Imprimir

El 29 de octubre la Fundación para la Libertad de Prensa (FLIP) publicó el articulo *"Los jueces de la verdad, el mar de mentiras detrás del ciberpatrullaje del Estado"*, acompañado de un conjunto de piezas gráficas y mensajes que tuvieron como centro sus redes sociales. En estas se denunciaban las irregularidades que afirman existen en las estrategias de ciberseguridad realizadas entre mediados de abril y mayo en el marco del Paro Nacional.
La polémica se ha suscitado teniendo como centro un contrato firmado por el Ministerio de Defensa con la empresa Alotrópico SAS por $ 898'450.000, el cual tenía como objeto la gestión de la implementación de la metodología *"Transformar Comunicando"* –para el Ministro no es un contrato específico sino un contrato de asesoría al Ministerio de duración de nueve meses–. Sin embargo, la polémica no se reduce a dicho contrato, sino que se profundiza y tiene redes que afectan el entramado institucional del Ministerio de Defensa.

La investigación de la FLIP es fundamental porque permitiría establecer problemas actuales en cuanto a la libertad de expresión en redes sociales –un tema, sin duda novedoso- y la manera como el Estado ha venido actuando al respecto.

Las cuestiones de forma del contrato: ¿MinDefensa y preferencias en la contratación?

Inicialmente, llama la atención respecto al polémico contrato, que desde abril del presente año se tenían cuestionamientos respecto a la implementación de éste, dado que se consideraba que había arreglos predeterminados en cuanto a la consecución del mismo -lo cual parecía incluir favoritismos y una implementación amplia de recursos-.

De lo señalado respecto al contrato se debe hacer referencia a la agencia Alotrópico, al frente de las cual aparecen nombres de dos exfuncionarias que, al parecer trabajaron con el Ministro de Defensa, cuando éste se encontraba en la dirección del Instituto Colombiano de Bienestar Familiar.

Después de su paso por el sector público han tenido contratos millonarios con entidades del gobierno. Asimismo, existen sospechas de que el contrato se habría firmado el mismo día en

el que fue presentada la propuesta, siendo entonces contratados de manera directa, sin evidenciar las competencias para mejorar la percepción ciudadana de la cartera y la "*protección de los imaginarios (…) en relación con los temas relacionados con la seguridad y defensa del Estado*". Además de que dicha agencia habría obtenido un contrato -según el Portal de Transparencia Económica y el Secop- Publicado en un artículo de Infobae- con el DAPRE en el momento que el actual Mindefensa fue su director.

Estos aspectos colocan interrogantes y cuestionamientos respecto al contrato llevado a cabo por el Ministerio de Defensa, por lo que algunos sectores demandan una especie de "investigación exprés" que permita esclarecer los hechos ocurridos en la implementación de dichos recursos.

El contrato del Ministerio de Defensa y sus limitantes estructurales

El contrato señala que la estrategia "*Transformar Comunicando*" buscaba permitir "*la mayor comprensión por parte de la ciudadanía de los temas relacionados con la defensa y seguridad nacional, con comunicación asertiva, que parta de la escucha activa de la percepción ciudadana, encontrando oportunidades que potencialicen impactos positivos a partir de las herramientas institucionales existentes, buscando fortalecimiento institucional e impulso de procesos estratégicos*". No obstante, según los comunicados de la FLIP y derivado de los sucesos ocurridos en medio del paro nacional, se puede encontrar que:

- Primero, la relación que se establece respecto a la percepción ciudadana no se desarrollo de manera amplia, ni tuvo las repercusiones que se esperaban. Dentro de la institución es difícil atender a discursos disidentes a los que se encuentran establecidos bajo el mismo carácter que implica el pensamiento de cuerpo.
- Segundo, los impactos positivos llevados a cabo por medio de las herramientas que dispone el Ministerio no permitían salir de las formas y pensamientos que significan un apoyo para las instituciones de la cartera.
  Esto mostraría que existen limitaciones estructurales dentro del mismo contrato que llevaban a que la estrategia principal estuviera destinada a encontrarse condicionada.

Del mismo modo, el contrato -y, como tal, la estrategia de comunicación desarrollada durante el Paro Nacional- se enmarca en la concepción institucional de que existe un método premeditado de estrategia de desprestigio sistemática contra la Fuerza Pública. Esto lleva a una particular y cuestionable percepción: partir de la existencia de un enemigo al cual hay que hacer frente, al encontrar una respuesta reactiva y basada en un impulso, antes que en la búsqueda de informar a la ciudadanía.

La realidad es que al interior del Paro Nacional no es fácil hablar de que hubo una campaña de desprestigio contra la Fuerza Pública o la cartera de Defensa. Empero, si se intento crear la concepción de que existía dicha estrategia -un enemigo- desde los mismos pronunciamientos del Ministerio -aspecto ratificado por el informe de la FLIP-, cuando en realidad en su gran mayoría se trataba de ciudadanos –especialmente jóvenes- que cuestionaban el actuar de la Fuerza Pública, muchos basados en vídeos grabados por la misma sociedad civil.

La estrategia de Bloqueo y la Campaña de #ColombiaEsMiVerdad

La denuncia más grave que ha hecho la FLIP se da para el 6 de mayo, día en el cual se presenta un aparente autosabotaje a partir de un “ciberataque”, en el que amanecieron las páginas del Ministerio de Defensa y otras entidades adscritas con fondo negro y un mensaje que afirmaba un “Intento de Bloqueo”. Se reporta adicional a ello que entre las seis y las nueve de la mañana no se encontraban autorizados los funcionarios a atender ningún periodista ni medio de comunicación. A las nueve se restablecieron las páginas y comenzó la campaña #ColombiaEsMiVerdad, en la cual se planteaba que el Ministerio había sido víctima de lo ocurrido -intento de bloqueos- y se mostraron noticias falsas, sin aclarar que el sabotaje fue realizado por la misma institucionalidad.

Lo preocupante es la desinformación que se genera en la ciudadanía en general respecto a los sucesos ocurridos. Asimismo, esta situación crea un aparente enemigo con capacidades que realmente no se encuentra en el campo de la ciberseguridad como una amenaza. Al contrario, las noticias falsas que se reflejaron se presentan como generadas dentro de la

misma ciudadanía, poniendo a esta como la causante de las mimas.

Llama la atención que el Ministerio de Defensa no ha desmentido la existencia de la simulación de un ciberataque, por el contrario, lo ratifica bajo un modelo de "campaña pedagógica" que buscaba llamar la atención de la comunidad. [1]Esto se compaginaba con el vídeo que iniciaría #ColombiaEsMiVerdad, en el cual se buscaba mostrar a la comunidad las noticias falsas que debilitan la legitimidad de las Fuerzas Militares.

Además de paradójico, es poco responsable considerar que, a partir de una información mentirosa a la ciudadanía -la existencia de un intento de Bloqueo-, se intentara generar toda una lucha contra las noticias falsas. Hay una pérdida del propósito de la campaña y del carácter que deben tener las instituciones de seguridad en Colombia. No se debe buscar la sensación de seguridad en la comunidad a partir de campañas que reflejan la inseguridad cibernética.

Al respecto, en los señalamientos de la página oficial del Comando General de las Fuerzas Militares sobre la campaña "Colombia Es Mi Verdad" se anota: "*Minutos después de subir los mensajes del supuesto intento de bloqueo, 3 colectivos de hackers se atribuyeron el hecho. De esta manera se evidencia la sistematicidad en los ataques cibernéticos que están sufriendo las instituciones de defensa. Además, se evidenció que los numerales que eran propuestos para dialogar en redes de manera transparente, fueron objeto de ataques a través de la manipulación y la ridiculización de estos numerales, subiendo información de grupos de pop koreanos. Este ataque conocido como K-Pop consiste en que un grupo de personas, y quizás bots también, enfilan sus esfuerzos a detectar posibles numerales que sean positivos para el gobierno y convertirlos en tendencia, antes que las instituciones, pero llenos de contenido referente a bandas de pop koreanas*".

En cuanto a la anterior información es necesario hacer varias anotaciones:

1. Se justifica el autosabotaje a partir de la demostración de que sí hay un intento de ataques cibernéticos por parte de grupos de hackers. Nuevamente, una situación contradictoria en el

entendido que el Ministerio de Defensa y sus cuerpos adjuntos deben procurar por la seguridad de los colombianos, no generar campañas en las que parezca generar más sensación de riesgo institucional.

2. Preocupa que manifestaciones ciudadanas como las expresiones hechas con mensajes de K-pop sean tomadas como ataques por parte de las Fuerzas Militares. Aquí se genera una clara delimitación de que esta forma de protesta en redes contra mensajes positivos al gobierno y las instituciones es tachada de manipuladora, lo cual vuelve y pone en contexto la preocupación por la libertad de expresión en el país.
   Este tipo de acciones ciudadanas no deberían ser tomadas como ataques, buena parte del ejercicio de la ciudadanía consiste en expresar ideas de maneras diversas sin necesidad de que la institucionalidad las considere lesivas a sus propios intereses, las limite o las tache de ataque. En este punto se presenta una de las más delicadas acusaciones por parte de la FLIP, la cual señala que, a partir de este autosabotaje, se justifica la existencia de ciberpatrullajes contra las “Noticias Falsas”.

Los problemas de control de las estrategias del Ministerio de Defensa

Según el informe de la FLIP, en medio de la estrategia se creó un PMU-Ciber, el cual se encargaba de las noticias falsas. Este se encontraba conformado por: El Centro Cibernético Policial (CCP), el ColCERT (Grupo de Respuesta a emergencias cibernéticas), el MinTIC, la Dirección Nacional de Inteligencia (DNI), el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), Comando Conjunto Cibernético de las Fuerzas Militares (CCOC) y la Fiscalía. Sin embargo, existen contradicciones en cuanto a la forma de actuar de cada una de estas instituciones, sus objetivos y la manera como llevan a cabo sus tareas.

La existencia de dicho Grupo Cibernético no se encuentra claramente delimitada, no tiene reglamentos ni manuales de funcionamiento estrictos y restringidos, así como tampoco información clara respecto a sus labores. A lo anterior se complementa que no existe un contrapeso institucional demarcado que permita un control efectivo a esta serie de dinámicas. Según la FLIP se han invertido más de 21.000 horas de las Fuerzas Militares y el Ministerio de Defensa que no han tenido una correlación con un estudio de estas acciones

emprendidas.

Esto tiene aún mayor relevancia cuando se pone en contexto la preocupación sobre el abordaje de las noticias falsas, dado que se considera que muchos de los contenidos que son objeto de dicho examen no es porque su información sea contraria a la verdad, sino porque se encuentra en desacuerdo con las acciones emprendidas por las instituciones estatales en medio del paro. Al respecto, la FLIP tiene razón al preguntarse sobre los efectos que tiene en la prensa y en la ciudadanía en general, por el temor a represalias ante la capacidad con la que cuenta el Ministerio.

Conclusiones: Una mirada necesaria a la libertad de expresión en el medio virtual

Para los militares en el siglo XXI está claro que es necesaria la ciberseguridad ante los avances tecnológicos, convirtiéndose lo virtual en un campo de disputa con los diversos actores del entorno internacional, el cual debe ser reconocido por los Estados y protegido a partir de sus intereses vitales. No obstante, en el presente caso se crea la disyuntiva del uso de lo cibernético como herramienta de protesta social, cuyos repertorios aún no han sido delimitados y continúan en plena expansión. No hay una claridad respecto a los alcances que se puede tener en estos espacios ni las repercusiones que se darán en el mundo real.

En ese orden de ideas, lo primero es encontrar a la protesta social en estos nuevos espacios delimitados, con el objetivo de que no sea criminalizada. Entender las representaciones sociales hoy en día implica un reconocimiento de formas de manifestarse que se verán en crecimiento en los próximos años y que, por la plataforma que utilizan, no deberían ser juzgadas de inadecuadas o someterse a control de acuerdo con su afectación a la legitimidad de las instituciones.

Segundo, hay un acuerdo en que se debe ejercer -con ayuda de las plataformas- un control a las noticias falsas. No obstante, este debe elaborarse por medio de un acompañamiento ciudadano, ONG’s, instituciones judiciales, instituciones civiles del gobierno, universidades, medios de comunicación, entre otros; mas no a partir de una campaña reactiva en contra de

muchas de las opiniones o mecanismos de protesta virtual de la ciudadanía. Al respecto, es preocupante que las Fuerzas Militares señalen como “ataque” algunas de esas expresiones, ratificando los argumentos dados por la FLIP.

Tercero, es necesario fijar protocolos, instituciones y líneas de control en correlación a la manera como se viene tratando el tema de la ciberseguridad en el país en cuanto a la ciudadanía y sus manifestaciones. Las revelaciones de la FLIP son en extremo preocupantes ante la posibilidad de que se vea afectado el derecho a la libertad de expresión y todas las implicaciones que, en el ámbito de la democracia, esto conlleva.

---

[1] En unas declaraciones publicadas en El Tiempo en Noviembre 3/2021, “*Molano afirmó que nunca se dijo que la campaña, que incluyó poner un fondo negro y la frase “intento de bloqueo” en varias de sus páginas, fuera un ciberataque… Lo que está claro es que la campaña se activó con una frase que decía ‘intento de bloqueo’ para hacer la activación de la campaña, pero nunca se interrumpieron los servicios, nunca se dijo que era un ciberataque y lo que se buscaba era llamar la atención para poder hablar sobre las noticias falsas. Esas dos semanas no solo tuvimos ataques y vandalismos en las calles, sino que también se registró la publicación de hechos falsos, y se necesitaba ser contundentes para enfrentar esas informaciones falsas*.”

Alejo Vargas Velásquez, Profesor Titular de la Universidad Nacional y director del Grupo de Investigación en Seguridad y Defensa

Farid Camilo Rondón Raigoza, Politólogo y estudiante de la maestría en Estudios Políticos de la Universidad Nacional, y miembro del Grupo de Investigación en Seguridad y Defensa

Foto tomada de: wradio.com