Fundación Karisma

Respetable señora
Irene Khan
Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión
Organización de Naciones Unidas

Asunto. Desafíos a la libertad de opinión y expresión en tiempos de conflictos y disturbios

Introducción

La Fundación Karisma es una organización de la sociedad civil colombiana que busca asegurar que las tecnologías digitales protejan y avancen los derechos humanos fundamentales y promuevan la justicia social. Realiza actividades de estudio, análisis, capacitación y acciones para reconocer las oportunidades y enfrentar los desafíos que plantean los entornos digitales a través de un trabajo estructurado basado en cuatro líneas temáticas: democratización del conocimiento y la cultura, participación cívica, autonomía e inclusión social, además contamos con dos laboratorios que trabajan transversalmente en temas específicos, el K+LAB, nuestro laboratorio de Privacidad y seguridad digital y el laboratorio de apropiación tecnológica.

En este escrito queremos llamar la atención de la Relatoría sobre las regulaciones y prácticas del gobierno durante momentos de agitación social, como las protestas sociales. Durante las jornadas de 2021 pudimos evidenciar varias actuaciones que pueden afectar los derechos a la libertad de expresión, de información, de asociación y de participación política como a) la interferencia del servicio de internet, b) el monitoreo de internet, el perfilamiento de personas y la judicialización por conductas de desinformación por parte del Estado y c) la formulación de normas que dificultan el ejercicio del derecho a protestar. La mayor parte de la información resumida en este escrito se encuentra en el informe Pistolas vs. Celulares.

a) Posibles interferencias estatales en el servicio de internet

En Colombia no existe una institucionalidad que garantice el derecho al acceso a internet y que investigue las intromisiones a tal derecho. A ello se suma que la fuerza pública tiene facultades para inhibir las señales de internet sin rendir cuentas sobre sus actuaciones. Su presencia reiterada en zonas donde se han presentado bloqueos e interrupciones durante protestas, deja en el aire una sensación de desprotección y falta de garantías para los derechos humanos en entornos digitales en el marco de situaciones de agitación social.

Fundación Karisma

Entre abril y junio de 2021 tuvo lugar un movimiento masivo de protesta ciudadana en Colombia conocido como el paro nacional. 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.

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, 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.

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.

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 internet, en su comunicado Internet disrupted in Colombia amid anti-government protests 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.

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 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 la ciudad y una empresa prestadora del servicio reportó problemas de conexión en la red fija de internet. 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.

Al respecto, el Gobierno nacional señaló que el único reporte que habían recibido el 4 de mayo era por daños a la infraestructura. Y agregó que no avalaría cortes del servicio de internet. También denunció “actos vandálicos” que impidieron reparar los daños ocasionados.

Fundación Karisma

Uno de los factores que genera más dudas 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. 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.

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 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 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.

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 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. 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.

Fundación Karisma

b) Monitoreo de internet, perfilamiento de personas y la judicialización por conductas de desinformación por parte del Estado

> *En Colombia se ha estigmatizado la protesta social. La fuerza pública ha iniciado labores de monitoreo de internet bajo la facultad de ciberpatrullaje para la prevención de delitos. Ha emprendido campañas para disminuir las noticias falsas, emitiendo juicios públicos y judicializando a personas que desafían la narrativa oficial, desconociendo el derecho a la libertad de expresión. Para el mismo fin, la fuerza pública fingió un ciberataque. También ha aprovechado la tecnología para recopilar masivamente información y para perfilar personas que considera sospechosas.*

La criminalización de la protesta social ha sido una constante en Colombia durante las últimas décadas. No obstante, con la irrupción de las tecnologías de las telecomunicaciones, surgió la protesta digital y el panorama cambió. Internet es un espacio que propicia e impulsa el ejercicio de la protesta. Para poder abordarlo, en las jornadas de protesta, la fuerza pública realizó ejercicios de ciberpatrullaje.

En 2015 con la expedición de la Resolución 5839 de la Policía Nacional, 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". 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.

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 del Ministerio de Defensa 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. 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.

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". 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 cumpliendo estándares de derechos humanos.

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, otra forma de entender o posible dimensión del ciberpatrullaje es como el monitoreo de páginas, perfiles y redes sociales con el fin de rastrear noticias falsas.

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. 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".

En el informe mencionado, la fuerza pública 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".

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.

Además, la Fundación para la Libertad de Prensa (FLIP) denunció que el Ministerio de Defensa y las fuerzas armadas, durante el paro, iniciaron una campaña para atacar a quienes los critican y cuestionan, fingiendo un ciberataque:

> "El 6 de mayo, las redes sociales y la página web del Ministerio de Defensa y otras entidades adscritas amanecieron vestidas de negro. El último mensaje que aparecía en sus redes era: "Intento de bloqueo". Parecía un ciberataque. De las 6 a las 9 de la mañana, ningún funcionario estaba autorizado para atender a periodistas ni medios de comunicación. A las 9, las redes se restablecieron y comenzó la campaña "La verdad en un mar de mentiras #ColombiaEsMiVerdad". Se publicó un video en el que una voz en off decía "nos intentan bloquear, pero nosotros seguimos de pie". Luego, el ministro de Defensa Diego Molano y los comandantes de todas las fuerzas militares mencionaron algunas noticias que, a su juicio, consideraron falsas y recalcaron el valor de su trabajo en la protección de los colombianos. En el video se omitió, por completo, la aclaración de que nunca hubo un ciberataque real y que todo este espectáculo hacía parte de su estrategia para llamar la atención de la ciudadanía."

Hacen parte de dicha campaña de imagen, el Boletín de Fake News de la Policía Nacional o las publicaciones hechas el 13 de mayo por la policía y el 19 de mayo por el ejército 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". 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. 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". 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.

Resulta preocupante que el Ministerio de Defensa afirmó que la fuerza pública tiene atribuciones para indicar si "rumores a través de redes sociales que fomenten violencia o mientan sobre acciones de la fuerza pública" configuran o no terrorismo digital. Luego, también afirma que "sobre campañas de desinformación que generan una denuncia por adecuarse a tipologías penales, se le informa directamente a la Fiscalía General de la Nación". Y la Fiscalía, por su parte, advierte que estas noticias falsas pueden configurar el delito de calumnia.

La criminalización de las voces críticas institucionaliza un discurso de estigmatización y censura contra quienes denuncian irregularidades en las instituciones, al señalar esta información como falsa.

A ello se suma la preocupación porque el Ejército Nacional utiliza sus recursos para perfilar e identificar a líderes, ciudadanos y periodistas, recolectando y conservando datos personales sensibles de quienes consideran críticos. El Informe del Sector Defensa que hemos mencionado muestra que el ciberpatrullaje también sirvió para controlar la protesta en el mundo físico. Menciona que se realizaron 3.420 alertas preventivas anticipando actos de vandalismo, que analizaron 3.723 videos 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.

Estos episodios recuerdan los antecedentes de chuzadas y perfilamientos en Colombia, que siguen latentes: En 2020 la policía intentó adquirir el "sistema de ciberinteligencia basado en inteligencia artificial" y finalmente adquirió en julio de 2021 con el fin de realizar monitorear sitios web, redes sociales, TOR, I2p, Freenet y sistemas de mensajería instantánea como Telegram. 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.

c) Formulación de normas que dificultan el ejercicio del derecho a protestar

Fundación Karisma

> *En Colombia, en respuesta a las jornadas de protesta, se tramitó en el Congreso una norma que buscó limitarla de forma implícita: criminalizando los elementos que permiten conservar el anonimato, aumentando las penas de todas las conductas cometidas a través del internet y autorizando a la fuerza pública a acceder a las grabaciones de cámaras privadas sin necesidad de orden judicial previa.*

El 25 de enero de 2022, el Congreso promulgó la Ley 2197 de 2022 "tendiente al fortalecimiento de la seguridad ciudadana". La nueva ley de seguridad ciudadana es una respuesta desde el legislativo a la movilización social de 2021. Sin embargo, no tiene en cuenta las recomendaciones de la CIDH, respecto a no estigmatizar a los manifestantes.

Para empezar, en el artículo 7 de la Ley 2197 se agregó como una circunstancia de mayor punibilidad la realización de las conductas punibles cuando "se utilicen medios informáticos, electrónicos o telemáticos". Dicha norma representa un riesgo por dos razones: por un lado, la norma representa una doble tipificación respecto de los delitos informáticos y, por otro lado, al aplicarse a todo tipo de delitos aumenta las penas para los tipos de injuria, calumnia o instigación a delinquir. Estos últimos fueron utilizados para judicializar a personas que participaron de las movilizaciones en redes sociales.

También preocupa el artículo 16 de la ley de seguridad que agregue artículo 353B al Código Penal. La nueva norma establece como agravantes para el delito de *obstrucción a vías públicas que afecten el orden público (artículo 253 Código Penal)* el uso de "máscaras o elementos similares que sirvan para ocultar la identidad o la dificulten". Esto desconoce los parámetros interamericanos sobre libertad de expresión y anonimato, lo que promueve la censura y desincentiva la participación ciudadana. Además, pasa por alto lo dicho por la Corte Constitucional colombiana al revisar la constitucionalidad del artículo al decir que la norma no debía ser ampliada de forma tal que se impida ejercer el derecho a la protesta social.