Perfilamiento en redes sociales y ciberpatrullaje como nuevas modalidades de la vigilancia masiva desplegada por los Estados: casos relevantes en América Latina

Contribución de Derechos Digitales para la consulta "sobre tecnologías de vigilancia digital y derechos humanos" emprendida por la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH)

Agosto, 2024

Sobre Derechos Digitales

Derechos Digitales[1] es una organización regional latinoamericana sin fines de lucro fundada en 2005, que se dedica a la defensa y promoción de derechos humanos en el entorno digital para contribuir con sociedades más justas, inclusivas e igualitarias. Sus acciones combinan investigación, incidencia en políticas públicas y privadas, análisis de tecnologías, campañas y formación en los derechos digitales y la seguridad digital, entre otros.

Elaborado por: Lucía Camacho G., coordinadora de políticas públicas en Derechos Digitales. Contacto: lucia.camacho@derechosdigitales.org

[1] https://www.derechosdigitales.org/

Índice

Introducción

En los últimos años distintos gobiernos de América Latina han desplegado prácticas de monitoreo del discurso en línea de la ciudadanía. Del trabajo que realiza la organización en la temática, hemos identificado al menos dos finalidades que emergen como una *nueva tendencia en la vigilancia masiva e indiscriminada* que se despliega en internet: *los perfilamientos en línea*, y el *ciberpatrullaje*.

Si bien en latinoamérica no hay definiciones unánimes sobre la naturaleza del perfilamiento y el ciberpatrullaje, en la práctica ambas sirven a fines estatales diferenciados. La primera, a la identificación en línea de personas afines así como opositoras del gobierno, y la segunda, a la identificación y persecución de personas fruto de su actividad en internet.

En breve, tanto el ciberpatrullaje como los perfilamientos constituyen nuevas modalidades de la vigilancia masiva desplegada por el Estado porque:

- Implican un monitoreo generalizado del discurso de las personas, y de las personas, sus interacciones en línea, sus familiares y contactos.
- El monitoreo desplegado por ambas actividades es imperceptible o indetectable para las personas usuarias de internet.[2] En ocasiones también es encubierto.[3]
- Ambas prácticas significan una limitación extraordinaria del derecho a la libertad de expresión en línea, a la expectativa de privacidad en internet y la privacidad en entornos de comunicación o interacción privada entre las personas.
- A su vez, la falta de información sobre dichas actividades impide que las personas monitoreadas puedan ejercer alguna acción de reclamo y cese de aquellas lo cual tiene efectos en el derecho a acceso a la justicia.
- El monitoreo recae sobre las personas usuarias de internet que tienen una vida activa en línea; su implementación no está sujeta a la identificación de personas de interés vinculados con causas judicialmente activas, aunque tanto los perfilamientos como el

[2] Esto es así en buena medida por la forma en que están configuradas las principales plataformas de redes sociales donde ocurre este monitoreo y donde la visualización de las publicaciones dentro o fuera de la red social no es notificada o informada a las personas usuarias de las mismas salvo que haya una interacción directa a través de un "me gusta", un comentario o "retuit".

[3] Esto sucede principalmente en las plataformas donde, para visualizar las publicaciones o contenidos generados por los usuarios se precisa tener una cuenta de usuario. Esto obliga a que los agentes del Estado que emprenden el monitoreo creen una cuenta destinada a dicho fin con la cual navegar en línea. Para ello, la identidad y contenidos afiliados a esa cuenta, que son ficticios en general, le permiten al agente estatal pasar desapercibido por los otros usuarios de la plataforma, al tiempo que esto le facilita navegar, seguir o interactuar con los contenidos, publicaciones e interacciones de las personas activas en dicha plataforma.
Este es el caso particular de la red social X, que fruto de actualizaciones emprendidas a partir de 2023 para bloquear el *scraping,* cerró al público no usuario de la red social la visualización de las publicaciones y contenidos que circulan en dicha plataforma, lo que obligó a los agentes del Estado interesados en monitorear lo que sucede en dicha red social, a crear cuentas ficticias para navegar los contenidos y seguir de cerca a los usuarios de la red social que son los objetivos de estas prácticas. Ver: Social Media Today (2023). Twitter Updates Viewing Restrictions, Allowing Tweets to Appear in Google Search Agai N°En: https://www.socialmediatoday.com/news/twitter-updates-viewing-restrictions-allowing-tweets-appear-google/685070/#:~:text=Last%20Friday%2C%20as%20part%20of,log%2Din%20to%20the%20app.

ciberpatrullaje pueden potencialmente derivar en la apertura de causas judiciales fruto de la interacción en línea de las personas objetivo de esta tarea.

Los perfilamientos y el ciberpatrullaje merecen la atención de la Relatoría Especial para la Libertad de Expresión RELE, y la Comisión Interamericana de Derechos Humanos CIDH pues ambas constituyen una nueva amenaza para el ejercicio de los derechos humanos en línea, incluidos la libertad de expresión, la privacidad y la protección de datos.

En este informe, presentamos los casos más representativos en la América Latina (en adelante LATAM) en donde se han desplegado casos de perfilamientos y ciberpatrullaje, y al final presentamos recomendaciones para ser sugeridas a los Estados, así como a otros actores.

El objetivo del informe es responder a las preguntas elevadas en la consulta[4] sobre casos de incidentes de uso de tecnologías de vigilancia estatal y sobre las prácticas de transparencia aplicadas en su despliegue (preguntas 1 y 4) así como información adicional sobre nuevas modalidades de vigilancia masiva (pregunta 6).

1. El uso de OSINT y SOCMINT en el marco de los perfilamientos y el ciberpatrullaje

La inteligencia en fuentes abiertas (OSINT por sus siglas en inglés) y la inteligencia en redes sociales (SOCMINT) son empleadas en el marco de los perfilamientos y el ciberpatrullaje desplegado por los Estados de LATAM. Su uso, especialmente cuando se orienta a fines de la protección de la seguridad ciudadana o la seguridad nacional, requiere aplicar una perspectiva de derechos humanos.

La inteligencia en fuentes abiertas (OSINT) es, al tiempo, una metodología, una técnica, y una tecnología que pueden ser aplicables a la obtención de información accionable extraída de la visualización, recolección y procesamiento de fuentes de información en línea que, en principio, no está restringida por leyes de privacidad o derechos de autor.[5]

La inteligencia en redes sociales (SOCMINT) –como un subtipo de la información en fuentes abiertas— se enfoca particularmente en la consulta, acceso, uso y procesamiento de la información personal publicada por las personas en sus cuentas de redes sociales, y que tiene un gran valor por el detalle de información estratégica que aportan sobre redes de contacto sobre la persona de interés, su geolocalización, hábitos y temas de interés, entre otros.[6]

[4] Comisión Interamericana de Derechos Humanos (2024). Cuestionario de Consulta sobre tecnologías de vigilancia digital y derechos humanos. En: https://www.oas.org/es/cidh/jsForm/?File=%2Fes%2Fcidh%2Finformes%2Fcuestionarios.asp&Q=58
[5] Camacho Gutiérrez, L.; Ospina Celis, D.; Upegui Mejía, J.C. (2022). Inteligencia estatal en internet y redes sociales: el caso colombiano. Dejusticia. En:https://www.dejusticia.org/wp-content/uploads/2022/12/InteligenciaEstatalEnInternet-Web-Dic23.pdf ver página 8
[6] Camacho Gutiérrez, L.; Ospina Celis, D.; Upegui Mejía, J.C. (2022). Inteligencia estatal en internet y redes sociales: el caso colombiano. Dejusticia. En:https://www.dejusticia.org/wp-content/uploads/2022/12/InteligenciaEstatalEnInternet-Web-Dic23.pdf

La aplicación de la perspectiva de los derechos humanos a estas dos prácticas cuando son desplegadas por los Estados en el marco de los perfilamientos o el ciberpatrullaje debe empezar por "disolver la narrativa según la cual la posibilidad de encontrar y acceder a información personal en línea permite a los cuerpos de inteligencia [de la policía o de otros organismos] hacer con ella prácticamente cualquier cosa".[7]

Tal y como lo sostiene un informe publicado por Dejusticia sobre este asunto, la "información disponible en línea no pierde, por su publicación, su naturaleza de información privada o sensible".[8] Aun así, en los casos que exploraremos en este informe, las autoridades que despliegan perfilamientos y ciberpatrullaje en línea parecen despreciar cualquier distinción sobre la naturaleza de la información abierta o cerrada en línea, al tiempo que difumina la expectativa de privacidad de las personas en internet.

En el marco de este informe, entendemos tanto al ***perfilamiento* como el *ciberpatrullaje* como *parte de una misma dinámica operativa que erosiona los derechos en línea y que instalan una nueva modalidad de la vigilancia masiva estatal***, donde la única distinción entre una y otra son, en esencia, las sanciones jurídicamente relevantes que puede imponerse a la persona objetivo de la vigilancia en línea del Estado –en el caso del ciberpatrullaje--.

En ambas subyace una visión según la cual no hay entornos privados en línea y en la que cualquier información disponible en internet es posible de ser explotada por el Estado para fines que no superan los *tests* de los criterios reconocidos internacionalmente de necesidad, proporcionalidad o razonabilidad, mucho menos el requisito de legalidad. Asimismo, se trata de dos prácticas que –contrario a la presunción de inocencia- ponen a las personas en un estado de sospecha continua por su sola interacción en internet, lo que las convierte en objetivos potenciales de la vigilancia del Estado y, por tanto, ser sujetas a un proceso penal.

2. El perfilamiento de personas usuarias de las redes sociales

De los casos analizados en Latinoamérica, se identifica que el perfilamiento de usuarios de cuentas de redes sociales se ha desplegado por gobiernos de LATAM con dos fines en particular:

- Caracterizar a las personas en razón a su opinión crítica o favorable frente al gobierno como una vía para medir el nivel de aceptación de las políticas públicas, cuidar la imagen institucional y posicionar al gobierno y sus autoridades en redes sociales, e
- Identificar los contenidos catalogados como desinformación y los usuarios que realizan dicha acción, en especial, en contextos socialmente sensibles como la protesta social o la pandemia.

[7] Camacho Gutiérrez, L.; Ospina Celis, D.; Upegui Mejía, J.C. (2022). Inteligencia estatal en internet y redes sociales: el caso colombiano. Dejusticia. En:https://www.dejusticia.org/wp-content/uploads/2022/12/InteligenciaEstatalEnInternet-Web-Dic23.pdf ver página 10

[8] Camacho Gutiérrez, L.; Ospina Celis, D.; Upegui Mejía, J.C. (2022). Inteligencia estatal en internet y redes sociales: el caso colombiano. Dejusticia. En:https://www.dejusticia.org/wp-content/uploads/2022/12/InteligenciaEstatalEnInternet-Web-Dic23.pdf ver página 10

La primera finalidad genera distintos riesgos para los derechos humanos de las personas objeto de perfilamiento. En materia de ***libertad de expresión***, por ejemplo, puede acarrear el silenciamiento y autocensura de las personas que han sido o creen estar siendo objetivos de las tareas de perfilamiento estatal; e incluso cuando los listados de personas "opositoras" o "negativas" frente al gobierno son publicadas o filtradas, las expone a eventuales actos de incitación a la violencia o acoso en línea en su contra; y la estigmatización fruto de una opinión manifestada en línea.

En ***materia de privacidad***, la caracterización de personas significa el despliegue de una intensiva recolección de información personal disponible en línea que permitan la identificación plena de la persona, así como la conformación de bases de datos sin importar la fuente de dicha información, si su uso está autorizado o no por su titular, entre otros.

Ambos riesgos se encuentran aunados a un efecto perjudicial para la salud de las democracias donde la caracterización de personas críticas o favorables al gobierno puede erosionar el debate público en la esfera digital, y con ello, la riqueza de opiniones que nutren y fortalecen a los ámbitos democráticos y solidifican los Estados de Derecho.

La segunda finalidad, desplegada también por organismos oficiales, y en especial, por organismos administrativos afiliados a las oficinas de presidencia de los países –incluyendo en algunos casos en LATAM a los cuerpos de policía– genera distintos efectos igualmente críticos en materia de derechos humanos.

Los gobiernos podrían emplear los informes sobre los contenidos catalogados como desinformación y sobre los usuarios identificados como presuntos propagadores de la desinformación, en herramientas para deslegitimar pedidos sociales legítimos o en mecanismos de estigmatización de medios de comunicación o usuarios de internet. Es más, los perfilamientos pueden escalar al punto que permite a las autoridades que lo despliegan alertar a aquellas otras de investigación criminal para la persecución en materia penal de las personas que presuntamente desinforman.[9]

Esto, sin mencionar que estas prácticas no se encuentran reguladas pero se despliegan como fruto de la interpretación arbitraria de ciertas facultades administrativas que habilitan a las autoridades a monitorear el ciclo de las políticas públicas o prevenir el crimen –y que se aplica también a la detección temprana de crímenes que pueden tener lugar por la actividad de quienes presuntamente desinforman–. Este es un escenario que, sin duda, genera "inseguridad jurídica y [un] efecto amedrentador, lo que dificulta que las personas utilicen internet para ejercer sus derechos".[10]

---

[9] Lara-Castro, P. (2023). When protection becomes an excuse for criminalisation: Gender considerations on cybercrime frameworks. Derechos Digitales. En: https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf

[10] Consejo de Derechos Humanos, Informe del Relator Especial sobre los Derechos a la libertad de Reunión Pacífica y de Asociación (17 de mayo, 2019). A/HRC/41/41, párrafo 32. En:https://documents.un.org/doc/undoc/gen/g19/141/05/pdf/g1914105.pdf

Ahora bien, el perfilamiento de los usuarios y su actividad y discurso en línea pueden ejecutarlo las autoridades de manera manual[11] o automatizada.[12] En cualquier caso, subyace una visión estatal preocupante según la cual todos los contenidos que circulan en internet, y en particular, en las redes sociales, son públicos y abiertos, lo que se traduce en que las autoridades puedan emplearlos para fines completamente ajenos a aquellos que motivaron a los usuarios de internet a interactuar en línea, como el intercambio libre de sus ideas y opiniones.

Este perfilamiento, además, sucede en condiciones de opacidad. Las autoridades que lo despliegan no informan de manera activa, suficiente y clara sobre los límites, alcances y objetivo de la actividad como tal –en ocasiones, ni siquiera reconocen que se trata de un perfilamiento sino que lo identifican como una inocua "medición de audiencias"-; así como tampoco informan de manera activa del gasto público destinado a la contratación de servicios de terceros que asisten a las autoridades en las tareas de perfilamiento en línea, o las condiciones mismas en que se lleva a cabo dicha contratación.

Casos relevantes

Colombia

Una investigación[13] de la Fundación para la Libertad de Prensa (FLIP) reveló en 2020 que el gobierno de entonces había contratado, con recursos públicos para la implementación del proceso de paz, a una empresa privada para posicionar positivamente al gobierno ante la opinión pública.

La ejecución de dicho contrato implicó, en la práctica, la elaboración de un listado de hasta 486 usuarios[14] de la red social Twitter (hoy X) y su caracterización como "positivo" o "neutro" en relación con sus opiniones emitidas en línea entre los meses de junio y diciembre de 2019 y que refiriesen al gobierno o sus políticas públicas.

Medios de prensa locales que hicieron seguimiento a dicho informe, dieron cuenta de cómo la Consejería Presidencial de las Comunicaciones defendió, ante la solicitud de acceso a la información elevada por la FLIP, la realización de dicha tarea sosteniendo que "se realizó a partir de criterios objetivos como es interacciones digitales que incluyen indicadores como los

[11] Es decir, a través de una persona o equipo de personas que navegan manualmente a diario en distintas plataformas de internet para llevar a cabo los perfilamientos, y fruto del cual recogen dicha información de manera artesanal en bases de datos que buscan cumplir alguna de las dos finalidades advertidas en esta sección.
[12] Es decir, a través de algoritmos que facilitan el raspado de contenidos generados por los usuarios en línea -crawlers- que automatizan la búsqueda y descarga de datos de interés, así como su posterior procesamiento, analítica y procesamiento.
[13] Fundación para la Libertad de Prensa (2020). Pauta Visible. La pantalla del presidente Duque y la Pauta, parte I. En: https://pautavisible.org/mapa/5100; Fundación para la Libertad de Prensa (2020) Pauta Visible. La pantalla del presidente Duque y la Pauta, parte II. En: https://pautavisible.org/mapa/5125
[14] Infobae (2021). Corte Suprema cuestionó al gobierno de Duque y a la firma Du Brands por perfilar tuiteros. En: https://www.infobae.com/america/colombia/2021/02/27/corte-suprema-cuestiono-al-gobierno-de-duque-y-a-la-firma-du-brands-por-perfilar-tuiteros/

actores más relevantes de la red en término de número de seguidores e interacciones".[15] Dichos perfilamientos incluyeron a influenciadores, figuras políticas, periodistas, medios de comunicación, integrantes de organizaciones sociales, entre otros.

Una de las personas afectadas y calificadas como de posición "negativa" frente al gobierno, elevó ante la Corte Suprema de Justicia una acción de tutela para reclamar el amparo de su derecho a la protección de datos y privacidad en línea.[16] La Corte Suprema falló[17] a su favor al considerar que el Departamento Administrativo de Presidencia, al que está afiliada la Consejería de las Comunicaciones, habría hecho un tratamiento no autorizado de los datos sensibles del tutelante que referían a su posicionamiento político, lo que vulneró su derecho a la protección de datos.

En el fallo, la Corte Suprema de Justicia precisó que:

> Independientemente que la información del accionante en su cuenta de Twitter y trinos puedan ser consultados abiertamente por el público, la accionada [la Presidencia de la República] no estaba facultada *para hacer uso de la misma como si se tratase de datos de naturaleza pública* y con fundamento en ello elaborar el listado de influenciadores en el que incluyó al acto, pues es evidente que lo que determinó su inclusión y el calificativo de «negativo» fue precisamente su ideología política, plasmada en su interacción en la red social (Subrayado propio).

El fallo, con efectos aplicables solo respecto del tutelante, ordenó el retiro de su información personal de la base de datos constituida con información fruto del perfilamiento, y llamó la atención de las autoridades sobre los riesgos asociados a las bases de datos o "listas negras" que contienen información de esta naturaleza.

Brasil

Según una investigación periodística del medio The Intercept publicada en julio de 2021, los contratos de monitoreo de redes sociales fueron desplegados en ese país por entidades del sector público desde 2014.[18]

El monitoreo, en el contexto de Brasil, así como en el de Colombia, implica el perfilamiento de personas para la medición de la aceptación del gobierno y sus autoridades, y diseñar estrategias para asegurar su posicionamiento en redes sociales. El reportaje de The Intercept señala que este tipo de contratos iniciaron en Brasil durante el gobierno de Dilma Rousseff sin que mediara un amparo legal que los justificara. Con el paso del tiempo, según el reportaje, el monitoreo de redes sociales se convirtió en una práctica acostumbrada de las autoridades que se justifican en la necesidad de medir el éxito de las políticas públicas.

---

[15] El Espectador (2020). La lista de influenciadores a los que la Presidencia les pone el ojo. En: https://www.elespectador.com/politica/la-lista-de-influenciadores-a-los-que-la-presidencia-les-pone-el-ojo-article/

[16] El Tiempo (2021). Gobierno debe explicar para qué usó lista con nuestros nombres. En: https://www.eltiempo.com/colombia/cali/corte-suprema-cuestiona-a-gobierno-por-lista-de-influenciadores-569951

[17] Corte Suprema de Justicia, Sala de Casación Penal, Sala de Decisión de Tutelas Nro 1, STP 9319-2020. En: https://lavozdelderecho.com/files/STP9319-2020.pdf

[18] The Intercept (2021). O Legado Da Secom. En: https://www.intercept.com.br/2021/07/07/governo-bolsonaro-deturpou-edital-de-dilma-para-fichar-detratores-na-internet/

En la práctica, esos contratos de monitoreo de redes sociales apuntan a identificar el posicionamiento de la ciudadanía con fichas individualizadas de aquellas que tienen una postura "positiva", "negativa" o "neutral" del gobierno y sus autoridades, y que constituyen una nueva modalidad de la vigilancia masiva desplegada por el Estado.

Según dicho reportaje, fruto del monitoreo se habrían creado bases de datos con más de 100 gigabytes de información en donde consta más de 100 mil publicaciones en redes sociales (Facebook y X mayormente) que identifican a su autor, a las personas con las que ésta interactúa, su posición o sentimiento frente al gobierno, el asunto de su opinión (corrupción, educación, etc.), la foto de perfil del usuario, entre otros.[19]

En Brasil, más de una docena de entidades públicas llevan a cabo este tipo de monitoreo de redes sociales entre las que se encuentran el Banco Central de Brasil, la Asamblea Legislativa de Minas Gerais, la Prefectura de Sao Paulo, y la Presidencia de la República.[20]

Para 2021, esta última entidad pública acumulaba en la base de datos de monitoreo más de 20 millones de publicaciones extraídas de redes sociales que incluían información de periodistas, influenciadores, detractores, figuras políticas, así como de la ciudadanía en general[21]. Asimismo, The Intercept da cuenta que, fruto del monitoreo de redes sociales que se extendió también en 2020, un tuitero que había decidido comentar de manera crítica un tuit de Bolsonaro, fue incluido en el listado individualizado del gobierno federal de influenciadores bajo el rótulo "negativo" frente al gobierno.[22]

En abril de 2024, la Cámara de Diputados de Brasil elevó una solicitud de acceso a la información[23] dirigida al Tribunal de Cuentas de la Unión para que éste informara por el gasto público de $ 197,7 millones de reales (el más alto de la historia de las licitaciones de la Secretaría Especial de Comunicación Social) que serían destinados por el gobierno a tareas de perfilamiento en redes sociales. La solicitud incluía entre sus preguntas las siguientes:

> O TCU pode esclarecer quais foram as justificativas apresentadas pelo governo para o investimento de R$ 197,7 milhões em um contrato de monitoramento de redes sociais? Como esse gasto se alinha com os princípios de economicidade e eficiência da administração pública?
>
> O TCU considera proporcional e necessário o montante destinado especificamente para a análise de emoções e sentimentos através de inteligência artificial, que representa 36% do total do contrato? Como isso se justifica frente às prioridades nacionais?

[19] The Intercept (2021). O Legado Da Secom. En: https://www.intercept.com.br/2021/07/07/governo-bolsonaro-deturpou-edital-de-dilma-para-fichar-detratores-na-internet/
[20] The Intercept (2021). O Legado Da Secom. En: https://www.intercept.com.br/2021/07/07/governo-bolsonaro-deturpou-edital-de-dilma-para-fichar-detratores-na-internet/
[21] The Intercept (2021). O Legado Da Secom. En: https://www.intercept.com.br/2021/07/07/governo-bolsonaro-deturpou-edital-de-dilma-para-fichar-detratores-na-internet/
[22] The Intercept (2021). O Legado Da Secom. En: https://www.intercept.com.br/2021/07/07/governo-bolsonaro-deturpou-edital-de-dilma-para-fichar-detratores-na-internet/
[23] Câmara dos Deputados SIT N°5-2024, Do Sr. Evair Vieira De Mejo. En: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2415093&filename=Tramitacao-SIT%205/2024 ; https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2430379

Las condiciones de la licitación[24] –citadas en la solicitud de acceso a la información en cuestión– señalan como objetivos del contrato (i) medir la popularidad del gobierno en redes sociales, (ii) efectuar a través del uso de la inteligencia artificial análisis de sentimientos y emociones de los usuarios de redes sociales en sus opiniones sobre el gobierno y sus políticas, y (iii) combatir la desinformación y la difusión de noticias falsas en redes sociales, así como "incentivar su denuncia" para "construir una educación mediática"[25] en línea.

Hay que resaltar, además, que los términos de la licitación y sus condiciones se conocen gracias al trabajo de la prensa local y la solicitud de acceso a la información elevada por la Cámara de Diputados.

Sobre la licitación, organizaciones y *think tanks* locales emprendieron una acción judicial amparada en la Ley de Acción Civil Pública, la cual está dirigida a cuestionar el proceso de licitación emprendido precisamente en un año electoral en el país por considerar que "viola los principios constitucionales, como de moralidad, impersonalidad y de igualdad frente a la ley [así como por] configurar abuso de poder económico, y posible influencia indebida en el proceso electoral".[26]

Este perfilamiento, según el plan de licitación –del que no hay información pública disponible sobre si ya fue asignado contractualmente y a quién– en la solicitud de acceso a la información, incluiría análisis a los comentarios e interacciones en línea de usuarios de internet, en idiomas inglés, español y portugués. A la fecha, la solicitud de acceso a la información elevada por la Cámara de Diputados no ha sido respondida.

Por su parte, en junio de este año, el Supremo Tribunal Federal STF anunció la apertura de una licitación para encargar servicios de monitoreo en las redes sociales de contenidos relacionados con la actividad del Tribunal. La iniciativa surge como un mecanismo del Tribunal que alude a combatir la difusión de noticias falsas y desinformación. Según el medio Veja Abril, el propósito del Tribunal es "saber tudo que se fala sobre ele nas redes sociais"[27]/ saber todo lo que se habla de éste en las redes sociales.

Este contrato de licitación incluiría la exigencia de identificación de las personas usuarias que difunden cierto tipo de contenidos calificados como falsos por el Tribunal y la parte contratista, y en especial a las personas involucradas en menciones "positivas", "negativas" o "neutras" sobre

---

[24] Citadas en la solicitud de acceso a la información elevada por la Cámara de Diputados. Ver: Câmara dos Deputados SIT N°5-2024, Do Sr. Evair Vieira De Mejo. En: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2415093&filename=Tramitacao-SIT%205/2024 ; https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2430379

[25] Revista Oeste (2024). Associações processam governo Lula por abrir licitação de R$200 milhões para 'moderar' redes sociais. En: https://revistaoeste.com/politica/associacoes-processam-governo-lula-por-abrir-licitacao-de-r-200-milhoes-para-moderar-redes-sociais/

[26] Revista Oeste (2024). Associações processam governo Lula por abrir licitação de R$200 milhões para 'moderar' redes sociais. En: https://revistaoeste.com/politica/associacoes-processam-governo-lula-por-abrir-licitacao-de-r-200-milhoes-para-moderar-redes-sociais/ Cita original "As associações consideram que a contratação, especialmente em ano eleitoral, viola os princípios constitucionais, como a moralidade, a impessoalidade e a isonomia. Isso configura abuso de poder econômico e possível influência indevida no processo eleitoral".

[27] Veja Abril (2024). STF vai monitorear redes sociais e rastrear usuários. En: https://veja.abril.com.br/politica/stf-vai-monitorar-redes-sociais-e-rastrear-usuarios

el trabajo del Tribunal[28] así como su localización geográfica, una base de datos de personas influenciadoras, así como de acciones eventuales organizadas en línea.

Este monitoreo significa en la práctica, que cualquier contenido generado por usuarios de internet sobre el trabajo del Supremo Tribunal Federal, sin importar su contenido, significa operativamente su inclusión en una base de datos de monitoreo para su posterior caracterización en razón a su postura.

Los requisitos del contrato exigen informar al STF periódicamente de los debates en línea y su posible repercusión a la imagen del Tribunal. Obliga asimismo a compartir los datos de eventuales amenazas a los ministros del STF con la Policía Federal para la eventual investigación y judicialización de personas envueltas en posibles actividades criminales.[29]

3. El "ciberpatrullaje" para la aludida seguridad ciudadana

En LATAM cada vez más gobiernos despliegan acciones de "ciberpatrullaje" que dicen simular las acciones de patrullaje que ocurre en las calles, pero aplicado a las actividades que suceden en la red.

El ciberpatrullaje es desplegado por los cuerpos de policía principalmente por motivos que aluden a la prevención de delitos ordinarios y ciberdelitos, pese a que, en la práctica, también se lo ha empleado para la identificación de noticias falsas y desinformación –de hecho, en ocasiones el ciberpatrullaje se despliega justamente para la persecución de noticias falsas y la desinformación en los países donde dichas prácticas son consideradas delitos o ciberdelitos[30]–.

A la fecha, no hay claridad en los marcos normativos de los estados en materia criminal o policial sobre la naturaleza jurídica del ciberpatrullaje. Si bien se la presenta como una tarea de prevención del delito, la verdad es que su despliegue operativo sería el de una tarea de inteligencia criminal propensa a la vigilancia masiva de la ciudadanía.[31] Tampoco surgen de los casos relevantes la información clara sobre cuáles serían los límites de esta actividad, los controles judiciales o administrativos aplicables, entre otros.

El despliegue del ciberpatrullaje implica, al igual que las tareas de perfilamiento del punto anterior, la vigilancia masiva sobre la interacción en línea de las personas, principalmente aquellas que son usuarias de redes sociales. Las autoridades recopilan, de manera manual o automatizada, la información disponible en línea que podría utilizarse después para iniciar

[28] Tudo Celular (2024). TCU Deve investigar licitação do STF para monitoreamiento das redes sociais. En: https://www.tudocelular.com/seguranca/noticias/n222602/stf-deve-monitorar-redes-sociais-usuarios.html
[29] Veja Abril (2024). STF vai monitorear redes sociais e rastrear usuários. En: https://veja.abril.com.br/politica/stf-vai-monitorar-redes-sociais-e-rastrear-usuarios
[30] Lara-Castro, P. (2023). When protections becomes an excuse for criminalisation: Gender considerations on cybercrime frameworks. Derechos Digitales. En: https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf
[31] Centro de Estudios en la Libertad de Expresión y Acceso a la Información CELE (s.f.). Marco normativo y grises en una discusión que impacta directamente en nuestros derechos humanos. En: https://observatoriolegislativocele.com/ciberpatrullaje-o-inteligencia/

procesos judiciales en contra de las personas con presencia en internet. En algunos casos, esto ha privado incluso de libertad a las personas que han sido objeto de esta vigilancia.

Esta práctica, según distintas solicitudes de acceso a la información elevadas por la sociedad civil, declaraciones en prensa de las autoridades que despliegan dicha tarea y regulaciones de naturaleza infralegal que serán descritas a continuación, se basa en la premisa de que las autoridades estarían autorizadas para acceder y utilizar ***cualquier información disponible en línea en tanto que se considera, por su publicación, como pública y abierta*** a su explotación y uso indiscriminado. Información en línea sobre la cual las personas ya no tienen control o no pueden limitar su uso por terceros con fines de persecución criminal.

Casos relevantes

Argentina

En el año 2020 el Ministerio de Seguridad de la Nación propuso a consideración de la ciudadanía el borrador del protocolo de ciberpatrullaje, en atención a la Resolución 31 del 26 de julio de 2018 que ordenaba su creación para la prevención de los ciberdelitos.

Según el Centro de Estudios Legales y Sociales (CELS) que elaboró un informe analizando el contenido del protocolo, aquel no proporcionaba en su momento información clara sobre "qué tipo de decisión (y tomada por qué actor es la que podría iniciar las intervenciones de las áreas dedicadas a los ciberdelitos".[32] En el informe también se señala que "el proyecto de protocolo habilita a los organismos de las fuerzas de seguridad a buscar información en fuentes de internet abiertas para detectar y alertar sobre la comisión de eventuales delitos. Esto no es "patrullaje", son tareas de inteligencia criminal",[33] lo que les distingue claramente de las labores de prevención del delito.

Es importante destacar que la aprobación del protocolo no fue determinante para el inicio de actividades en ese sentido. Un ejemplo observado es el caso de Kevin Guerra, judicializado , por el delito de "intimidación pública"[34] por haber efectuado comentarios en su cuenta de la red social Twitter (hoy X) en el contexto de saqueos durante la pandemia, y que justificaron la apertura de una causa penal en su contra. La causa fue sobreseída en 2021 pues a consideración del Juzgado Federal N°3 de Mar del Plata no habría existido tal delito. Sin embargo, la justicia omitió en este caso cualquier análisis sobre la naturaleza del ciberpatrullaje o sus alcances.[35]

[32] Centro de Estudios Legales y Sociales CELS (2020). Sobre el proyecto de protocolo de ciberpatrullaje. En: https://www.cels.org.ar/web/wp-content/uploads/2020/04/CELS-sobre-protocolo-ciberpatrullaje.pdf pg. 2
[33] Centro de Estudios Legales y Sociales CELS (2020). Sobre el proyecto de protocolo de ciberpatrullaje. En: https://www.cels.org.ar/web/wp-content/uploads/2020/04/CELS-sobre-protocolo-ciberpatrullaje.pdf pg. 3
[34] Centro de Estudios Legales y Sociales CELS (2020). Vigilancia masiva: pedimos el sobreseimiento de Kevin Guerra. En: https://www.cels.org.ar/web/2020/04/vigilancia-masiva-pedimos-el-sobreseimiento-de-kevin-guerra/
[35] Centro de Estudios Legales y Sociales CELS (2021). La justicia federal sobreseyó a Kevin Guerra por sus expresiones en Twitter. En: https://www.cels.org.ar/web/2021/01/la-justicia-federal-sobreseyo-a-kevin-guerra-por-sus-expresiones-en-twitter/

En otro informe elaborado por Fundación Vía Libre e ILSED se afirmó – sobre el borrador del protocolo- que "el 'ciberpatrullaje' no tiene 'significado técnico o jurídico' y que se trata de una tarea ilegal".[36] Por su parte, una investigación publicada por el Centro de Estudios para la Libertad de Expresión (CELE) señala que "[e]ntre el 31 de mayo de 2020 y el 31 de octubre de 2022 rigió en efecto un 'Protocolo general para la prevención policial del delito con uso de fuentes digitales abiertas', aprobado por la resolución N° 144/2020 del ministerio de Seguridad de la Nación".[37] En octubre de 2022 se derogó el contenido de la Resolución N° 144 de 2020.

Sin embargo, en 2024 el Ministerio de Seguridad expidió la Resolución N° 428 que reinstauró dicha figura[38]. La nueva resolución, que no propone un protocolo para el despliegue del ciberpatrullaje sino lineamientos generales que orientan su despliegue, los fines que atiende y los delitos que busca perseguir, trae consigo la regulación de dicha figura a través del uso de sistemas de inteligencia artificial y la búsqueda y explotación de información "en sitios web *de acceso público y fuentes digitales abiertas* entendiéndose estas como los medios y plataformas de información y comunicación digital de carácter público, no sensible y sin clasificación de seguridad",[39] o lo que es igual, cualquier pieza de información disponible en línea (Subrayado propio).

En esta nueva resolución emergen tres problemas[40] críticos como son (i) el uso del ciberpatrullaje para la persecución de crímenes o delitos ordinarios que no constituyen cibercrimen –como el lavado de activos, la falsificación de documentos públicos, entre otros- (ii) la persecución de personas que hagan un uso "irregular, inusual o poco inherente" a internet, lo que habilita a interpretaciones arbitrarias y al abuso policial, y (iii) la visión según la cual todo contenido disponible en línea, sin importar la configuración de privacidad efectuada por los usuarios de cuentas de redes sociales, es pasibles de ser objeto de este patrullaje.

Esta última resolución expedida en mayo de 2024 repite los errores del pasado en tanto que omite cualquier alusión a los controles judiciales o administrativos aplicables y no considera salvaguardias concretas para la protección de las personas usuarias de internet y sus derechos humanos.

---

[36] El Destape (2020). CELS, Vía Libre y el ILSED piden eliminar el ciberpatrullaje y critican el protocolo que prepara el Ministerio de Seguridad https://www.eldestapeweb.com/nota/cels-via-libre-y-el-ilsed-piden-eliminar-el-ciberpatrullaje-y-critican-el-protocolo-que-prepara-el-ministerio-de-seguridad-202042317300

[37] Centro de Estudios en la Libertad de Expresión y Acceso a la Información CELE (2023). Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay. En: https://www.palermo.edu/Archivos_content/2023/cele/papers/233008-reporte-regional-OSINT.pdf ver página 9

[38] Ministerio de Seguridad de la Nación Argentina (2024). Resolución 428/2024, RESOL-2024-428-APN-MSG. En: https://www.boletinoficial.gob.ar/detalleAviso/primera/308291/20240528

[39] Ministerio de Seguridad de la Nación Argentina (2024). Resolución 428/2024, RESOL-2024-428-APN-MSG. En: https://www.boletinoficial.gob.ar/detalleAviso/primera/308291/20240528 ver artículo 1

[40] Camacho Gutiérrez, L (2024). Ciberpatrullaje en Argentina. Análisis de una Resolución problemática. Centro de Estudios en Libertad de Expresión y Acceso a la Información CELE. En: https://observatoriolegislativocele.com/ciberpatrullaje-en-argentina-analisis-de-una-resolucion-problematica-por-lucia-camacho-g/

Bolivia

El ciberpatrullaje fue desplegado en ese país a partir de 2017 con la creación de la Fuerza Especial de Lucha Contra el Crimen (FELCC) de la Paz. Según el medio La Razón, los miembros de dicha división estarían a cargo de "fenómenos derivados del uso del internet con fines delictivos [para lo cual] realizarán patrullaje cibernético en las diferentes redes sociales y en las páginas web".[41] Con posterioridad fueron creadas unidades especializadas de este tipo para operar también en Cochabamba y Santa Cruz.[42]

En la pandemia, y por orden del Ministerio de Gobierno, se ordenó a las fuerzas de seguridad el despliegue de las tareas de ciberpatrullaje en línea "para evitar la desinformación respecto al coronavirus".[43] El ministro de entonces a cargo de dicha cartera señaló que con el ciberpatrullaje serían revisadas "las redes sociales y a la gente que desinforme tendrá procesos penales y legales".[44]

Según un informe publicado por la Fundación Internet Bolivia, el despliegue del ciberpatrullaje para la identificación de la desinformación fue de hecho instrumentalizado para la persecución de opositores políticos que derivaron en 37 personas condenadas por supuestamente haber participado de "movimientos desestabilizantes".[45] En ese mismo informe se advierte cómo la Defensoría del Pueblo habría elevado un comunicado en marzo de 2020 señalando que el ciberpatrullaje "podía constituirse en acciones contrarias a la libertad de expresión".[46]

A la fecha, el ciberpatrullaje sigue siendo desplegado por las autoridades en condiciones de total opacidad, aunado además al hecho de que en Bolivia no existe un marco jurídico garante del derecho al acceso a la información y la transparencia.

Brasil

Si bien en Brasil las autoridades en materia criminal no han usado expresiones como "ciberpatrullaje" o "patrullaje cibernético" para justificar la aprehensión de personas que se expresan en línea, operativamente sus resultados son los mismos.[47] En 2021, por ejemplo, fruto

[41] La Razón (2018). FELCC estrena División de Cibercrimen en La Paz. En: https://www.la-razon.com/sociedad/2018/07/25/felcc-estrena-division-de-cibercrimen-en-la-paz/
[42] Céspedes, D.; Machaca W. (2021). Ciberpatrullaje y desinformación durante la pandemia en Bolivia. Fundación Internet Bolivia. En: .https://internetbolivia.org/wp-content/uploads/2021/07/ib_invdi.pdf ver página 13
[43] Opinión (2020). Murillo ordena ciberpatrullaje y advierte con juicio a quienes desinformen en las redes sociales. En: https://www.opinion.com.bo/articulo/pais/murillo-anuncia-ciberpatrullajes-redes-sociales-pide-mas-desinformar/20200318073555757096.html
[44] Opinión (2020). Murillo ordena ciberpatrullaje y advierte con juicio a quienes desinformen en las redes sociales. En: https://www.opinion.com.bo/articulo/pais/murillo-anuncia-ciberpatrullajes-redes-sociales-pide-mas-desinformar/20200318073555757096.html
[45] Céspedes, D.; Machaca W. (2021). Ciberpatrullaje y desinformación durante la pandemia en Bolivia. Fundación Internet Bolivia. En: .https://internetbolivia.org/wp-content/uploads/2021/07/ib_invdi.pdf ver página 26
[46] Céspedes, D.; Machaca W. (2021). Ciberpatrullaje y desinformación durante la pandemia en Bolivia. Fundación Internet Bolivia. En: .https://internetbolivia.org/wp-content/uploads/2021/07/ib_invdi.pdf ver página 29
[47] Asociación para el Progreso de las Comunicaciones; Derechos Digitales; Artigo 19; Intervozes (2022). Examen Periódico Universal, 41 período de sesiones, Brasil. Contribución Conjunta de las Partes Interesadas. En: https://www.apc.org/sites/default/files/upr_brazil-sp-final.pdf

del “rastrillaje”[48] de las redes sociales a cargo de la Policía Militar, se aprehendió a una persona que se expresó en Twitter de manera satírica sobre el entonces presidente Bolsonaro. La Policía Federal consideró su publicación una amenaza para la seguridad nacional.[49]

Junto a la persona autora del tuit, también se judicializó a las que interactuaron con su publicación. Aunque horas después éstas fueron puestas en libertad, la investigación judicial en su contra sigue abierta. Recientemente, el Ministerio Público Federal propuso a los imputados un acuerdo de culpabilidad y el pago de una multa de hasta 20 mil reales, a cambio de no ser privadas de la libertad. Según el medio G1 Globo, aquellas no estarían dispuestas a aceptar el acuerdo de transacción por ser desproporcionado. Por lo que la actuación penal en contra de estas personas a la fecha continúa.[50]

El ciberpatrullaje (o “rastreamento”, como se lo denomina en portugués) de redes sociales emprendido por las autoridades penales se intensificó en el marco de eventos culturales masivos, como el concierto de la artista Madona que tuvo lugar en mayo de 2024 en Río de Janeiro.[51]

Hay que mencionar, además, que cuando se trata del control del espacio público en línea y fuera de él, el ciberpatrullaje se traslapa con otras tecnologías que facilitan la vigilancia masiva sobre las personas, como el uso de cámaras de reconocimiento facial, cuya masificación en ciudades como Río ha sido ampliamente criticada por diversas organizaciones de la sociedad civil[52]. La superposición de estas tecnologías para la vigilancia de las personas tiene, entre otras consecuencias, un efecto *chilling* para la expresión de las personas que buscan hacer parte de estos eventos culturales, así como la criminalización de la población empobrecida y afrodescendiente que transita o habita en las inmediaciones donde estas tecnologías son desplegadas.

Tal y como fue reportado[53] por el medio Metrópoles, la Policía Militar de Río de Janeiro intensificó para entonces el monitoreo de la actividad de las personas en redes sociales como parte de la estrategia del Centro Integrado de Comando y Control Móvil desplegado para la prevención de disturbios y detección del crimen organizado. El *rastreamento* o ciberpatrullaje en el contexto de Brasil se adelanta amparado en el marco de las facultades regulares de las

[48] G1 (2023). MPF propõe multa de R$ 20 mil a jovem detido por publicação sobre visita de Bolsonaro em MG. En: https://g1.globo.com/mg/triangulo-mineiro/noticia/2023/02/03/mpf-propoe-multa-de-r-20-mil-a-jovem-detido-por-publicacao-sobre-visita-de-bolsonaro-em-mg.ghtml
[49] UOL (2021. Jovem é preso em Uberlândia após publicação contra Bolsonaro no Twitter. En: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2021/03/04/jovem-e-preso-em-uberlandia-apos-publicacao-contra-bolsonaro.htm
[50] G1 (2023). MPF propõe multa de R$ 20 mil a jovem detido por publicação sobre visita de Bolsonaro em MG. En: https://g1.globo.com/mg/triangulo-mineiro/noticia/2023/02/03/mpf-propoe-multa-de-r-20-mil-a-jovem-detido-por-publicacao-sobre-visita-de-bolsonaro-em-mg.ghtml
[51] O Globo (2024). Show de Madonna em Copacabana: inteligência da PM monitora redes sociais para evitar organização de criminosos. En: https://oglobo.globo.com/rio/noticia/2024/05/03/show-de-madonna-em-copacabana-inteligencia-da-pm-monitora-redes-sociais-para-evitar-organizacao-de-criminosos.ghtml
[52] Outras Mídias (2024). Os Riscos do reconhecimento facial no Brasil. En: https://outraspalavras.net/outrasmidias/os-riscos-do-reconhecimento-facial-no-brasil/
[53] Metrópoles (2024). Inteligência da PMRJ monitora redes sociais antes de show de Madonna. En: https://www.metropoles.com/entretenimento/musica/inteligencia-da-pmrj-monitora-redes-sociais-antes-de-show-de-madonna

autoridades policiales, sin que exista un marco jurídico preciso que detalle a la fecha los alcances, límites y controles aplicables a dicha tarea.

Colombia

El ciberpatrullaje fue regulado en Colombia a través de la Resolución N° 5839 de 2015,[54] expedida por el Ministerio de Defensa. Su adopción se hizo sin mediar valoraciones de proporcionalidad, necesidad, razonabilidad o legalidad. El artículo 15 numeral 12 de la Resolución señala que el Centro Cibernético Policial tendrá entre sus facultades:

> Realizar ciberpatrullajes 24/7 en la web, con el propósito de identificar amenazas desde y hacia Colombia en contra de la ciberseguridad ciudadana, desarrollando la capacidad de identificación y detección de factores comunes en los incidentes de su conocimiento así como la vulnerabilidad a la disponibilidad, integridad y confidencialidad de la información que circulan por el ciberespacio.

Como actividad vinculada a la seguridad ciudadana, se la desplegó ampliamente en el marco del Paro Nacional que tuvo lugar en los meses de marzo a junio de 2021 con el fin de detectar, por una parte, noticias falsas --también respecto del covid-19[55]--, y por otro, para detectar a los manifestantes que presuntamente habrían incurrido en hechos ilícitos en el marco de las protestas.

De hecho, en el Informe Anual de 2021 publicado por la Relatoría Especial para la Libertad de Expresión (RELE) sobre tendencias sobre el derecho a la libertad de expresión en el hemisferio se dio cuenta del uso del ciberpatrullaje por las autoridades colombianas en el marco del paro nacional.[56]

En éste, se cita un informe del Estado colombiano que señala que dicha tarea se empleó durante el paro nacional por "21.675 horas", y permitió la identificación de "154 noticias falsas, y más de 2.300 publicaciones que contienen amenazas a la vida o la integridad física"[57] así como la generación de "3.420 alertas preventivas anticipando actos de vandalismo y analizando 3.723

---

[54] Ministerio de Defensa Nacional (2015). Resolución N° 5839 del 31 de diciembre de 2015 "por la cual se define la estructura orgánica interna de la Dirección de Investigación Criminal e INTERPOL, se determinan las funciones de sus dependencias y se dictan unas disposiciones". En: http://web.archive.org/web/20220319221326/https://www.policia.gov.co/file/32305/download?token=OA0OIAOJ

[55] Índice Derechos Digitales (2023). Ciberpatrullaje de la Policía Nacional para identificar desinformación. En: https://indicederechos.digital/docs/CiberpatrullajeDesinformacion/

[56] Relatoría Especial para la Libertad de Expresión; Comisión Interamericana de Derechos Humanos (2022). Informe Anual de la Comisión Interamericana de Derechos Humanos, 2021. Volumen II. Informe Anual de la Relatoría Especial para la Libertad de Expresión. Tendencias sobre el derecho a la libertad de expresión en el hemisferio. OEA/Ser.L/V/II, Doc. 64 rev.1. En: https://www.oas.org/es/cidh/expresion/informes/IA2021ESP.pdf ver párrafos 264 y ss

[57] Relatoría Especial para la Libertad de Expresión; Comisión Interamericana de Derechos Humanos (2022). Informe Anual de la Comisión Interamericana de Derechos Humanos, 2021. Volumen II. Informe Anual de la Relatoría Especial para la Libertad de Expresión. Tendencias sobre el derecho a la libertad de expresión en el hemisferio. OEA/Ser.L/V/II, Doc. 64 rev.1. En: https://www.oas.org/es/cidh/expresion/informes/IA2021ESP.pdf ver párrafos 264 y ss

videos para identificar e individualizar responsables, logrando así la apertura de 9 procesos de investigación".[58]

Sobre el ciberpatrullaje que despliegan las autoridades de policía y otras entidades que llevan a cabo tareas de inteligencia, la organización colombiana Dejusticia encontró que incluso en una misma jurisdicción, las autoridades pueden tener visiones distantes y heterogéneas sobre qué constituye información abierta o cerrada en línea, una categoría que resulta esencial en las tareas de ciberpatrullaje y donde éste se limita –supuestamente- a las fuentes abiertas.[59]

Más aún, dicha organización encontró que los procesos de capacitación de los servidores en la inteligencia en fuentes abiertas --empleada como una de las metodologías/técnicas/tecnologías centrales en el ciberpatrullaje-- se reduce, en el caso colombiano, a sendos manuales y pocas o ninguna sesión de capacitación sobre sus límites y controles, el estudio y análisis de los escenarios en que su uso resulta ilegítimo, etc.[60]

Sobre la accesibilidad al contenido de la resolución N° 5839 de 2015 queremos llamar la atención de la RELE por cómo, al parecer, las autoridades han dado de baja su contenido para que no sea accesible en los repositorios oficiales de información normativa del Ministerio de Defensa. La resolución ya no es accesible en línea y su contenido solo fue posible recuperarlo para este informe a través del repositorio de Wayback Machine de la iniciativa Internet Archive que tiene almacenada una versión del enlace oficial a la resolución en su repositorio desde 2022.

México

Desde 2016 se despliegan actividades de ciberpatrullaje en México. Dicha actividad estaba contemplada en el "Modelo de Homologación de las unidades de policía cibernética" según el Acuerdo 06/XLI/16 de 20 de diciembre de ese año aprobado por el Consejo Nacional de Seguridad Pública.[61]

Según el Modelo de Homologación, el ciberpatrullaje o "patrullaje cibernético" apuntaba a "identificar las probables conductas constitutivas de delitos cibernéticos cometidas en internet, a través de la búsqueda de datos en fuentes públicas que permitan la generación de inteligencia y nuevas líneas de investigación con otras unidades de la Policía".[62]

---

[58] Botero, C. (2021). 21.647 horas vigilando internet: el ciberpatrullaje en 36 días del paro. El Espectador. En: https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/21647-horas-vigilando-internet-el-ciberpatrullaje-en-36-dias-del-paro/

[59] Camacho Gutiérrez, L.; Ospina Celis, D.; Upegui Mejía, J.C. (2022). Inteligencia estatal en internet y redes sociales: el caso colombiano. Dejusticia. En:https://www.dejusticia.org/wp-content/uploads/2022/12/InteligenciaEstatalEnInternet-Web-Dic23.pdf

[60] Camacho Gutiérrez, L.; Ospina Celis, D.; Upegui Mejía, J.C. (2022). Inteligencia estatal en internet y redes sociales: el caso colombiano. Dejusticia. En:https://www.dejusticia.org/wp-content/uploads/2022/12/InteligenciaEstatalEnInternet-Web-Dic23.pdf ver páginas 26 y ss

[61] Centro de Estudios en la Libertad de Expresión y Acceso a la Información CELE (2023). Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay. En: https://www.palermo.edu/Archivos_content/2023/cele/papers/233008-reporte-regional-OSINT.pdf ; y Article 19. Informe de Open Source Intelligence (OSINT) en México. En: https://articulo19.org/wp-content/uploads/2023/07/Informe-OSINT-Mexico.pdf

[62] Gobierno de México (s.f.). Modelo Homologado de Unidades de Policía Cibernética. En: https://www.gob.mx/cms/uploads/attachment/file/189189/Modelo_homologado_unidades_policia_cibernetica.pdf ver página 9

Luego, en 2019, la Ley que creó a la Guardia Nacional en reemplazo de la Policía Federal, concedió a este nuevo organismo la facultad de "vigilar, identificar, monitorear y rastrear la red pública de internet sobre sitios web con el fin de prevenir conductas delictivas".[63]

Sin embargo, una investigación publicada en 2024 por la Red en Defensa de los Derechos Digitales R3D en México reveló,[64] gracias a la información publicada en las filtraciones de Guacamaya, que la Guardia Nacional emplea esas facultades para monitorear a las personas usuarias de internet que son críticas del actuar del ejército.

Para hacer dicho monitoreo, el ejército emplea un software especializado de origen israelí denominado HIWIRE, que facilita el rastrillaje de internet, monitoreo de usuarios de redes sociales en tiempo real, el mapeo de sus interacciones en línea con otros usuarios, así como facilita el análisis del contenido de sus publicaciones en la red, la localización de cuentas de posibles amigos o familiares, todo esto facilitado además por la creación de cuentas falsas de usuarios en esas redes sociales para facilitar la interacción encubierta entre los agentes del ejército y la persona objetivo de este monitoreo.[65]

Como resultado del monitoreo, se generan fichas personalizadas de información de los usuarios de redes sociales "a fin de identificar y detectar oportunamente nuevas publicaciones, así como su impacto".[66]

Según la publicación de R3D, el ejército habría estado monitoreando a usuarios de internet desde 2019[67], particularmente en la red social X y Facebook, así como habría empleado estrategias para forzar la desactivación de las cuentas de ciertos usuarios críticos del gobierno en línea, así como operaciones de información dirigidas a influenciar o distorsionar las conversaciones en línea encubiertas en campañas de supuesta lucha contra la desinformación o de cuidado de la imagen institucional del ejército.[68]

En esa misma investigación trascendió que se habrían desplegado acciones de ciberpatrullaje respecto de las actividades de las cuentas de usuario @soy_militar ; @soy_militarmx y @yosoyyoio de la red social X, y cómo algunas de esas cuentas habrían sido objeto de ataques para quitar a su propietario el control de las mismas. A la fecha, la cuenta @soy_militar se

[63] Ley de la Guardia Nacional. Diario Oficial de la Federación el 27 de mayo de 2019. En: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGN.pdf Ver art. 9, literal XXXVIII
[64] Red en Defensa de los Derechos Digitales (2024). Ejército de bots: las operaciones militares para monitorear críticas en redes sociales y manipular la conversación digital. En: https://r3d.mx/2024/02/27/ejercito-de-bots-las-operaciones-militares-para-monitorear-las-criticas-en-redes-sociales-y-manipular-la-conversacion-digital/
[65] Animal Político (2024). Ejército monitorea redes sociales para identificar críticos de militares y del gobierno; crea bots para influenciar web. En: https://animalpolitico.com/seguridad/ejercito-monitorea-redes-sociales-criticos-bots
[66] Animal Político (2024). Ejército monitorea redes sociales para identificar críticos de militares y del gobierno; crea bots para influenciar web. En: https://animalpolitico.com/seguridad/ejercito-monitorea-redes-sociales-criticos-bots
[67] Red en Defensa de los Derechos Digitales (2024). Ejército de bots: las operaciones militares para monitorear críticas en redes sociales y manipular la conversación digital. En: https://r3d.mx/2024/02/27/ejercito-de-bots-las-operaciones-militares-para-monitorear-las-criticas-en-redes-sociales-y-manipular-la-conversacion-digital/
[68] Animal Político (2024). Ejército monitorea redes sociales para identificar críticos de militares y del gobierno; crea bots para influenciar web. En: https://animalpolitico.com/seguridad/ejercito-monitorea-redes-sociales-criticos-bots

encuentra desactivada. Según el Centro de Operaciones del Ciberespacio del Ejército Mexicano "había sido el propio usuario el que la desactivó por temor a perder el control de la cuenta".[69]

Paraguay

En junio de 2024 se dio recepción a la figura del ciberpatrullaje en el marco de la Ley N°7280 de reforma y modernización de la Policía Nacional.

En el artículo 6, numeral 32, se faculta a la Policía Nacional a "aplicar técnicas especiales, procesos de interceptación de comunicaciones, pesquisas y patrullas cibernéticas e investigaciones preliminares para la prevención e investigación de todo tipo de criminalidad, siempre con autorización judicial y bajo dirección del Ministerio Público".[70]

Es importante destacar que es el único país, por ahora, donde la figura del ciberpatrullaje o "patrullaje cibernético" estaría explícitamente sujeto a la revisión judicial. Sin embargo, la ley no señala si dicha revisión es previa o posterior; cuáles son las garantías que asisten a las personas objeto de este tipo de actividad; o cuáles son los límites aplicables al patrullaje línea, previsiones sobre si este puede ser encubierto o no, a qué tipos de información disponible en línea estaría delimitado, entre otros.

Uruguay

Según informes[71] de Datysoc, el ciberpatrullaje se habría desplegado en este país desde 2020. En ese año, una noticia periodística publicada en el medio Salto al Día, y que luego fue retirada de internet, daba cuenta de las capacidades de las autoridades de policía para monitorear las redes sociales, en especial las cuentas de usuarios con inclinaciones políticas de izquierda.[72]

Un pedido de acceso a la información elevado en 2022 por esta organización de la sociedad civil confirmó, luego de un intenso litigio que culminó recientemente, que el Ministerio del Interior y las autoridades de policía llevan a cabo actividades de "recolección de datos personales en fuentes abiertas en el marco de tareas de prevención e investigación de delitos".[73]

---

[69] Animal Político (2024). Ejército monitorea redes sociales para identificar críticos de militares y del gobierno; crea bots para influenciar web. En: https://animalpolitico.com/seguridad/ejercito-monitorea-redes-sociales-criticos-bots

[70] Ley N° 7280 de Reforma y Modernización de la Policía Nacional. En: https://www.bacn.gov.py/leyes-paraguayas/12364/ley-n-7280-de-reforma-y-modernizacion-de-la-policia-nacional

[71] Datysoc (2024). Ciberpatrullaje: ampliación del informe y resultados del litigio sobre vigilancia policial en internet. En: https://datysoc.org/litigio-ciberpatrullaje/#seccion1 ; Datysoc (2023). Ciberpatrullaje: Los límites borrosos de la vigilancia policial en Uruguay. En: https://datysoc.org/informe-ciberpatrullaje/

[72] Datysoc (2024). Ciberpatrullaje: ampliación del informe y resultados del litigio sobre vigilancia policial en internet. En: https://datysoc.org/litigio-ciberpatrullaje/#seccion1

[73] Datysoc (2024). Ciberpatrullaje: ampliación del informe y resultados del litigio sobre vigilancia policial en internet. En: https://datysoc.org/litigio-ciberpatrullaje/#seccion1

Dicha organización también obtuvo información que el Ministerio del Interior emplea un software especializado en el análisis de redes sociales denominado UCINET. Sin embargo, ante la solicitud de acceso a la información la entidad negó haber adquirido tecnologías específicas para dicho fin, lo que acentúa la duda ante la posible opacidad en el uso y despliegue del ciberpatrullaje en el país.[74]

En abril de 2024, la Dirección General de la Policía reconoció que se "está monitoreando las redes sociales".[75] Como resultado del ciberpatrullaje, se tiene conocimiento de la aprehensión en el mes de junio de un adolescente que habría sido identificado en redes sociales como partícipe de unos enfrentamientos en centros educativos y que habrían llamado la atención de las autoridades de policía.[76]

Sin embargo, el adolescente aprehendido habría sido identificado erróneamente por las autoridades –confundido por su homónimo en las redes sociales-, tal y como dio cuenta de ello una investigación periodística publicada en junio de este año que advertía a las autoridades del equívoco.[77] Pese a la advertencia, la Fiscalía abrió un expediente en contra del adolescente aprehendido.

En su reporte, Datysoc concluyó que la "policía uruguaya se encuentra realizando actividades de vigilancia en internet sin los protocolos y regulaciones necesarios para brindar garantías a la ciudadanía".[78]

3.1. Condiciones que fortalecen el ciberpatrullaje y amenazan los derechos humanos de las personas en línea

3.1.1. Operaciones encubiertas bajo la creación de perfiles falsos de agentes encubiertos en redes sociales

Por su naturaleza, el ciberpatrullaje se despliega en la práctica de manera encubierta y sigilosa, es decir, la persona usuaria de internet no tiene manera alguna de saber cuándo está siendo objeto de este tipo de vigilancia en línea por parte de las autoridades. El sigilo de esta tarea está asegurado, en parte, por la arquitectura y configuración técnica de la mayoría de las plataformas de redes sociales en que el ciberpatrullaje se despliega pues es común que éstas no informen a la persona usuaria de la red social de las terceras personas que visualizan sus publicaciones o

[74]Datysoc (2024). Ciberpatrullaje: ampliación del informe y resultados del litigio sobre vigilancia policial en internet. En: https://datysoc.org/litigio-ciberpatrullaje/#seccion1
[75] Subrayado (2024). "Se están previniendo situaciones", dice el director de la Policía, "hay monitoreo de redes por peleas". En: https://www.subrayado.com.uy/se-estan-previniendo-situaciones-dice-el-director-nacional-policia-hay-monitoreo-redes-peleas-n945084
[76] El País (2024). Imputaron a Dante, el adolescente líder de la facción rival de "El Chepe" en peleas masivas en shoppings. En: https://www.elpais.com.uy/informacion/judiciales/imputaron-a-dante-el-adolescente-lider-de-la-faccion-rival-de-el-chepe-en-peleas-masivas-en-shoppings
[77] Caras y Caretas (2024). Increíble: Policía se llevó detenido a un joven inocente y la Fiscalía lo formalizó. En: https://www.carasycaretas.com.uy/politica/increible-policia-se-llevo-detenido-un-joven-inocente-y-fiscalia-lo-formalizo-n74402
[78]Datysoc (2024). Ciberpatrullaje: ampliación del informe y resultados del litigio sobre vigilancia policial en internet. En: https://datysoc.org/litigio-ciberpatrullaje/#seccion1

contenidos. Pero además, el sigilo busca ser asegurado a partir de la creación y uso de cuentas en redes sociales con identidades ficticias por parte de las autoridades.

De hecho, en el marco de las tareas de ciberpatrullaje hemos identificado cómo la adopción legal creciente de figuras como el "agente encubierto informático" que otorga facultades a las autoridades de policía para la creación de perfiles ficticios o falsos de agentes estatales encubiertos, puede incrementar el potencial del ciberpatrullaje para vigilar de manera directa a las personas ya ***no solo a través de la observación pasiva*** de sus actividades e interacciones, ***sino a través de la interacción activa y directa*** entre las autoridades y la persona objetivo de esta tarea.

Sin límites claros, esta figura amenaza la libertad de las personas en el uso de internet, así como deshace cualquier presunta distinción entre las fuentes públicas y privadas de información, en donde el ciberpatrullaje supuestamente solo opera respecto de la información publicada sin restricción de privacidad o derechos de autor en línea.

Así, una cuenta con una identidad de usuario ficticia –que facilita el ocultamiento de la verdadera identidad del investigador–, permitiría a las autoridades de policía acceder a grupos cerrados de redes sociales, grupos cerrados en servicios de mensajería, entre otros.

Los casos de regulación de la figura del "agente virtual encubierto" –o sus denominaciones derivadas– generan serias preocupaciones en materia de derechos humanos, en especial, por los riesgos que puede acarrear su uso indebido o abusivo para la protección de la privacidad en línea de las personas y para encubrir prácticas ilegales de vigilancia masiva.

Casos relevantes

Colombia

Una investigación[79] de Fundación Karisma da cuenta de la adquisición por parte de la Fiscalía General de la Nación de un software que permite crear agentes encubiertos virtuales, o sea, cuentas falsas en redes sociales para "enseñar a los agentes de esa entidad técnicas de búsqueda o anonimización en internet"[80] para adicionar a su trabajo manual de ciberpatrullaje en fuentes abiertas.

En Colombia la figura del agente encubierto virtual está regulada en el artículo 16 de la Ley 1908 de 2018 que reformó el Código Penal. Aunque la ley exige que una autoridad judicial autorice la intervención de las comunicaciones de una persona por parte de un agente encubierto, el uso de tecnologías digitales para la intrusión encubierta de estos agentes en grupos cerrados de redes

[79] Fundación Karisma (2023). Cuando el Estado vigila. Ciberpatrullaje y OSINT en Colombia. En: https://web.karisma.org.co/wp-content/uploads/2023/02/Cartilla_Cuando_el_estado_vigila_2_V_WEB-1.pdf
[80] Fundación Karisma (2023). Cuando el Estado vigila. Ciberpatrullaje y OSINT en Colombia. En: https://web.karisma.org.co/wp-content/uploads/2023/02/Cartilla_Cuando_el_estado_vigila_2_V_WEB-1.pdf ver página 19

sociales o para hacerse pasar como un amigo de un usuario de internet, no se ajusta a la visión tradicional de la "interceptación de comunicaciones".[81]

Ecuador

En 2023 se expidió la Ley Orgánica Reformatoria a Varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral, que reformó el Código Integral Penal COIP e introdujo a través del artículo 77 la figura del "agente encubierto informático".[82]

Conforme a dicho cuerpo legal, dicha figura, que podrá ser desplegada con permiso previo de la fiscalía, facilitaría a futuro las tareas de investigación criminal a través del ocultamiento de la verdadera identidad del investigador en donde sea preciso "realizar patrullajes o acciones digitales en el ciberespacio",[83] lo que le permitiría a las autoridades su intromisión en sistemas informáticos e infiltrarse para "entrar a foros, grupos de comunicación e incluso a fuentes cerradas de información y comunicación".[84]

El uso de esta figura no solo se limitaría a contextos de investigación criminal, sino también para los de "descubrimiento" o "esclarecimiento" de hechos delictivos cometidos o que podrían cometerse en línea. El artículo 77 habilita al agente encubierto a la obtención de imágenes, la realización de grabaciones de audio o video, así como de conversaciones con los investigados. También autoriza a "utilizar cualquier medio tecnológico, en cualquier lugar"[85] previa autorización que deberá ser solicitada por el fiscal ante la autoridad judicial.

Aun cuando el artículo en cuestión menciona la intervención de la fiscalía para conceder autorizaciones, la redacción del artículo es problemática. En primer lugar, porque habilita al uso de esta figura no solo para la investigación de delitos sobre los que existe una sospecha fundada, sino para "descubrir" actividades criminales sobre las que no existe información o sospecha previa, siendo esto último un pase libre para el uso del "agente encubierto informático" para el simple "patrullaje cibernético", donde la autoridad que emplea una identidad falsa podría observar, vigilar e interactuar con cualquier usuario de internet sin que exista motivo fundado para ello.

---

[81] Congreso de Colombia (2018). Ley 1908 de 2018 "por medio de la cual se fortalecen la investigación y judicialización de organizaciones criminales, se adoptan medidas para su sujeción a la justicia y se dictan otras disposiciones. En: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=87301

[82] Encalada, M. (2023). Agente encubierto informático. Derechos Digitales. En: https://www.derechosdigitales.org/21323/agente-encubierto-informatico/#:~:text=Una%20de%20las%20modificaciones%20m%C3%A1s%20pol%C3%A9micas%20es%20la,incluso%20a%20fuentes%20cerradas%20de%20informaci%C3%B3n%20y%20comunicaci%C3%B3 N°

[83] Asamblea Nacional, República del Ecuador (2023). Ley Orgánica Reformatoria a varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral. En: https://www.edicioneslegales-informacionadicional.com/webmaster/directorio/SU279_2023.pdf ver artículo 77

[84] Encalada, M. (2023). Agente encubierto informático. Derechos Digitales. En: https://www.derechosdigitales.org/21323/agente-encubierto-informatico/#:~:text=Una%20de%20las%20modificaciones%20m%C3%A1s%20pol%C3%A9micas%20es%20la,incluso%20a%20fuentes%20cerradas%20de%20informaci%C3%B3n%20y%20comunicaci%C3%B3 N°

[85] Asamblea Nacional, República del Ecuador (2023). Ley Orgánica Reformatoria a varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral. En: https://www.edicioneslegales-informacionadicional.com/webmaster/directorio/SU279_2023.pdf ver artículo 77

En segundo lugar, porque es una figura que habilita a las autoridades a "enviar de manera directa archivos, ficheros con contenido ilícito". Esto da lugar a que sean empleados por ejemplo sistemas de malware o spyware, en los dispositivos de las personas que interactúan con el agente encubierto informático. En el artículo, sin embargo, no media valoración sobre las amenazas o riesgos que ese contenido pueda significar para personas sobre las que no recae sospecha justificada o formen parte de un caso judicial activo, y mucho menos para los riesgos que puede representar para los derechos de las terceras personas que interactúan con ella.

Uruguay

Según Datysoc, la redacción actual del artículo 21 de la Ley de Inteligencia habilitaría el despliegue de agentes encubiertos sin orden judicial para la realización de actividades de monitoreo en redes sociales a través de la creación de "perfiles falsos en diferentes plataformas, acceder con una identidad encubierta a grupos de servicios de mensajería como WhatsApp o Telegram, interactuar directamente con las personas para obtener información, o simplemente acceder a información de perfiles privados por el solo hecho de ser aceptado como contacto".[86]

3.2. Uso y adquisición de software para el ciberpatrullaje

La capacidad expansiva y la masividad del ciberpatrullaje están sujetas, en buena medida, a los recursos operativos de las que disponen las autoridades de policía para desplegar dicha tarea. Cuando la tarea es ***automatizada*** o se apoya en sistemas de software que reemplazan o dan soporte al trabajo manual, el ciberpatrullaje aumenta de manera significativa su impacto.

Esto se debe a que la automatización permite su despliegue en tiempo real a través de distintas plataformas permitiendo a las autoridades la extracción de datos inferidos y la producción analítica sobre la información monitoreada, lo cual posee gran valor estratégico.

En la revisión de casos evidenciamos cómo los Estados adquieren tecnologías de monitoreo de redes sociales, mientras persiste – y en algunos casos se incrementa- la opacidad en la información relacionada con su licitación, adquisición, naturaleza, controles, responsables, y gasto público invertido en su compra.

Este escenario de opacidad, como veremos en los siguientes casos, se mantiene incluso en países en donde la sociedad civil ha acudido a las solicitudes de acceso a la información para echar luz sobre asuntos de interés público, en buena medida por argumentos de las autoridades que responden apelando a la seguridad nacional para mantener en reserva la información solicitada por éstas. Sin mencionar, en todo caso, la falta de claridad y transparencia respecto de las bases de datos que son creadas que facilitan el procesamiento de la información en línea recogida a través del ciberpatrullaje.

[86]Datysoc (2024). Ciberpatrullaje: ampliación del informe y resultados del litigio sobre vigilancia policial en internet. En: https://datysoc.org/litigio-ciberpatrullaje/#seccion1

Casos relevantes

Colombia

En un informe de Fundación Karisma sobre la adquisición de tecnologías que permitiesen a las autoridades desplegar capacidades de ciberpatrullaje en línea sobre fuentes abiertas, se obtuvo información sobre la tenencia de al menos 5 herramientas privativas contratadas por el Estado entre 2016 y 2022.[87]

Las herramientas tecnológicas adquiridas por la Policía Nacional, la Fiscalía General de la Nación, el Comando Conjunto Cibernético, la Dirección de Investigación Criminal e Interpol DIJIN, y el Ejército Nacional, permiten entre otros, hacer inteligencia en fuentes abiertas para el ciberpatrullaje.[88]

En su investigación, la Fundación Karisma documenta cómo, ante las solicitudes de acceso a la información sobre la adquisición de este tipo de tecnologías, las autoridades en cuestión respondieron negando su existencia. Sin embargo, Karisma encontró que dicha información estaba públicamente disponible en el sistema de información de contratación del Estado. Esto "evidencia una práctica repetida que vulnera el derecho a obtener respuestas de fondo, claras, completas y oportunas conforme a lo determinado por la Constitución y la ley".[89]

Al mismo tiempo, la organización destaca que las razones de seguridad nacional[90] podrían permitir a las autoridades justificar la falta de publicación de los contratos o procesos de licitación para la compra pública de cierto tipo de tecnología. Esto sugiere que el Estado pudo haber adquirido más herramientas tecnológicas de las que actualmente se tienen en conocimiento.

Más aún, en su informe, se cuenta cómo una filtración de documentos de inteligencia realizada por el grupo Guacamaya que tuvo lugar en 2022, revela que la empresa Mollitiam Industries – señalada previamente en un reportaje del medio El Espectador publicado 2020[91] como la empresa proveedora de software de espionaje utilizado de forma irregular por el Ejército

[87] Fundación Karisma (2023). Cuando el Estado vigila. Ciberpatrullaje y OSINT en Colombia. En: https://web.karisma.org.co/wp-content/uploads/2023/02/Cartilla_Cuando_el_estado_vigila_2_V_WEB-1.pdf ver páginas 11 y 12
[88] Fundación Karisma (2023). Cuando el Estado vigila. Ciberpatrullaje y OSINT en Colombia. En: https://web.karisma.org.co/wp-content/uploads/2023/02/Cartilla_Cuando_el_estado_vigila_2_V_WEB-1.pdf ver paginas 11 y 12
[89] Fundación Karisma (2023). La punta del iceberg. Los problemas de transparencia del OSINT en Colombia. En: https://web.karisma.org.co/la-punta-del-iceberg-los-problemas-de-transparencia-del-osint-en-colombia/
[90] Fundación Karisma (2023). La punta del iceberg. Los problemas de transparencia del OSINT en Colombia. En: https://web.karisma.org.co/la-punta-del-iceberg-los-problemas-de-transparencia-del-osint-en-colombia/
[91] El Espectador (2020). Chuzadas: las exigencias del Ejército en contrato de software de inteligencia. En: https://www.elespectador.com/judicial/chuzadas-las-exigencias-del-ejercito-en-contrato-de-software-de-inteligencia-article-899922/?_gl=1*csp3xs*_gcl_au*MTYzMzg0NzI0MS4xNzIzODE5OTcy*_ga*MzY4NDY5NzE3LjE3MjM4MTk5NzY.*_ga_FPLL0E7S46*MTcyMzgxOTk3NS4xLjEuMTcyMzgyMDE5MS42MC4wLjA.

colombiano- es también una de las proveedoras de herramientas de inteligencia en fuentes abiertas para su uso por la Dirección Nacional de Inteligencia DNI. La empresa Mollitiam Industries ha sido calificada por Reporteros Sin Fronteras como una de las veinte depredadoras digitales de la libertad de prensa.[92]

Tal y como lo señala Karisma, los 5 contratos son "nada más que la punta del iceberg de los problemas con la adquisición y uso de programas OSINT en el país".[93] La organización afirma que, en ausencia de información pública, "es difícil hacer control ciudadano sobre las características de las herramientas como sobre su uso".[94]

México

En su informe sobre las capacidades de ciberpatrullaje con las que cuentan la Guardia Nacional en ese país, R3D da cuenta[95] de la adquisición por la Secretaría de Defensa del software HIWIRE desarrollado por la empresa israelí WebintPro. Su compra en 2020 no consta en las bases de datos públicas de contratación.

Según el reporte de R3D, el software empleado tiene capacidad para "identificar activistas e influenciadores clave y monitorear redes opositoras en tiempo real",[96] así como "vigilar en tiempo real en distintas redes sociales, mapear automáticamente vínculos entre usuarios y analizar el contenido de sus publicaciones" y "la creación y utilización de usuarios simulados o bots para manipular la conversación pública en línea".[97]

Uruguay

[92] La Vanguardia (2020). La española Mollitiam, en la lista de depredadores de la prensa de RSF. En: https://www.lavanguardia.com/politica/20200311/474086914489/la-espanola-mollitiam-en-la-lista-de-depredadores-de-la-prensa-de-rsf.html
[93] Fundación Karisma (2023). La punta del iceberg. Los problemas de transparencia del OSINT en Colombia. En: https://web.karisma.org.co/la-punta-del-iceberg-los-problemas-de-transparencia-del-osint-en-colombia/
[94] Fundación Karisma (2023). Chécheres, juguetes y armas. Un inventario parcial de las tecnologías que utiliza la Policía Nacional en Colombia. En: https://web.karisma.org.co/wp-content/uploads/2023/07/CHECHERES-JUGUETES-Y-ARMAS.pdf
[95] Red en Defensa de los Derechos Digitales (2024). Ejército de bots: las operaciones militares para monitorear críticas en redes sociales y manipular la conversación digital. En: https://r3d.mx/2024/02/27/ejercito-de-bots-las-operaciones-militares-para-monitorear-las-criticas-en-redes-sociales-y-manipular-la-conversacion-digital/
[96] Red en Defensa de los Derechos Digitales (2024). Ejército de bots: las operaciones militares para monitorear críticas en redes sociales y manipular la conversación digital. En: https://r3d.mx/2024/02/27/ejercito-de-bots-las-operaciones-militares-para-monitorear-las-criticas-en-redes-sociales-y-manipular-la-conversacion-digital/
[97] Red en Defensa de los Derechos Digitales (2024). Ejército de bots: las operaciones militares para monitorear críticas en redes sociales y manipular la conversación digital. En: https://r3d.mx/2024/02/27/ejercito-de-bots-las-operaciones-militares-para-monitorear-las-criticas-en-redes-sociales-y-manipular-la-conversacion-digital/

Según los informes sobre ciberpatrullaje de Datysoc, el Ministerio del Interior adquirió en 2020 una herramienta de monitoreo de redes sociales llamada UCINET, que sirve para el análisis de redes sociales y la visualización de interacciones entre redes de contacto.[98]

La organización tuvo conocimiento de esta información gracias a la publicación de la Memoria Anual del año 2020 del Ministerio del Interior que señala que el Observatorio Nacional de Violencia y Criminalidad "ha incorporado recientemente a su paquete de herramientas informáticas un software para el análisis de redes sociales (UCINET), lo que permitirá profundizar en los aspectos vinculares o relacionales de la criminalidad, un aspecto clave aún no abordado en nuestro país con la importancia que merece".[99]

Según Datysoc, la herramienta privativa UCINET de propiedad de Analytic Technologies permitiría, entre otros, "medir las relaciones de determinadas personas dentro de una red, comprender el comportamiento de grupos y detectar personas influyentes".[100] Cuando la organización remitió un pedido de acceso a la información al Ministerio del Interior sobre los fines y protocolos empleados en el uso de ese software, aquella entidad declaró la información reservada.

Luego de un arduo litigio emprendido por Datysoc que obligó al Ministerio del Interior a responder su pedido inicial, la entidad sostuvo que no habría negociado ni firmado contratos con empresas privadas para la compra de software dirigido a la recopilación y análisis de datos en fuentes abiertas, lo que siembra dudas entre la versión sugerida en la respuesta y el contenido de la Memoria Anual de 2020 que permitiría sostener lo contrario.

4. El perfilamiento y el ciberpatrullaje desde el sistema internacional de los derechos humanos

Uno de los retos que enfrenta el análisis de ciberpatrullaje y el perfilamiento en el sistema internacional de los derechos humanos tiene que ver con la falta de estandarización en el uso de ambos términos.

Así, mientras que el Sistema Interamericano de Derechos Humanos se refiere en propiedad al ciberpatrullaje y los perfilamientos –en tanto que son expresiones empleadas a su vez por los Estados de LATAM-; en el entorno de las Naciones Unidas dicha terminología no ha sido todavía empleada, en su lugar, se ha enfocado la atención al impacto que traerían consigo la inteligencia en redes sociales SOCMINT y el monitoreo en línea del discurso.

---

[98] Datysoc (2023). Ciberpatrullaje: Los límites borrosos de la vigilancia policial en Uruguay. En: https://datysoc.org/informe-ciberpatrullaje/ ver punto 5.3; y Datysoc (2024). Ciberpatrullaje: ampliación del informe y resultados del litigio sobre vigilancia policial en internet. En: https://datysoc.org/litigio-ciberpatrullaje/#seccion1 ver punto 4.3

[99] Datysoc (2023). Ciberpatrullaje: Los límites borrosos de la vigilancia policial en Uruguay. En: https://datysoc.org/informe-ciberpatrullaje/ ver punto 5.3

[100] Datysoc (2024). Ciberpatrullaje: ampliación del informe y resultados del litigio sobre vigilancia policial en internet. En: https://datysoc.org/litigio-ciberpatrullaje/#seccion1 ver punto 4.3

4.1. Sistema Interamericano de Derechos Humanos

El Sistema Interamericano de Derechos Humanos se ha referido en tres ocasiones sobre el despliegue del ciberpatrullaje. La primera vez, cuando la Comisión Interamericana de Derechos Humanos CIDH y la Relatoría Especial para la Libertad de Expresión RELE se profirieron en 2020 en comunicado de prensa N° R78/20 sobre el despliegue del ciberpatrullaje por Colombia y Argentina en el marco de la pandemia afirmando entonces que "podría afectar las libertades fundamentales".[101]

La segunda vez, con ocasión del informe con Observaciones y Recomendaciones fruto de la visita de trabajo a Colombia[102], publicado en 2021. El informe dio cuenta de la recepción de información proporcionada por la sociedad civil sobre el despliegue del ciberpatrullaje en el marco de la protesta social que tuvo lugar en marzo de ese año, y en el que la policía nacional persiguió los contenidos que ésta consideraba que desinformaron en ese contexto.

Sobre esa práctica, la CIDH manifestó su "preocupación [de] que las fuerzas de seguridad se estarían abrogando facultades de chequeo de información, clasificando estos contenidos como verdaderos o falsos [por lo que esto] resulta especialmente preocupante cuando la información que categoriza corresponde, en su mayoría, sobre la actuación de las fuerzas de seguridad [por lo que podrían incurrir] en prácticas de censura".[103]

Y en una tercera ocasión, en el Informe Anual de Tendencias de 2021 publicado por la RELE expresó que el ciberpatrullaje sería una práctica emprendida "por criterios subjetivos en vez de parámetros objetivos, legítimos y transparentes, conforme a estándares internacionales de derechos humanos".[104] En este mismo informe la RELE se refirió al perfilamiento en línea como una práctica que vulnera el derecho a la libertad de expresión, el ejercicio de la reunión pacífica -en donde su uso se ha empleado en contextos de protesta social- y el derecho a la libertad de prensa cuando los perfilamientos han sido dirigidos contra periodistas.[105]

[101] Comisión Interamericana de Derechos Humanos y Relatoría Especial para la Libertad de Expresión 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. Comunicado de Prensa R78/20. En: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1173&lID=2

[102] Comisión Interamericana de Derechos Humanos (2021). Observaciones y Recomendaciones. Visita de Trabajo a Colombia. En: https://www.oas.org/es/cidh/informes/pdfs/ObservacionesVisita_CIDH_Colombia_SPA.pdf

[103] Comisión Interamericana de Derechos Humanos (2021). Observaciones y Recomendaciones. Visita de Trabajo a Colombia. En: https://www.oas.org/es/cidh/informes/pdfs/ObservacionesVisita_CIDH_Colombia_SPA.pdf ver párrafos 177 y 178

[104]Relatoría Especial para la Libertad de Expresión; Comisión Interamericana de Derechos Humanos (2022). Informe Anual de la Comisión Interamericana de Derechos Humanos, 2021. Volumen II. Informe Anual de la Relatoría Especial para la Libertad de Expresión. Tendencias sobre el derecho a la libertad de expresión en el hemisferio. OEA/Ser.L/V/II, Doc. 64 rev.1. En: https://www.oas.org/es/cidh/expresion/informes/IA2021ESP.pdf ver párrafos 264 y ss

[105]Relatoría Especial para la Libertad de Expresión; Comisión Interamericana de Derechos Humanos (2022). Informe Anual de la Comisión Interamericana de Derechos Humanos, 2021. Volumen II. Informe Anual de la Relatoría Especial para la Libertad de Expresión. Tendencias sobre el derecho a la libertad de expresión en el hemisferio. OEA/Ser.L/V/II, Doc. 64 rev.1. En: https://www.oas.org/es/cidh/expresion/informes/IA2021ESP.pdf ver párrafos 3 y 249

4.2. Resoluciones en Naciones Unidas

En el seno del Consejo de Derechos Humanos se aprobó en 2022 el informe sobre "el derecho a la privacidad en la era digital" que por primera vez explora las prácticas de inteligencia en redes sociales SOCMINT y de monitoreo del discurso en línea como nuevas modalidades de la vigilancia masiva en internet desplegadas por los Estados.

Sobre el monitoreo y la inteligencia en redes sociales, sostuvo que son prácticas que tienen un serio impacto en los derechos humanos. Por ejemplo, el uso de tecnologías digitales que facilitan ambas tareas puede dar un mayor alcance y escala al monitoreo que puede tener fines legítimos o ilegítimos.

Más aún, esta amenaza se agrava cuando las fuentes de información obtenidas de las redes sociales son cruzadas con otras bases de datos, como las de reconocimiento facial y videovigilancia -también a disposición de los Estados- la información que reposa en manos de los proveedores de servicios de internet, las bases de datos de migrantes, incluso las que son armadas para perfilan a opositores políticos, lo que magnifica la capacidad de la vigilancia masiva y en tiempo real de la que éstos disponen.[106]

Las amenazas del monitoreo en línea y la inteligencia en redes sociales son múltiples. Ponen en riesgo el ejercicio del derecho a la libertad de expresión, a la reunión pacífica, a la participación en entornos en línea y fuera de ella. Al respecto, la resolución afirma que "individuals should have a space free from systematic observation and intrusion, in particular by government entities"[107]/ las personas deberían tener un espacio libre de la sistemática observación e intrusión, en especial de las entidades gubernamentales.

Asimismo, la resolución sostiene que el monitoreo general del espacio público es casi siempre desproporcionado. Y recomendó a los Estados adoptar marcos legales adecuados para regular la recolección, análisis y compartición de inteligencia obtenida de redes sociales que delimite claramente los escenarios en que ésta se encuentra permitida, sus prerrequisitos, las autorizaciones y procedimientos, así como los mecanismos para garantizar su supervisión adecuada.[108]

[106] Human Rights Council (August 4th, 2022) The Right to Privacy in the Digital Age, report of the Office of the United Nations High Commissioner for Human Rights. A/HRC/51/17 En: https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf?OpenElement ver párrafos 38 y ss

[107] Human Rights Council (August 4th, 2022) The Right to Privacy in the Digital Age, report of the Office of the United Nations High Commissioner for Human Rights. A/HRC/51/17 En: https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf?OpenElement ver párrafo 43

[108] Human Rights Council (August 4th, 2022) The Right to Privacy in the Digital Age, report of the Office of the United Nations High Commissioner for Human Rights. A/HRC/51/17 En: https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf?OpenElement ver párrafo 57 literal c

5. Preocupaciones en derechos humanos y recomendaciones

El perfilamiento y el ciberpatrullaje generan múltiples riesgos para el ejercicio de los derechos humanos en línea. Ambas actividades implican operativamente un *monitoreo encubierto e imperceptible para los usuarios de internet*, que recae *de manera generalizada sobre quienes tengan una presencia activa en línea* que se traduce en la práctica en:

- La generación de consecuencias social o jurídicamente relevantes para las personas enlistadas en bases de datos en razón a su actividad en línea, y que van desde su caracterización como opositor/a político/a, y su estigmatización social; la apertura de causas judiciales –y eventuales falsos positivos judiciales-, hasta la eventual privación de su libertad.
- La extensión indeterminada en el tiempo de la vigilancia masiva sobre las personas, así también de la conformación indefinida de bases de datos de quienes se expresan en distintos espacios y plataformas digitales y su eventual instrumentalización para criminalizar la libre expresión y otros derechos interdependientes a éste, como el de asociación pacífica y protesta, el de libre asociación, entre otros.
- La ausencia de seguridad jurídica y transparencia asociada a los límites, controles, mecanismos de supervisión, garantías judiciales y administrativas, mecanismos para la reparación de derechos –entre otros- aplicable a ambas actividades.
- Un mecanismo de represión o lucha contra lo catalogado como desinformación que puede derivar en el deterioro del ecosistema informativo en tanto que los perfilamientos y el ciberpatrullaje pueden posicionar los Estados y sus autoridades como fuentes unívocas de la verdad donde la verdad se la emplea como una herramienta de persecución criminal[109].

Así mismo, (i) la falta de claridad sobre la naturaleza del ciberpatrullaje como actividad de investigación o inteligencia policial, y los límites que corresponden aplicar en tanto que pertenezca a una u otra categoría; (ii) la desproporción de los perfilamientos para medir la aceptación de políticas sociales, o apoyar los procesos de cuidado de la imagen institucional, y (iii) la adquisición poco transparente de tecnologías que aumentan la capacidad de los Estados para perfilar y ciberpatrullar a la ciudadanía, derivan en conjunto en riesgos concretos para la libertad de expresión y la privacidad que pueden traer como consecuencia un efecto derrame o "spillover effect" frente al ejercicio de otros derechos que éstos otros dos habilitan o articulan.

Riesgos materia de libertad de expresión. Tanto los perfilamientos como el ciberpatrullaje son un riesgo generalizado para el ejercicio de la libertad de expresión y la protección de discursos que, siendo críticos, ácidos o incómodos, están protegidos.

También representan un riesgo en tanto que, por ejemplo, las listas de personas perfiladas o la criminalización de personas como consecuencia del ciberpatrullaje, puede inducir a la

[109] Lara-Castro, P. (2023). When protection becomes an excuse for criminalisation: Gender considerations on cybercrime frameworks. Derechos Digitales. En: https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf

autocensura y el efecto *chilling,* así como la estigmatización de ciertos tipos de discursos, personas o grupos de personas.

En los eventos más graves, los perfilamientos pueden conducir, por ejemplo, a la incitación a la violencia en línea particularmente contra las personas caracterizadas como "opositoras" a los gobiernos.

Riesgos en materia de privacidad y protección de datos. Los perfilamientos y el ciberpatrullaje suponen la eliminación de la expectativa de privacidad en línea y, en general, la anulación de los espacios privados en línea que deberían de estar libres de de la vigilancia estatal, especialmente en aquellos casos donde dicha vigilancia estatal no se encuentra plenamente delimitada por garantías consagradas en un marco legal que satisfaga estándares en derechos humanos.

Ambas actividades, en tanto que imperceptibles por las personas usuarias de internet, no son –y tampoco pueden ser- consentidas o repelidas por éstas, a menos que el perfilamiento o ciberpatrullaje que recaiga sobre éstas trascienda a la opinión pública o sea conocida por estas gracias a la apertura de una causa judicial en su contra.

Pero, además, tanto los perfilamientos como el ciberpatrullaje pueden derivar en la creación de bases de datos con información personal y sensible de las personas objeto de la vigilancia del Estado (incluyendo datos inferidos que también son personales), sobre sus redes de contactos, amigos y familiares. Dichas bases de datos deberían ser en sí mismas ilegales, independientemente a base jurídica del tratamiento que pueda ser argüida por las autoridades que las conforman a través de la explotación intensiva de internet.

Ambas actividades ameritan desde luego un abordaje desde la perspectiva de los marcos jurídicos para la *moderna* vigilancia estatal, más allá del enfoque de la protección de datos, por diversas razones.

En primer lugar, porque los marcos de protección de datos suelen exceptuar[110] de su aplicación a las tareas asociadas a la protección de la seguridad ciudadana y seguridad nacional –en las que se puede amparar al ciberpatrullaje-.

En segundo lugar, porque los marcos de protección de datos en América Latina no permiten responder a la garantía colectiva de derechos; las acciones o derechos que garantiza la protección de datos (acceso, rectificación, cancelación, oposición) tienen una vocación de protección individual.

En tercer lugar, porque en varios países, las autoridades de protección de datos, donde existen, no son organismos independientes y autónomos, o no cuentan con facultades para la investigar y sancionar a las autoridades por abusar de sus facultades para la conformación de bases de datos ilegales.

[110] Camacho Gutiérrez, L. (2022). Iniciativas legislativas sobre privacidad y protección de datos en Argentina, Brasil, Chile, Colombia, Ecuador, México, Guatemala, Paraguay y Perú, período 2019 a 2021. En: https://www.palermo.edu/Archivos_content/2022/cele/papers/iniciativas-legislativas-sobre-privacidad.pdf

Y, en cuarto lugar, porque la protección de datos es un mecanismo *reactivo* más no *preventivo* para la protección del derecho a controlar los datos sobre uno mismo cuando éste se enmarca en tareas estatales de naturaleza encubierta o que no son perceptibles para los ciudadanos –como sucede con los perfilamientos y el ciberpatrullaje-.

Por tanto, Derechos Digitales llama la atención para que la Relatoría Especial para la Libertad de Expresión y la Comisión Interamericana de Derechos Humanos:

- Reconozcan las tareas de perfilamiento en redes sociales y de ciberpatrullaje como mecanismos de vigilancia del discurso que se transforman, a su vez, en nuevas modalidades de la vigilancia masiva en línea desplegada por los Estados.

- Reconozcan que el perfilamiento de la ciudadanía en redes sociales y el ciberpatrullaje pueden constituir amenazas para los derechos humanos, en especial para el derecho a la libertad de expresión en línea, el derecho a la privacidad y la protección de datos, así como a otros derechos que éstos instrumentalizan o articulan.
- Reafirmen la importancia de aplicar los estándares interamericanos en derechos humanos en materia de vigilancia de las comunicaciones y su aplicabilidad frente a las nuevas modalidades de vigilancia estatal que emergen gracias a las nuevas y emergentes tecnologías digitales.

- Inviten y recomienden a los Estados:

    - A dar claridad sobre la naturaleza jurídica del ciberpatrullaje como tarea de investigación criminal o de inteligencia policial, a través de un marco legal que satisfaga, a través del consenso democrático, los estándares de legalidad, necesidad, proporcionalidad y razonabilidad.
        - En caso de que se trate de una tarea de inteligencia policial, recomendar a los Estados a que se aplique al ciberpatrullaje las garantías, controles y mecanismos de protección de derechos aplicables a las tareas de inteligencia y vigilancia estatal, invitando a los Estados a adherir y aplicar los “Los Principios Internacionales Sobre La Aplicación De Los Derechos Humanos A La Vigilancia De Las Comunicaciones”.[111]
        - En caso de que se trate de una tarea de investigación criminal, recomendar a los Estados a que su uso y despliegue se ajuste al debido proceso en materia criminal, a que esté supeditado a la supervisión judicial previa y posterior, y a que su uso como recurso investigativo sea empleado solo en el marco de investigaciones judiciales en curso.

    - Llamar la atención de los Estados para dar transparencia a la regulación, protocolos o marcos jurídicos en que se soportan los perfilamientos y el

[111] Necesarios & Proporcionados. Sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones. En: https://necessaryandproportionate.org/es/13-principles/

ciberpatrullaje; a que los Estados deroguen[112] los marcos jurídicos habilitadores de esas prácticas que sean incompatibles con los derechos humanos, y modifiquen la normativa existente para que se alinee a los estándares interamericanos en derechos humanos.

- Llamar la atención de los Estados para que los perfilamientos y el ciberpatrullaje no sean empleados para la persecución de la desinformación, y a fortalecer en su lugar el ecosistema mediático e informativo nacional a través mecanismos de financiación, protección e incentivo para la generación de mejores y más contenidos que permitan luchar contra el desorden informativo.

- Llamar la atención de los Estados para que el cuidado de la imagen institucional o la medición de la aceptación de las políticas públicas se efectúe a través de mecanismos proporcionales a esos fines y compatibles con los derechos humanos en línea. Los perfilamientos en línea para la satisfacción de esos fines, no es proporcional ni compatible con el derecho a la libertad de expresión o privacidad y protección de datos en línea.

- Llamar la atención de los Estados para la protección en línea de los datos de las personas y (i) reafirmar su protección incluso cuando esos datos han sido publicados por las personas de manera proactiva; a (ii) reafirmar que dicha protección también se extiende sobre las fuentes de información que sean calificadas como públicas; a (iii) reiterar la obligación de las autoridades a cumplir con los marcos de protección de datos en el marco de sus facultades legales; y (iv) a recordar a los Estados que aún no cuentan con mecanismos de protección del derecho a la protección de datos, a que lo sancionen.

- Llamar la atención de los Estados para que informen de manera transparente y proactiva (i) sobre si despliegan perfilamientos en línea y tareas de ciberpatrullaje, a las autoridades involucradas en cada una, su antigüedad y finalidades que cada una persiguen, (ii) sobre los recursos destinados a dichas actividades, incluida la adquisición de tecnologías digitales para su ejecución, (iii) informar sobre los controles judiciales o administrativos que aplican a cada una, los mecanismos de supervisión, así como los mecanismos para la protección de derechos de las personas.

- Llamar la atención de los Estados de la región para que desplieguen evaluaciones de impacto en derechos humanos de manera previa y posterior a los procesos de adquisición, compra, licenciamiento o licitación de las tecnologías digitales que habilitan a la vigilancia estatal en línea; y a que sean empleadas moratorias en

[112] Tomando en cuenta que, en el pasado, la CIDH ha conminado a Nicaragua a derogar la Ley de Ciberdelitos por su incompatibilidad con los Derechos Humanos. Ver: Comisión Interamericana de Derechos Humanos. (2021). Nicaragua: Concentration of power and the undermining of the Rule of Law. En: https://www.oas.org/en/iachr/reports/pdfs/2021_nicaragua-en.pdf

dicha adquisición, compra, licitación o licenciamiento cuando los riesgos para los derechos humanos sean mayores que los eventuales beneficios esperados.

- Instar a los Estados a la generación de protocolos públicos y transparentes sobre el uso de la inteligencia en fuentes abiertas OSINT y la inteligencia en redes sociales SOCMINT en el marco de las tareas de perfilamiento y ciberpatrullaje.

***