policía Nacional estrenó, en Bogotá y Medellín, una cámara para monitorear las manifestaciones que se llevaron a cabo durante el mes de noviembre[91]. Según se informó en varios medios nacionales, las

88 Fundación Karisma. Guía Reconocimiento Facial en Colombia. Disponible en: https://digitalid.karisma.org.co/2021/07/01/guia-reconocimiento-facial/
89 Fundación Karisma. El sistema de reconocimiento de la Registraduría General. Disponible en: https://digitalid.karisma.org.co/2021/07/01/sistema-reconocimiento-facial-registraduria/
90 Fundación Karisma. El sistema multibiométrico ABIS de la Policía Nacional. Disponible en: https://digitalid.karisma.org.co/2021/07/01/ABIS-reconocimiento-facial/
91 Revista Semana. Así es el halcón, el helicóptero que vigilará el paro en Bogotá usando reconocimiento facial. Disponible en:https://www.semana.com/nacion/articulo/paro-21-de-noviembre-el-helicoptero-que-vigilara-en-bogota-usando-reconocimiento-facial/641014/

cámaras de alta calidad incorporadas en el helicóptero halcón de la policía contaban con un software que comparaba los rasgos físicos captados con los de las bases de datos del organismo de seguridad como la Dirección de Investigación Criminal e Interpol (Dijin) y con las bases de datos de la Registraduría Nacional.[92] La policía aseguró que estas cámaras se usarían en zonas donde se presentaran alteraciones al orden público como guía para los uniformados en tierra, y, se dijo, tenían un alcance de más de 15 metros.

No obstante, en enero de 2021, la ONG, Dejusticia, puso en duda si la Policía en efecto estaba usando herramientas de reconocimiento facial para monitorear manifestaciones, al señalar que "*esa comunicación fue un intento de las autoridades por disuadir a los colombianos de salir a protestar*"[93]. Esto tras consultar a través de derechos de petición a la Fiscalía y la Policía sobre investigaciones o judicializaciones "como resultado del uso efectivo de esta herramienta".

De lo que no hay duda es sobre la presencia de helicópteros que han sobrevolado las protestas durante el Paro Nacional en 2021, y durante las marchas asociadas al movimiento 21N en años anteriores. En Bogotá,[94] Cali[95], Buga[96], hay reportes o videos de helicópteros militares sobrevolando marchas. Lo que no es seguro, insistimos, es si han procesado imágenes captadas desde los helicópteros para identificar a las personas con ayuda de las bases de datos de la RNEC o cualquier otra. De nuevo, la opacidad extrema del Estado colombiano, por lo menos respecto al sector defensa, dificulta saber qué hacen o no los órganos de seguridad, esto, insistimos, no es compatible con las garantías exigibles al Estado respecto de una protesta ciudadana.

El otro tipo de tecnología sobre la que existen dudas respecto a la forma en que la policía la está utilizando en el marco de la protesta social son los drones. Lo primero que hay que decir es que la policía está equipada con este tipo de tecnología[97] y la usa con frecuencia[98] en distintas zonas del país[99]. Ahora bien, en 2020, la Corte Suprema de Justicia tuteló el derecho a la protesta de varias personas y ordenó una serie de cambios sobre los protocolos y elementos que puede usar el escuadrón antidisturbios de la policía[100]. Sin embargo, la tecnología fue el gran tema ausente de la sentencia, por lo cual hoy se podría usar estos dispositivos para vigilar las marchas del paro. De hecho, la Defensoría del Pueblo le recomendó a la Policía que usará los drones en el marco de la protesta[101].

---

92 El Tiempo. Helicóptero halcón de la Policía estrenando identificación facial. Disponible en: https://www.eltiempo.com/bogota/estrenan-helicoptero-halcon-con-reconocimiento-facial-en-paro-del-21-de-noviembre-435766

93 Dejusticia. Día de la protección de datos: helicópteros, reconocimiento facial y protesta. Disponible en: https://www.dejusticia.org/dia-de-la-proteccion-de-datos-helicopteros-reconocimiento-facial-y-protesta/

94 Revista Semana. ¿Por qué aterrizó un helicóptero de guerra Black Hawk anoche en Bogotá?. Disponible en: https://www.youtube.com/watch?v=fEMTX2vAz1g&ab_channel=RevistaSemana

95 Vice. Colombia Is Rising Up. Disponible en: https://www.youtube.com/watch?v=WB2isJA1JdU&ab_channel=VICENews

96 Infobae. Momentos de pánico en Buga por un helicóptero en medio de disturbios tras el paro nacional Disponible en: https://www.infobae.com/america/colombia/2021/05/06/video-momentos-de-panico-en-buga-por-un-helicoptero-en-medio-de-disturbios-tras-el-paro-nacional/

97 Alcaldía de Bogotá. Cinco drones de última tecnología ayudarán a cuidar la vida en Bogotá. Disponible en: https://bogota.gov.co/asi-vamos/drones-de-ultima-tecnologia-refuerzan-seguridad-de-bogota

98 El Tiempo. Patrulla con drones logró captura de 47 delincuentes en Barranquilla. Diponible en: https://www.eltiempo.com/colombia/barranquilla/patrulla-con-drones-ha-logrado-decenas-de-capturas-en-barranquilla-384854

99 Blue Radio. Con drones pretenden vigilar la ciudad de Medellín para evitar las construcciones ilegales. Disponible en:https://www.bluradio.com/tecnologia/con-drones-pretenden-vigilar-la-ciudad-de-medellin-para-evitar-las-construcciones-ilegales

100 Dejusticia. Corte Suprema de Justicia protege el derecho a la protesta frente a la violencia policial. Disponible en:https://www.dejusticia.org/corte-suprema-protege-el-derecho-a-la-protesta/

101 El Tiempo. Vigilar Protesta con drones y otras recomendaciones de LA Defensoría. Disponible en: https://www.eltiempo.com/justicia/servicios/marchas-y-protestas-las-33-recomendaciones-de-defensoria-del-pueblo-para-evitar-violencia-556308

Siendo así, no es descabellado pensar que los drones que en ocasiones sobrevuelan las marchas y aglomeraciones que sucedieron dentro del paro nacional fueran de la fuerza pública. El uso de estos dispositivos sin la debida regulación y control pone en riesgo el derecho a la intimidad y afecta el legítimo derecho a la protesta que tiene la ciudadanía. Pero, como con los cortes a internet y la tecnología de reconocimiento facial, no hay certeza. Dado que no hay una regulación clara sobre la tecnología y que el Estado no informa de forma periódica sobre estos asuntos, todo se queda en especulaciones.

En este caso, la entidad estatal llamada a regular e investigar los drones que sobrevuelan las marchas es la Aeronáutica civil, unidad administrativa que expidió el Reglamento Aeronáutico Colombiano, la norma que por analogía aplica a los drones[102]. Sin embargo, la Aeronáutica no se ha pronunciado al respecto, lo que de nuevo crea un vacío legal que deja desprotegidos los derechos de la ciudadanía. Se esperaría como mínimo que los drones que sobrevuelan una manifestación estén identificados de modo que se sepa quién los controla y el número del dispositivo, así como sucede con los propios agentes de la fuerza pública. Esta disposición permitiría a la ciudadanía ejercer algunos de sus derechos o pedir cuentas a la fuerza pública.

3.2 Las requisas a celulares. Una práctica común que vulnera el derecho fundamental a la intimidad

El artículo 159 del Código de Policía colombiano, y recientemente la Corte Constitucional[103], autorizan a la policía a requisar o catear a las personas con un alto nivel de discrecionalidad. Sin embargo, ese poder de la policía no es un permiso para revisar los celulares de las personas a discreción. Los contenidos de un celular, tales como chats, videos, imágenes, registros, claves, documentos, entre otros, están directamente relacionado con el derecho a la intimidad de las personas, pues es información que solo le concierne al propietario o propietaria del equipo, y que además puede estar conectada con otras garantías constitucionales como el secreto profesional o la reserva de la fuente.

Por tal razón, al igual que con un registro a una casa, la policía solo puede requisar un celular con una orden judicial. De otra forma se vulneran los derechos fundamentales a la intimidad, al debido proceso y a la presunción de inocencia. Ahora bien, las denuncias sobre requisas a celulares son una constante en Colombia en el contexto de la protesta social[104]. Incluso se han reportado casos en que la policía hace la requisa para revisar las redes sociales de las personas[105]. Estas acciones implican una intromisión de las fuerzas de seguridad del Estado en el ámbito más personal e íntimo de las personas.

Para entender qué sucede con las requisas a celulares en Colombia hay que hablar de la política del MinTIC de registro del IMEI, código único que identifica a los celulares, para combatir el robo de aparatos. Esta política es ineficiente, pues no ha solucionado el problema de hurtos de celulares, y, además, pone en riesgo derechos fundamentales de la ciudadanía[106], pues sirve para que la policía, que no puede revisar los celulares, pueda

---

102 Revista Universidad Externado. Del campo de batalla a las calles: el derecho a la intimidad en la era de los drones. Disponible en: https://revistas.uexternado.edu.co/index.php/derest/article/view/4339/5066

103 Infobae. Qué hacer si, en una requisa, la Policía le pide su celular. Disponible en: https://www.infobae.com/america/colombia/2021/03/04/que-hacer-si-en-una-requisa-la-policia-le-pide-su-celular/

104 Ámbito Jurídico. ¿Las requisas policivas pueden incluir la revisión de redes sociales?. Disponible en: https://www.ambitojuridico.com/noticias/general/constitucional-y-derechos-humanos/las-requisas-policivas-pueden-incluir-la

105 Fundación Karisma. Trino del 4 de diciembre de 2020: https://twitter.com/karisma/status/1202298426601463809?lang=es

106 Fundación Karisma. Revisar IMEI, excusa para el abuso policial. Disponible en: https://web.karisma.org.co/revisar-imei-excusa-para-el-abuso-policial/

obligar que las personas les muestres el IMEI de su celular para verificar que no es un equipo robado. Esto se ha prestado para algunas irregularidades.

En el marco de manifestaciones se han producido denuncias de que con la excusa de revisar el IMEI, algunos agentes de policía le pide a las personas la clave y desbloquea el celular, acto seguido pueden revisar las redes sociales o eliminar imágenes y videos prueba de posibles abusos o violaciones a derechos humanos[107][108]. Durante la protesta Fundación Karisma también recibió algunos reportes sobre intimidaciones directas de agentes de la policía a ciudadanos para que desbloquearan sus celulares o en las que aprovechaban el momento de poner o quitar las esposas para, sin consentimiento, poner la huella de los ciudadanos en el lector de celular y así desbloquearlo.

La cuestión es compleja: la policía no puede revisar el contenido de los celulares sin orden judicial, pero si pueden verificar el IMEI en las bases de datos de celulares robados, para lo cual puede exigir a la persona que le muestre el IMEI del equipo. De esta forma, cuando se armoniza la regulación, el procedimiento estipulado es que sea la propia persona la que marque *#06# para mostrar el IMEI del equipo, sin necesidad de entregar el celular o desbloquearlo.

Sin embargo, la línea entre revisar el celular y verificar el IMEI en medio de una requisa es demasiado tenue en la práctica y pone en riesgo los derechos fundamentales de la ciudadanía. En el contexto de una requisa es difícil explicar a un agente de policía las precisiones técnicas y jurídicas del caso, y muchas personas pueden acceder a entregar el celular al sentirse intimidados. De tal forma que, la existencia de la política del IMEI es un riesgo para los derechos fundamentales de la ciudadanía, ya que es una excusa de los policías para acceder a los celulares. Todavía más en contexto de protesta donde las requisas aumentan y se registran abusos por parte de la fuerza pública.

Siendo así, es necesario que se replanteen las políticas del MinTIC sobre celulares robados y se expidan protocolos que dejen claro que el registro de celulares es equivalente al allanamiento de una casa y por tanto, debe cumplir los más exigentes estándares para la protección de la privacidad de las personas.

107 Ibidem.
108 Temblores ONG. Bolillo, Dios y Patria. Disponible en: https://issuu.com/temblores/docs/bolillo-dios-patria-digital

CUATRO. EMPRESAS INTERMEDIARIAS. ACTORES CLAVES, PARA LA GARANTÍA Y PROTECCIÓN DE LOS DERECHOS HUMANOS DURANTE LAS PROTESTAS

Internet ha sido reconocida tanto por el Estado colombiano como por la CIDH como una herramienta que democratizó y amplió la posibilidades de ejercer derechos fundamentales de la ciudadanía[109]. Ahora bien, es un hecho que internet está gobernada de forma multisectorial, es decir, que aunque los gobiernos tienen importantes intereses en regular esta red, su despliegue y operación dependen en gran medida del sector privado. Además, se reconoce que por su carácter de medio de comunicación global, a internet le aplican normas de derecho público y su regulación no se limite únicamente a lo establecido en contratos privados[110]. Todo ello sin olvidar que la sociedad civil también juega un importante rol en sus discusiones.

Dado el papel que han adquirido internet y las redes sociales en la vida cotidiana de las personas, era solo cuestión de tiempo para que se evidenciara su relevancia en la vida pública y política de las sociedades. Así ha sucedido en los últimos años durante las elecciones y se ha mostrado en forma clara durante las recientes movilizaciones sociales en América Latina, así como en este caso, durante las manifestaciones sociales y políticas contra el gobierno colombiano en 2021.

Durante el paro nacional, en especial en medio de las jornadas con mayor participación ciudadana o en las que se han dado enfrentamientos entre manifestantes y fuerza pública, las redes sociales se convirtieron en el principal mecanismo de denuncia de abusos de la autoridad o de violaciones a los derechos humanos. Sin embargo, con la creciente indignación nacional, también aparecieron los reportes en redes sociales de personas que no podían subir videos a sus redes sociales, hacer transmisiones en vivo, compartir contenidos de otras personas o la información que estaban subiendo a sus redes sociales tenía el alcance restringido. Todo esto sumado a las denuncias de bloqueos de internet, ya explicadas, generaron una sensación de censura en línea.

Aunque la sensación de censura suele dirigirse al Estado, la comunicación la intermedian empresas privadas que de repente parecen no permitir a la ciudadanía expresarse en un momento importante y urgente. Por lo tanto, en momentos de creciente tensión social, y teniendo en cuenta la complejidad de la conectividad y uso de servicios en internet, poder establecer el origen y naturaleza de los problemas que las personas enfrentan para comunicarse puede evitar que aumente la sensación de censura estatal.

En el informe de 2016 sobre el rol del sector privado y el Estado en el ejercicio de la libertad de expresión en internet[111], el relator para la promoción y protección del derecho a libertad de expresión de la ONU reconoció el importante papel del sector privado en el respeto a la libertad de expresión en la era digital. El informe reconoce que las empresas están sometidas a presiones estatales que pueden derivar en limitaciones a los derechos de las personas, pero les recuerda que también desempeñan funciones independientes que pueden promover o restringir los derechos. La medida que se resalta en especial en este informe es la de transparencia tanto en los procedimientos que aplica el sector privado, en donde debe considerar evaluaciones de impacto a los derechos de las personas, como en la posibilidad de entregar información y datos sobre sus acciones que permitan el escrutinio público.

Aquí les explicamos tres posibles causas de los problemas para comunicarse a través de internet que se presentaron durante el paro nacional de 2021.

---

109 Relatoría para la Libertad de Expresión CIDH. Estándares para una internet libre, abierta e incluyente.

110 Naciones Unidas. Asamblea General. Resolución 70/125. Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información, UN Doc. A/RES/70/125. 1 de febrero de 2016. Párr. 9.

111 Ver: https://www.undocs.org/A/HRC/32/38

4.1. Problemas con la infraestructura para la prestación del servicio de internet

Como se explicó previamente, una primera causa de los problemas de conexión que experimentó la ciudadanía pueden tener origen en fallas en la infraestructura de internet (como daños, mantenimiento o cortes de energía) o la sobrecarga en las redes (que puede suceder cuando hay concentraciones de personas que demandan mucha conectividad). Este tipo de eventos son frecuentes y la información que las empresas suministren sobre su actuación y la salud de sus redes en estos momentos resulta importante para aclarar lo que está sucediendo.

Respecto del caso de la noche del 4 de mayo en Cali, reiteramos que el revuelo en redes sociales llevó a Movistar a informar a los medios de comunicación y al Ministerio TIC, que había afectaciones en su red producto del hurto de cables y la imposibilidad de repararlos debido a los problemas de orden público que sacudieron a Cali ese día. Esto permitió entender la falla informada por Netblocks y también establecer que las fallas que se presentaban en sitios como Siloé no respondían a problemas en la infraestructura de las empresas operadoras de internet en el país.

4.2. La moderación de contenidos

Una segunda causa de los problemas para difundir publicaciones en redes son las políticas de moderación de contenidos. Hay varios factores que ayudan a explicar la cancelación de cuentas, o las restricciones de alcance y el bloqueo de contenidos en redes sociales. Como lo explicamos en el capítulo sobre conectividad para que un Live en medio de una protesta funcione, muchos factores deben converger, no solo tiene que activarse la conectividad a través de la infraestructura física, además debemos poder usar los servicios que nos permiten compartir los contenidos que queremos comunicar y que se materializan en diferentes formatos (texto, audio, vídeo o imágenes), y allí es donde están las redes sociales, la capa más evidente para las personas que usamos internet.

Los contenidos que circulan por las redes sociales se someten a las reglas de comunidad, es decir, a las normas que las personas que las usan deben seguir para evitar que sus cuentas sean canceladas o que sus contenidos sean bloqueados o su alcance disminuido. La acción de aplicar esas normas y las sanciones se conoce como moderación de contenidos y se realiza conforme con la última versión de los términos de uso que aceptamos al registrarnos en la plataforma correspondiente.

Siendo así, para que el “Live” sea exitoso, como mínimo se necesita que las infraestructuras de internet y energía estén activas, el servicio de la plataforma funcione debidamente -sobre esto hablaremos justo en el siguiente caso-, y el contenido que se transmite debe pasar el filtro de la moderación de contenidos. La moderación de contenidos sucede todo el tiempo, sin embargo, el volumen de información que se produce en una protesta, la concentración de la producción de contenidos que puede darse en cabeza de unas pocas personas en determinados momentos, y la naturaleza de los mismos -un contenido que denuncia abuso policial puede ser catalogado por ejemplo como contenido violento que es prohibido por las reglas de comunidad- hacen que la moderación de contenidos sea protagonista de las protestas y muchas personas vinculadas con ese momento la resientan en forma especial.

Las redes sociales que en su uso cotidiano están pensadas para ser de “ambiente familiar” de repente durante protestas que se tornan violentas y enfrentan a diferentes actores pasan a ser escenarios de denuncia de violaciones a los derechos humanos y se crean tensiones e importantes frustraciones. Algo similar al derecho de ingreso en un bar, club o tienda, al ser un lugar privado aceptamos las reglas o de lo contrario quedamos

por fuera, sin embargo, esto no autoriza al club a tener actuaciones discriminatorias. En las redes sociales, que pertenecen a multinacionales privadas, todos los días se bloquean y bajan contenidos que no cumplen las normas de uso que aceptamos al registrarnos en ella, sin embargo, cuando se está ante un hecho social y las personas están contando con sus cuentas para informar, es necesario que estas empresas protejan las comunicaciones y actúen para evitar que sus normas de comunidad eviten la denuncia de graves atropellos a los derechos humanos.

Por citar algunos casos en el contexto del paro nacional, encontramos lo sucedido en Twitter con la cuenta oficial de Noís Radio, un medio alternativo de Cali. El 6 de mayo el medio reportó que su cuenta de Twitter @noisradio había sido "reiteradamente restringida y etiquetada con el aviso "Precaución: esta cuenta está temporalmente restringida", luego de publicar una nota sobre abuso policial. Aunque Twitter argumentó frente al medio que se trata de "retos de autenticidad", pues se le solicitó a Nois Radio demostrar que no era administrada por un robot. Nois Radio apeló las decisiones pero la situación se repitió varias veces lo que los llevó a manifestar que estos procesos de apelación ante las redes sociales no son eficaces. Además, desde Noís Radio consideran que etiquetas como esa terminan silenciando su voz al ser visibles los avisos de precaución tanto para quienes navegan en Colombia como en otros países por aplicación de las condiciones de uso de la plataforma privada, "vulneran la libertad de expresión y alimentan la sensación de censura en Internet en medio de una coyuntura como la que ha vivido Colombia en las últimas semanas", según informó directamente el medio.

Otro ejemplo paradigmático es el etiquetamiento por parte de Twitter de trinos sobre audiencias públicas ante la CIDH durante su visita de trabajo en Colombia como contenido "potencialmente delicado", tal como sucedió el 9 de junio en la cuenta de la defensora de derechos humanos y ambientalista, Francia Márquez[112].

Los problemas por bloqueo durante el paro han generado que algunos periodistas tuvieran que recurrir al uso de varias cuentas o a utilizar caracteres numéricos en las descripciones de sus publicaciones para intentar engañar el algoritmo. El periodista independiente, Jahfrann, en un testimonio inédito entregado a la FLIP lo explica así: "He tenido momentos en que he querido hacer un Live y las dos cuentas [de Instagram] me las tienen bloqueadas. Ahí ya me toca utilizar otro canal porque Instagram no responde, te puedes poner a esperar, pero ellos no te van a responder nunca. Simplemente ellos te avisan que te bloquearon y ya. Además, hay palabras que uno no puede colocar, un SOS COLOMBIA es un bloqueo seguro. Entonces, uno tiene que mirar qué y cómo publicar, y a veces no publica. O si uno dice ALERTA, uno usa un "4", en vez de una "A" o coloca un 3, en vez de la "E" (4L3RTA). Empezás a jugar con estos algoritmos".

Ante estas irregularidades respecto del control de contenido, donde se etiqueta de peligroso o se bloquean publicaciones relacionadas con la defensa de derechos humanos es necesaria una evaluación profunda y de contexto de lo que se está censurando. Muchas veces las normas de comunidad de las redes sociales son ambiguas o amplían los límites de la Convención Interamericana de Derechos Humanos o, simplemente, no están pensadas para el contexto latinoamericano ni, mucho menos, para una protesta social. Lo que de plano limita las posibilidades de expresión dentro de las redes.

Los desafíos de mitigar el impacto de la moderación de contenidos por parte de las plataformas durante los levantamientos sociales se mantienen. Aunque se identifican esfuerzos de las empresas por disminuir ese impacto, como usar más las etiquetas y la disminución del alcance de las publicaciones y menos el bloqueo de contenidos y la cancelación de cuentas, la sensación de censura durante las protestas es permanente y la ausencia de información sobre la forma como las empresas atienden estas coyunturas no aporta a dar tran-

112 Francia Márquez M. Trino del 9 de junio: https://twitter.com/FranciaMarquezM/status/1402648233621475329

quilidad a las personas que dependen de estas herramientas para publicar contenidos y denuncias de graves afectaciones a los derechos humanos. En esto, todavía hay mucho por mejorar.

4.3. El software de las plataformas también falla y puede impactar la protesta social

Ya hemos dicho que para que la comunicación de las personas que participan en la protesta suceda es necesario que la infraestructura física funcione y que el contenido no quede filtrado en los procesos internos de moderación de las plataformas, sitios web y aplicaciones propiamente dichas, pero también se requiere que el software de la red social que usamos funcione correctamente. De esto casi nunca se habla pero también es crucial durante una protesta. Los problemas con el software son una posible tercera explicación a los problemas de publicación y distribución de contenidos que se vivieron durante el paro.

En la primera semana de manifestaciones, muchas personas y organizaciones sociales reportaron problemas para subir contenido relacionado con el paro nacional a redes sociales. Entre el 6 y el 7 de mayo esto sucedió principalmente en Instagram[113]. Esta red social, estaba siendo usada para compartir contenido relacionado con el paro, así como videos sobre posibles abusos policiales y para realizar transmisiones en vivo de la marcha, presentaciones artísticas y enfrentamientos[114].

El 6 de mayo de 2021, los reportes sobre los problemas de las historias de Instagram fueron tendencia durante la mañana. El fenómeno fue tan generalizado, que en la Fundación Karisma pasamos de recibir 8 reportes de problemas con contenido en redes sociales entre el 28 de abril y el 5 de mayo, a 100 reportes tan solo el 6 de mayo en la mañana y en la noche del mismo día los reportes llegaron a un total de 800 casos. El 90% de los casos que nos fueron reportados eran por problemas en Instagram[115].

Ese mismo día, 6 de mayo, Facebook, la empresa dueña de la red social Instagram reportó una falla global[116] y la arregló en cuestión de un día[117]. Además, el 7 de mayo, Instagram explicó que la falla tuvo especial importancia en Colombia, pero que también afectó al pueblo palestino[118] y a comunidades indígenas de EEUU y Canadá[119] quienes conmemoraban el día en contra de la violencia contra los las comunidades nativas[120]. Esta declaración puso en evidencia que la falla no fue generalizada, sino que afectó a contenido relacionado a causas sociales, políticas y étnicas, en tres puntos geográficos específicos.

---

113 El Espectador. Represión en la calle, sensación de censura en redes. Disponible en: https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/represion-en-la-calle-sensacion-de-censura-en-redes-column/

114 Revista 070. Los en vivo: estar vivos y ser vistos. Disponible en: https://cerosetenta.uniandes.edu.co/los-en-vivo-estar-vivos-y-ser-vistos/

115 Fundación Karisma. #ParoNacionalColombia ¿Qué pasó con las historias de Instagram el 6 de mayo?. Disponible en: https://web.karisma.org.co/paronacionalcolombia-que-paso-con-las-historias-de-instagram-el-6-de-mayo/

116 Infobae. Una falla técnica dejó sin visibilidad las publicaciones de usuarios de Instagram. Disponible en:https://www.infobae.com/america/tecno/2021/05/10/una-falla-tecnica-dejo-sin-visibilidad-las-publicaciones-de-usuarios-de-instagram/

117 Cuenta oficial de Instagram. Trinos del 6 de mayo: https://twitter.com/InstagramComms/status/1390376354332487681?s=20 y https://twitter.com/InstagramComms/status/1390485897787883523?s=20

118 Logically. Palestinians Bear The Brunt Of Big Tech Moderation. Disponible en: https://www.logically.ai/articles/no-platform-has-a-public-moderations-policy-for-war-zones

119 Vice. Instagram Stories About Violence Against Indigenous Women Are Disappearing. Disponible en: https://www.vice.com/en/article/jg8843/instagram-stories-about-mmiwg-violence-against-indigenous-women-are-disappearing

120 Cuenta oficial de Instagram. Trino del 7 de mayo: https://twitter.com/InstagramComms/status/1390818110664593409?s=20

En el caso de Instagram, según reportó la misma plataforma, hablamos de un problema a escala con el software encargado de evaluar la disponibilidad del contenido que se sube a la red social, en específico, sobre un componente que se encarga de borrar *re-publicaciones* cuyo contenido original había sido borrado previamente. Lo extraño es que afectó especialmente esos días a los sitios donde había expresiones colectivas de causas socio políticas.

Otros ejemplos de fallas en el software que se tradujeron en censura de material relacionado con el paro nacional son lo sucedido el 4 de mayo, cuando falló la funcionalidad de tendencias en Twitter; o la que tuvo lugar el 18 de mayo en Facebook en donde personas usuarias de la red social informaron sobre la deshabilitación de la opción que permitía hacer transmisiones en vivo.

Finalmente, resaltamos que la política de asumida por Facebook, como intermediario de internet, reconocer mediante trinos el problema de software y sus consecuencias es un buena práctica que debería extenderse a otras plataformas en casos en que los inconvenientes con el software afectan el ejercicio de derechos de los usuarios y usuarias de estas plataformas.

4.4 Un breve llamado a que los intermediarios persistan y profundicen su política de transparencia

Durante mayo de 2021, y por primera vez en la historia de la protesta en Colombia, los problemas relacionados con el acceso y la conectividad de internet así como la moderación de contenidos y las fallas en el software de las redes sociales han sido evidentes y se han materializado gracias a que en algunos casos vimos a las empresas proveedoras de internet reconocer la importancia de proporcionar información pública sobre sus acciones.

Actuaron Movistar y Emcali, ante los reportes de corte de internet en Cali los días 4 y 5 de mayo, lo hizo Instagram tras los reportes de bloqueo de historias el 6 de mayo, nada han dicho ni Twitter, ni Facebook sobre lo que sucedió el 4 y el 18 de mayo respectivamente. Pero aunque estos ejercicios de transparencia son importantes no son generalizados, responden más a coyunturas muy concretas y, además, la información que entregan las empresas privadas no permite determinar cuál es el origen de los problemas de acceso y uso de internet durante la protesta, simplemente permiten determinar que hubo fallas. Y dado que por motivos políticos o de diseño institucional el Estado colombiano no ha determinado cual es el origen de los problemas de internet durante el paro, se crea una sensación de censura, donde lo único seguro es que hubo problemas.

En relación con la moderación en redes sociales la protesta en Colombia confirmó que es uno de los temas que más genera incertidumbre entre las personas que ni entienden lo que sucede ni reciben información sobre la forma como las plataformas deciden sobre las reglas aplicables en las redes sociales durante las protestas y se empeora con la poca información que ofrecen cuando el software falla e impacta también a las personas en momentos claves de la movilización social.

Finalmente, a pesar de la profundidad y amplitud con que la CIDH se refirió al internet en su documento de observaciones y recomendaciones a Colombia, llama la atención que no hizo ninguna mención o llamado a las empresas intermediarias para que persistan y profundicen con sus políticas de transparencia respecto a la información relacionada con la mediación y prestación del servicio de internet, llamado que la ONU y la misma CIDH ha realizado en otras ocasiones. Y, no debemos olvidar, que aún está por verse el impacto de posibles peticiones que hayan hecho las autoridades para remover contenidos o peticiones de información sobre sus personas usuarias en el marco del paro que podrían evidenciarse en los reportes de transparencia.

CONCLUSIONES Y RECOMENDACIONES

El panorama general de los derechos en el entorno digital durante el Paro Nacional es oscuro. Por un lado, existen múltiples denuncias de violaciones a los derechos humanos en los espacios digitales, sin que se evidencie interés por parte del Estado por investigar y sancionar a los responsables. Por otra lado, la opacidad relacionada con las facultades para bloquear, patrullar y señalar en internet es total. La información al respecto proveniente del Estado es nula y lo que se sabe es gracias a denuncias ciudadanas, investigaciones de organizaciones de la sociedad civil o incluso comunicados de las empresas privadas intermediarias que han asumido su deber de transparencia.

Con este opaco panorama, en la ciudadanía parece reinar una situación de indefensión ante posibles arbitrariedades cometidas por el Estado. En todo caso, estas son once recomendaciones para proteger y fomentar los derechos humanos en las manifestaciones sociales que están por venir:

1. Es necesaria la creación por parte del Estado de un mecanismo independiente que informe de forma periódica el estado de la infraestructura relacionada con las telecomunicaciones. Con el fin de permitir el escrutinio público en contextos donde la calidad del internet y el acceso al mismo sean fundamentales para proteger otros derechos.

2. Instamos al Estado, y de forma concreta a las fuerza pública, a que se comprometa a no usar inhibidores de señal durante las protestas, y a crear una política respetuosa con los derechos humanos respecto del uso y manejo transparente de este tipo de tecnología.

3. Exigimos tanto el Ministerio de Tecnologías de la Información y las Comunicaciones como la Superintendencia de Industria y Comercio no desplegar sus funciones de bloqueo de url, dominios o cualquier otro elemento de internet sin asegurarse de que sus acciones cumplen con los requisitos de legalidad, necesidad, proporcionalidad y con el debido proceso tal como lo establecen los estándares interamericanos de derechos humanos.

4. La Agencia Nacional del Espectro debe investigar las denuncias sobre interferencias (o no) de las señales durante las manifestaciones y en los lugares más neurálgicos de la protesta, mientras no se hagan cambios en la institucionalidad necesarios para proteger los derechos de la ciudadanía.

5. La Policía Nacional debe adoptar una política que permita la fácil identificación de drones y aeronaves no tripuladas que tiene en su poder. Además, debe establecer de forma clara y respetuosa de los derechos humanos protocolos para el uso transparente y democrático de estas tecnologías.

6. Es necesario que el Estado en su conjunto, pero especialmente el Ministerio de Defensa, se abstengan de participar, usar o promover narrativas que estigmaticen la protesta digital, generalizando el uso de expresiones tales como vandalismo o terrorismo digital o de señalar las denuncias ciudadanas en internet y redes sociales como noticias falsas. El Estado debe dar información que contribuya al debate público y a entender su posición como uno de los actores principales de la crisis social que enfrentamos

7. El Estado debe evaluar sus acciones de vigilancia de las comunicaciones, incluido el "ciberpatrullaje" a la luz de estándares de derechos humanos y ajustar las normas de esta actividad a los criterios de legalidad, necesidad, proporcionalidad y debido proceso. Es decir, la fuerza pública debe ajustar su accionar a los estándares de derechos humanos en todos los asuntos relacionados con tecnología y telecomunicaciones. En especial en lo relacionado con "ciberpatrullaje", "perfilamientos", "amenazas cibernéticas" y requisas a teléfonos celulares.

8. Es imperativo que el Estado además de regular el uso de fuerza y las armas en la protesta, adecue a los estándares de derechos humanos la reglamentación interna sobre tecnología que se usa para controlar la protesta social. Estos son los casos, por ejemplo, de los inhibidores de señales y las cámaras de reconocimiento facial, tecnología en poder del Estado y la cual se sospecha ha sido utilizada.

9. Hacemos un llamado al Estado para que adelante las reforma legislativas necesarias para ajustar su institucionalidad de modo que se garantice un regulador del sector de comunicaciones independiente y autónomo; con funciones de vigilancia y control de la infraestructura (internet y espectro) y que pueda hacer pública información suficiente para garantizar el escrutinio público.

10. Es necesario que todas las entidades estatales, pero especialmente aquellas con funciones de defensa o promoción de los derechos fundamentales, analicen el impacto que tiene la tecnología en el ejercicio de derechos de la ciudadanía antes de presentar políticas o hacer propuestas respecto al control y manejo de protesta social.

11. Solicitamos a las empresas proveedoras e intermediarias de internet que en ejercicio de su responsabilidad con las personas que usan sus servicios y en desarrollo del principio de neutralidad de la red analicen toda solicitud de bloqueo o interferencia a la luz de los estándares de derechos humanos.

12. En el mismo sentido, pedimos a las plataformas responsables de las redes sociales transparencia sobre: 1) los criterios de moderación de contenidos que usan sobre todo cuando pueden afectar la protesta y garantizar mecanismos efectivos de apelación, 2) la información sobre medidas usadas para escalar sus respuestas en moderación de contenidos derivadas del repentino incremento en uso de estas plataformas durante las protestas y 3) sobre las fallas en sus infraestructuras, aplicaciones o software, indicando origen y naturaleza, además de impacto a la protesta y las medidas que se adoptan para mitigar y evitar que vuelvan a suceder.

PISTOLAS contra CELULARES

Fundación Karisma