CELE

Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay

Septiembre 2023

Facultad de Derecho
Centro de Estudios en Libertad
de Expresión y Acceso a la Información

UP
Universidad
de Palermo

Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay

Nicolás Zara[1]
CELE

I. Introducción

Dentro de los múltiples cambios que internet produjo en las sociedades contemporáneas, uno de los más problemáticos es el vinculado al incremento de la capacidad de vigilancia de los Estados sobre sus ciudadanos y ciudadanas.[2] En la actualidad, la cantidad de información disponible sobre las personas en internet es mayor que nunca. Conforme ese volumen de información aumenta, los mecanismos para recolectarla, procesarla y almacenarla se vuelven cada vez más eficaces.

La información que dejamos en nuestras interacciones en la red es rutinariamente recogida y utilizada por empresas para ofrecer servicios de publicidad a terceros quienes, a su vez, nos ofrecen sus productos o servicios. Además, hay otros rastros que dejamos que cualquiera puede recoger, procesar y con ellos aprender mucho sobre nosotros y nosotras; incluso los Estados, con fines más o menos problemáticos.

La inteligencia de fuentes abiertas (en adelante OSINT, acrónimo de "Open Source Intelligence") forma parte de un conjunto de términos que hacen alusión a

[1] Investigador del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE-UP). Abogado graduado de la Universidad de Buenos Aires con orientación en Derecho Público. Magíster en Derecho (LL.M.) en Tulane University. Maestrando en Derecho Constitucional y Derechos Humanos en la Universidad de Palermo. Docente de Derecho Constitucional en la Universidad de Buenos Aires. Este trabajo es el producto de una investigación que comenzó en el año 2022 en el CELE, y que tuvo a Eduardo Bertoni como autor de un trabajo preparatorio en la materia. El autor agradece a Morena Schatzky, quien lo precedió a cargo de la investigación y formuló una primera versión de este trabajo, y a Agustina Del Campo, Ramiro Álvarez Ugarte, Paulo Lara, Catalina Moreno, Juan Pablo Parra, Martha Tudón y Patricia Díaz por sus valiosos aportes y comentarios.

[2] Organización de las Naciones Unidas (ONU), Consejo de Derechos Humanos, "El derecho a la privacidad en la era digital", informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, A/HRC/27/37, 30 de junio de 2014, § 2.

técnicas de inteligencia como COMINT,[3] SIGINT,[4] HUMINT,[5] GEOINT,[6] etc. Es posible entender a OSINT como la recopilación y el análisis de información recogida de fuentes abiertas (y disponibles públicamente) para producir inteligencia accionable. Recién en el momento en que a dicha información se le encuentra una utilidad o propósito, y es asignada a una acción concreta, pasa a convertirse en inteligencia propiamente dicha.[7]

El escenario global actual muestra un crecimiento en el desarrollo, adquisición y uso de tecnologías de vigilancia masiva por parte de los Estados.[8] El contexto regional no es diferente.[9] El cuadro se agudizó a partir de la intensificación de su uso a raíz del advenimiento de la pandemia de covid-19.[10] Además, los Estados se han mostrado reacios a brindar información acerca del uso de las tecnologías de vigilancia.[11] Los casos de espionaje estatal ilegal se han multiplicado en la región, e involucran

[3] Communications Intelligence (COMINT) se refiere a la información recopilada de comunicaciones de individuos, sea conversaciones telefónicas, mensajes de textos, y otros tipos de interacción en línea. Ver más en Tech Target, "COMINT (Communications Intelligence)", disponible en: https://www.techtarget.com/whatis/definition/COMINT-communications-intelligence, último acceso: 9 de agosto de 2023.

[4] Signal Intelligence (SIGINT) es aquella que recoge información mediante la interceptación de una amplia gama de señales (por ejemplo, radares u otros sistemas). Ver más en Everything RF, "What is SIGINT?", 2022, disponible en: https://www.everythingrf.com/community/what-is-sigint, último acceso: 9 de agosto de 2023.

[5] Human Intelligence (HUMINT) es el término utilizado para la recolección de información por fuentes humanas. Ver más en Odin-OSINT y Ciberinteligencia, "Qué es la HUMINT, ejemplos, técnicas y su relación con OSINT", 2022, disponible en: https://odint.net/humint-osint, último acceso: 9 de agosto de 2023.

[6] Geospatial Intelligence (GEOINT) consiste en la obtención de información sobre lugares y zonas geográficas –normalmente mediante mapas–, observaciones sobre el terreno, imágenes o sistemas de información geográfica. Ver más en Odin-OSINT y Ciberinteligencia, "Qué es la GEOINT y para qué se usa la inteligencia geoespacial", 2022, disponible en: https://odint.net/geoint, último acceso: 9 de agosto de 2023.

[7] ADC, "Seguidores que no vemos. Una primera aproximación al uso estatal del Open-Source Intelligence (OSINT) y Social Media Intelligence (SOCMINT)", 2018, disponible en: https://adc.org.ar/wp-content/uploads/2019/06/045-seguidores-que-no-vemos-10-2018.pdf, último acceso: 9 de agosto de 2023.

[8] ONU, *supra* nota 2, § 2.

[9] Centro por la Justicia y el Derecho Internacional (CEJIL) y otros, "Organizaciones advierten riesgos de tecnologías de vigilancia en audiencia ante la CIDH", 2021, disponible en: https://cejil.org/comunicado-de-prensa/organizaciones-civiles-advierten-riesgos-a-los-ddhh-sobre-tecnologias-con-capacidades-de-vigilancia-en-audiencia-ante-la-cidh, último acceso: 9 de agosto de 2023.

[10] En Colombia, las fuerzas de seguridad realizarían "ciberpatrullaje", al menos desde el año 2015, de acuerdo con el art. 15 de la res. Nº 5.389 del 31 de diciembre de 2015 de la Policía Nacional. Esas actividades se llevan adelante sin estar sujetas a normas que fijen estándares en su actuación. Ver, por ejemplo, la respuesta del Gobierno colombiano al pedido de información pública de la Fundación para la Libertad de Prensa (FLIP) a propósito de la utilización del "ciberpatrullaje" en la detección de "noticias falsas" (Ministerio de Defensa Nacional, Policía Nacional, Dirección de Investigación Criminal e Interpol, Nº GS-2021, DIJIN-CECIP-1.10, 30 de junio de 2021, disponible en: https://drive.google.com/file/d/1Z7AKesIM_LY5Jde-8tH2mQnDbyNZCc2a-/view, último acceso: 9 de agosto de 2023). En Argentina, las res. Nº 31/2018 y Nº 144/2020, hoy derogadas, autorizaban el "ciberpatrullaje".

[11] Por ejemplo, para el caso de Colombia, ver Fundación Karisma, "La punta del iceberg. Los problemas de transparencia del OSINT en Colombia", 2023, disponible en: https://web.karisma.org.co/la-punta-del-iceberg-los-problemas-de-transparencia-del-osint-en-colombia, último acceso: 9 de agosto de 2023.

generalmente a disidentes políticos, defensores y defensoras de derechos humanos, manifestantes, así como miembros de organizaciones sindicales y periodistas.[12]

En este marco se inserta la creciente utilización de OSINT por parte de los Estados con fines de vigilancia. Esta práctica presenta desafíos específicos en materia de derechos humanos. Se trata de herramientas cuyo empleo puede implicar una vulneración de derechos básicos y se usan en general, al margen de la legalidad. Como se verá en este estudio, su práctica generalmente no se encuentra reglamentada y allí donde existe regulación, esta es deficiente.[13] Bajo definiciones amplias y poco precisas, las autoridades encargadas de la inteligencia y la seguridad monitorean fuentes abiertas de información en internet como redes sociales, blogs, revistas y periódicos. En algunos casos, la información obtenida es organizada, sistematizada e incorporada a informes de inteligencia, que puede incluir la elaboración de perfiles de ciudadanos y ciudadanas.

El presente informe pretende ser una aproximación empírica y un análisis comparado de la utilización de OSINT por parte de los Estados de la región para fines de vigilancia. Se trata de un estudio de campo que permite conocer la magnitud del uso de estas técnicas, quiénes son los actores que las emplean, y cuáles han sido, si es posible medirlos, su impacto y su utilidad.

Esta investigación fue realizada por un consorcio de organizaciones (Artículo 19 Brasil y Sudamérica, Artículo 19 México y Centroamérica, Centro de Estudios en Libertad de Expresión y Acceso a la Información –CELE–, Datysoc, y Fundación Karisma). La coordinación estuvo a cargo del CELE, que propuso, como metodología de estudio, un método de entorno analítico-cualitativo. La investi-

[12] Ver, por ejemplo, Comisión Interamericana de Derechos Humanos (CIDH), Relatoría Especial para la Libertad de Expresión (RELE) y Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH), "La CIDH, RELE y OACNUDH expresan preocupación ante los hallazgos sobre uso del software Pegasus para espiar a periodistas y organizaciones de la sociedad civil en El Salvador", comunicado de prensa Nº 22/2022, 31 de enero de 2022. Scott-Railton, John y otros, "Project Torogoz. Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware", Munkschool of Global Affairs & Public Policy, University of Toronto & The Citizen Lab, 2022, disponible en: https://tspace.library.utoronto.ca/bitstream/1807/123609/1/Report%23148--project-torogoz.pdf, último acceso: 9 de agosto de 2023. Article 19 México, Red en Defensa de los Derechos Digitales (R3D) y Social TIC, "Gobierno espía: vigilancia sistemática a periodistas y defensores de derechos humanos en México", 2017, disponible en: https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf, último acceso: 9 de agosto de 2023. FLIP, "Inteligencia Militar incrementa su capacidad para vigilar a periodistas y ciudadanía con tecnología de fuentes abiertas", 2023, disponible en: https://www.flip.org.co/index.php/es/publicaciones/informes/item/3007-inteligencia-militar-incrementa-su-capacidad-para-vigilar-a-periodistas-y-ciudadania-con-tecnologia-de-fuentes-abiertas, último acceso: 9 de agosto de 2023. Por otra parte, también Colombia apareció dentro de la lista de clientes de software espía utilizado en contra de periodistas y dirigentes políticos en 2021. Dvilyanski, Mike, Agranovich, David y Gleicher, Nathaniel, "Threat Report on the Surveillance-for-Hire Industry", Meta, 2021, p. 10, disponible en: https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf, último acceso: 9 de agosto de 2023.

[13] Ver, por ejemplo, res. Nº 144/2020 del Ministerio de Seguridad de Argentina, derogada por res. Nº 720/2022.

gación partió de una extensa revisión de bibliografía existente en la materia, la elaboración de una metodología común, el envío de pedidos de acceso a la información pública a reparticiones estatales, entrevistas a diversos actores de los sectores público y privado de Argentina, Brasil, Colombia, México y Uruguay, y la elaboración de cinco informes nacionales.

En la sección II de este trabajo, se precisan algunos conceptos necesarios para la investigación. En la sección III se detalla el marco legal aplicable a la práctica de OSINT en cada uno de los países donde se llevó a cabo el estudio, particularmente en lo que respecta a su utilización por parte del Estado. Ello, en tanto la OSINT practicada por privados no constituye el foco principal de esta investigación, y en muchos casos está alcanzada por regulaciones generales, como las respectivas leyes de acceso a la información pública y de protección de datos personales. En la sección IV se relatan las prácticas de OSINT constatadas en cada uno de los Estados, ya sea como producto de las respuestas de los entes estatales a los requerimientos de información, como a través de entrevistas y de artículos de prensa. La sección V versa sobre las afectaciones a los derechos humanos que implica la actividad OSINT por parte del Estado para fines de vigilancia, principalmente en materia de privacidad y libertad de expresión. Finalmente, la sección VI sirve como conclusión.

II. OSINT e inteligencia estatal

OSINT (acrónimo de "Open-Source Intelligence", inteligencia de fuentes abiertas) es "la práctica que conlleva el uso de un conjunto de técnicas y tecnologías que facilitan la recolección de información que se encuentra disponible públicamente, como pueden ser textos, imágenes, videos, audios, e incluso datos geoespaciales. Recién en el momento que a dicha información se le encuentra una utilidad o propósito, y es asignada a una acción concreta, pasa entonces a convertirse en inteligencia propiamente dicha".[14] Ha sido definida también como "inteligencia producida utilizando información disponible públicamente, que es recolectada, utilizada y diseminada en tiempo oportuno a una audiencia apropiada, con el propósito de responder a un requisito específico de inteligencia".[15] La información

[14] ADC, *supra* nota 7, p. 5.

[15] Office of the Director of National Intelligence, "U.S. National Intelligence: An Overview 2011", 2011, p. 54, citado en Williams, Heather J. e Ilana Blum, "Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise", RAND Corporation, 2018, p. 1.

puede ser encontrada en diferentes fuentes, como por ejemplo libros, periódicos, radio, televisión, bases de datos gubernamentales, publicaciones en plataformas digitales, y en formatos diversos como texto, fotografías, videos, voz, etc.

Para entender de qué hablamos exactamente cuando hablamos de OSINT, es necesario formular precisiones respecto de las nociones de "inteligencia" y de "fuentes abiertas". Las definiciones de estos conceptos serán relevantes a la hora de establecer distinciones y de hacer valoraciones sobre la conducta estatal.

Según Peter Gill y Mark Phythian, se entiende por inteligencia al conjunto de "actividades –generalmente secretas– de focalización, recolección, análisis, diseminación y acción, dirigidas a mejorar la seguridad y/o mantener el poder relativo respecto de competidores, por medio de la detección temprana de amenazas y oportunidades".[16] Aunque existen otras definiciones posibles, la citada es valiosa porque de ella se desprenden varios elementos comunes a todas las actividades de inteligencia. En primer lugar, el hecho de que se realiza generalmente en secreto. En segundo lugar, la existencia de una finalidad determinada. En tercer lugar, su función de detección temprana o preventiva. Muchas de las actividades presentadas por los Gobiernos de la región como "ciberpatrullaje" comparten estas características y por ese motivo se trata, en rigor de verdad, de actividades de inteligencia. Finalmente, vale aclarar que se llama "inteligencia" tanto al ciclo de acciones mencionadas como al producto resultante de él. OSINT es una de las diferentes fuentes o disciplinas de recolección de inteligencia, tales como SIGINT,[17] COMINT,[18] HUMINT,[19] y GEOINT.[20]

---

16 Gill, Peter y Phythian, Mark, *Intelligence in an Insecure World,* Cambridge, Polity Press, 3º ed., 2018, p. 19, citado en Omand, David y Phythian, Mark, *Principled Spying: The Ethics of Secret Intelligence,* Oxford, Oxford University Press, 2018, p. 10.

17 SIGINT es aquella que recoge información mediante la interceptación de una amplia gama de señales (tales como radares, comunicaciones telefónicas, etc.). Ver más en Office of the Director of National Intelligence, "What is Intelligence?", disponible en: https://www.dni.gov/index.php/what-we-do/what-is-intelligence, último acceso: 9 de agosto de 2023.

18 COMINT es la parte de SIGINT que refiere a la información recopilada de comunicaciones de individuos, sea conversaciones telefónicas, mensajes de textos y otros tipos de interacción en línea. Tech Target, *supra* nota 3.

19 HUMINT es el término utilizado para la recolección de información por fuentes humanas. No necesariamente implica espionaje o actividad encubierta; la mayor parte de la HUMINT es producida por personas no encubiertas, tales como informantes estratégicos, agregados militares, etc. Ver más en Office of the Director of National Intelligence, *supra* nota 17.

20 GEOINT consiste en el análisis y la representación visual de las actividades relacionadas con la seguridad en la tierra. Se produce a través de la integración de imágenes, inteligencia de imágenes e información geoespacial. Ver más en Office of the Director of National Intelligence, *supra* nota 17.

Una vez definida OSINT e inserta dentro del marco de la actividad de inteligencia, resta dilucidar lo que se entiende por fuente abierta. Como primera medida, vale mencionar que "fuentes abiertas" incluye tanto información accesible offline (en medios de prensa tradicionales, como la televisión, la radio, los periódicos, y también en publicaciones académicas y bibliotecas) como online. El concepto de OSINT, entonces, es previo a internet. Como es evidente, la categoría de "fuentes abiertas" abarca diferentes tipos de información, accesibles por vías diversas.[21]

Este trabajo se centrará particularmente en la utilización de fuentes abiertas en internet por parte del Estado, para fines de vigilancia. Esta actividad presenta algunas peculiaridades relevantes. En primer lugar, el crecimiento vertiginoso de la web ha provocado que la cantidad de información disponible y susceptible de ser analizada haya crecido exponencialmente. Esto ha generado un rápido desarrollo de herramientas tecnológicas para recolectar masivamente esa información, analizarla y clasificarla.

La práctica de OSINT para vigilancia se ha masificado y su uso se ha "normalizado" en los Estados. Incluso se la ha intentado presentar a la ciudadanía como una herramienta legítima de seguridad interna, bajo el nombre de "ciberpatrullaje". Ello sin advertir a la población acerca de su potencial incidencia en el goce de los derechos humanos.[22]

Estas afectaciones tienen que ver, en primer lugar, con el derecho a la privacidad de las personas. La información obtenida de la web, a diferencia de la que antiguamente se extraía de los medios masivos de comunicación o de libros u otras publicaciones analógicas, puede no estar destinada a su difusión masiva. Además, en la inmensa mayoría de los casos, la información que existe en internet sobre una persona es muchísima más que la que existe offline, y los métodos utilizados para su recopilación podrían ser desproporcionados en relación con las necesidades estatales y los fines para los cuales se emplean.

Finalmente, a eso se agrega el posible efecto disuasorio que la práctica masiva de OSINT por parte del Estado podría suponer sobre los usuarios y las usuarias de internet, que podría tener una importante incidencia en el derecho a la libertad de expresión, tanto en su faz individual como en su faz colectiva.

---

[21] Bertoni, Eduardo, "¿Las prácticas OSINT son amigas o enemigas de los derechos humanos?", 2022 (pendiente de publicación).

[22] Fundación Karisma, "El Estado monitorea internet: implicaciones en los derechos humanos del ciberpatrullaje", 2023, disponible en: https://web.karisma.org.co/el-estado-monitorea-internet-implicaciones-en-los-derechos-humanos-del-ciberpatrullaje, último acceso: 9 de agosto de 2023.

III. Marco legal

III.1. Argentina

III.1.a. Leyes nacionales

La actividad de los organismos de inteligencia en la Argentina se encuentra regulada por la Ley de Inteligencia Nacional (Nº 25.520),[23] que dispone la inviolabilidad de las comunicaciones y documentos "privados o de entrada o lectura no autorizada o no accesible al público".[24] En tanto, la Ley de Defensa Nacional (Nº 23.554)[25] prohíbe a las Fuerzas Armadas realizar tareas de inteligencia relativas a la política interna del país.[26] La ley no establece distinciones en cuanto a la naturaleza de las tareas de inteligencia que se pueden llevar adelante, aunque la actuación del Sistema de Defensa se encuentra acotada a la prevención y al manejo de hipótesis de conflicto.[27]

III.1.b. El "protocolo de ciberpatrullaje" del Ministerio de Seguridad

En la actualidad, no existe un protocolo específico que regule la práctica de OSINT por las fuerzas de seguridad ni por los organismos de inteligencia. Sin embargo, entre el 2018 y el 2022, se sucedieron dos protocolos que intentaron hacerlo en el marco de la actividad de las fuerzas de seguridad.

El 26 de julio de 2018, la Secretaría de Seguridad del Ministerio de Seguridad de la Nación emitió la resolución Nº 31/2018, que facultó a las fuerzas nacionales de seguridad

---

[23] Información Legislativa (Infoleg), Ministerio de Justicia y Derechos Humanos, Presidencia de la Nación, Ley de Inteligencia Nacional Nº 25.520, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm, último acceso: 9 de agosto de 2023.

[24] Art. 5º: "Las comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario".

[25] Infoleg, Ministerio de Justicia y Derechos Humanos, Presidencia de la Nación, Defensa Nacional, "Principios básicos. Finalidad y estructura del sistema. Organización de las Fuerzas Armadas. Servicio de Defensa Nacional. Organización Territorial y Movilización. Disposiciones generales y transitorias", ley Nº 23.554, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm, último acceso: 14 de agosto de 2023.

[26] "Las cuestiones relativas a la política interna del país no podrán constituir en ningún caso hipótesis de trabajo de organismos de inteligencia militares" (art. 15). Además, de acuerdo con el art. 4º, "se deberá tener permanentemente en cuenta la diferencia fundamental que separa a la Defensa Nacional de la Seguridad Interior".

[27] La actividad del Sistema de Defensa Nacional es confinada por el art. 3º de la mencionada ley al "conjunto de planes y acciones tendientes a prevenir o superar los conflictos que esas agresiones generen, tanto en tiempo de paz como de guerra, conducir todos los aspectos de la vida de la Nación durante el hecho bélico, así como consolidar la paz, concluida la contienda".

interior a realizar OSINT en lo inherente a delitos como la venta ilegal de armas por internet o de cualquier artículo cuyo origen pudiera provenir de la comisión de un crimen o de la infracción de normas aduaneras, la difusión de imágenes que pudieran estar vinculadas a la trata y al tráfico de personas, y el hostigamiento sexual a menores.

La resolución estableció además que "los actos investigativos deberán limitarse a *sitios de acceso público*, haciendo especial hincapié en redes sociales de cualquier índole, fuentes, bases de datos públicas y abiertas, páginas de internet, dark web y demás sitios de relevancia de acceso público".[28] Las tareas de OSINT realizadas al amparo de esta norma debían tener por objetivo reunir los medios probatorios necesarios a fin de efectuar una denuncia ante las autoridades judiciales correspondientes.

Si bien esta investigación ha tenido acceso a la resolución, lo cierto es que no ha sido publicada en el Boletín Oficial[29] y recién tomó estado público en el marco de la discusión que antecedió a la sanción de la resolución Nº 144/2020, que la derogó.

Entre el 31 de mayo de 2020 y el 31 de octubre de 2022 rigió el "Protocolo general para la prevención policial del delito con uso de fuentes digitales abiertas", aprobado por la resolución Nº 144/2020 del Ministerio de Seguridad de la Nación,[30] que derogó la resolución Nº 31/2018. Dicho protocolo tenía por finalidad "establecer principios, criterios y directrices generales para las tareas de prevención del delito que desarrollan en el espacio cibernético los cuerpos policiales y fuerzas de seguridad dependientes del Ministerio de Seguridad".[31] Su alcance recaía sobre delitos específicos vinculados a la pandemia del covid-19.

Finalmente, el 27 de octubre de 2022 el Ministerio de Seguridad de la Nación dictó la resolución Nº 720/2022,[32] mediante la que dispuso la derogación de la resolución ministerial Nº 144 del 31 de mayo de 2020 y sus complementarias. En respuesta a un pedido de información pública del CELE, el Ministerio de Seguridad de la Nación informó que la derogación de la resolución Nº 144/2020 no restableció la vigencia de la resolución Nº 31/2018.

---

[28] El destacado no pertenece al original.

[29] Así lo afirman fuentes oficiales. Infoleg, Ministerio de Justicia y Derechos Humanos, Presidencia de la Nación, Ministerio de Seguridad, resolución Nº 144/2020, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=338229, último acceso: 9 de agosto de 2023.

[30] *Ibíd*.

[31] *Ibíd*., art 1º.

[32] Infoleg, Ministerio de Justicia y Derechos Humanos, Presidencia de la Nación, Ministerio de Seguridad, resolución Nº 720/2022, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/370000-374999/373942/norma.htm, último acceso: 9 de agosto de 2023.

III.1.c. Policía de la Ciudad Autónoma de Buenos Aires

En la Ciudad de Buenos Aires, la Ley del Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires (Nº 5.688),[33] en su artículo 89, confiere a la Policía de la Ciudad la atribución de realizar tareas de inteligencia criminal, aunque solamente en el marco de procesos judiciales.

III.2. Brasil

Según el artículo 144 de la Constitución Federal de Brasil, la seguridad pública "se ejerce para la preservación del orden público y la seguridad de las personas y los bienes", a través de diferentes órganos, a saber: Policía Federal; Policía Vial Federal; Policía Civil; Policía Militar y departamentos de bomberos militares; Policía Criminal Federal, Estatal y del Distrito Federal.

La ley Nº 13.675/2018[34] instituye el Sistema Único de Seguridad Pública (SUSP) y crea la Política Nacional de Seguridad Pública y Defensa Social (PNSPDS).[35] Los lineamientos de la PNSPDS son la "sistematización e intercambio de información sobre seguridad ciudadana, penitenciaria y drogas, a nivel nacional" y el "uso de un sistema integrado de información y datos electrónicos".

La ley Nº 9.883/1999[36] instituye el Sistema Brasileño de Inteligencia y crea la Agencia Brasileña de Inteligencia (ABIN). Esta ley entiende a la inteligencia como "la actividad que tiene por objeto obtener, analizar y difundir el conocimiento dentro y fuera del territorio nacional sobre hechos y situaciones de influencia inmediata o potencial en la toma de decisiones y la actuación gubernamental y en la salvaguarda y seguridad de la sociedad y del Estado".

Mediante el decreto Nº 3.695/2000[37] se creó el Subsistema de Inteligencia de Segu-

[33] Buenas Aires Cuidad, "Digesto G.C.B.A. - Detalle de la norma", 2018, disponible en: https://digesto.buenosaires.gob.ar/buscador/ver/25729, último acceso: 9 de agosto de 2023.

[34] Presidencia de la República, Secretaría General, Subdirección de Asuntos Jurídicos, ley Nº 13.675, 2018, disponible en: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13675.htm, último acceso: 9 de agosto de 2023.

[35] El decreto Nº 9.489/2018 reglamenta, en el ámbito de la Unión, la ley Nº 13.675/2018, por la que se establecen normas, estructura y procedimientos para la implementación de la Política Nacional de Seguridad Pública y Defensa Social. Decreto Nº 9.489, 2018, disponible en: https://dspace.mj.gov.br/bitstream/1/2221/4/DEC_2018_9489.htm, último acceso: 9 de agosto de 2023.

[36] Presidencia de la República, Casa Civil, Subdirección de Asuntos Jurídicos, ley Nº 9.883, 1999, disponible en: http://www.planalto.gov.br/ccivil_03/leis/L9883.htm, último acceso: 9 de agosto de 2023.

[37] Presidencia de la República, Secretaría General, Subdirección de Asuntos Jurídicos, decreto Nº 3.695, 2000, disponible en: http://www.planalto.gov.br/ccivil_03/decreto/d3695.htm, último acceso: 9 de agosto de 2023.

ridad Pública (SISP), en el ámbito del Sistema Brasileño de Inteligencia. Según el decreto, los integrantes del Subsistema deben "identificar, monitorear y evaluar las amenazas reales o potenciales a la seguridad pública y generar conocimientos e información que sustente acciones para neutralizar, frenar y reprimir actos delictivos de cualquier naturaleza". El SISP fue reglamentado mediante la resolución Nº 1 del 15 de julio de 2009, de la Secretaría de Seguridad Pública de la Nación, que delimitó las funciones y el ámbito de actuación de los organismos de inteligencia. Si bien la norma no alude específicamente a la inteligencia de fuentes abiertas, sí refiere al uso de la información y los datos y a su respectivo tratamiento estratégico.[38]

Por último, cabe mencionar a la Secretaría de Operaciones Integradas (SEOPI), perteneciente al ámbito del Ministerio de Justicia y Seguridad Pública, creada por el decreto Nº 9.662/2019, reglamentada por el decreto Nº 11.103/2022[39] y posteriormente disuelta mediante decreto Nº 11.348/2023.[40] Correspondía a la SEOPI, entre otras funciones: i) asesorar al ministro en las actividades de inteligencia y operativos policiales, con foco en la integración con los organismos internacionales, federales, estatales, municipales y distritales, así como cuerpos de seguridad pública; ii) implementar, mantener y modernizar las redes de integración y los sistemas nacionales de inteligencia de seguridad pública; y iii) promover la integración de las actividades de inteligencia de seguridad pública, en línea con las agencias de inteligencia federal, estatal, municipal y distrital que integran el Subsistema de Inteligencia de Seguridad Pública. El mismo decreto determina que es competencia de la Dirección de Inteligencia (art. 32): i) promover, con los órganos componentes del Sistema Brasileño de Inteligencia, el intercambio de datos y conocimientos, necesarios para la toma de decisiones administrativas y operativas por la Secretaría de Operaciones Integradas; y ii) planificar, supervisar y ejecutar acciones relacionadas con la obtención y análisis de datos para la producción de conocimiento de inteligencia de seguridad pública destinados a asesorar a la Secretaría de Operaciones Integradas.

[38] Cfme. al art. 7º de la res. Nº 1 del 15 de julio de 2009.

[39] Presidencia de la República, Secretaría General, Subdirección de Asuntos Jurídicos, decreto Nº 11.103, 2022, disponible en: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Decreto/D11103.htm, último acceso: 9 de agosto de 2023.

[40] Presidencia de la República, Secretaría General, Subdirección de Asuntos Jurídicos, decreto Nº 11.348, 2022, disponible en: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11348.htm, último acceso: 9 de agosto de 2023.

III.3. Colombia

La resolución Nº 5.839/2015 de la Policía Nacional de Colombia autoriza al Centro Cibernético Policial, parte de la dirección encargada de las investigaciones judiciales, a:

> 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 vulneración a la disponibilidad, integridad y confidencialidad de la información que circulan por el ciberespacio.[41]

El Código Procesal Penal, ley Nº 906 de 2004, establece en el artículo 242B la posibilidad de realizar "operaciones encubiertas en medios de comunicación virtual" a los funcionarios de la Fiscalía General de la Nación, ente encargado de investigar la comisión de delitos en Colombia, en investigaciones relacionadas con crimen organizado en las que "se verifique la posible existencia de hechos constitutivos de delitos cometidos por organizaciones criminales que actúan a través de comunicaciones mantenidas en canales cerrados de comunicación virtual". En todos los casos se deberá contar con una autorización previa por parte del juez de Control de Garantías.

La Ley de Inteligencia (Nº 1.621/2013) establece que los únicos organismos autorizados para llevar a cabo tareas de inteligencia y contrainteligencia son "las dependencias de las Fuerzas Militares y la Policía Nacional organizadas por estas para tal fin, la Unidad de Información y Análisis Financiero (UIAF)".[42] Además, su artículo 4º sujeta la actividad de inteligencia al "principio de reserva legal que garantiza la protección de los derechos a la honra, al buen nombre, a la intimidad personal y familiar, y al debido proceso".[43] El mismo artículo prohíbe que la información de inteligencia sea "recolectada, procesada o diseminada por razones de género, raza, origen nacional o familiar, lengua, religión, opinión política o fi-

---

[41] Ministerio de Defensa Nacional, Policía Nacional, Dirección General, resolución Nº 5.839, "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", 2015, disponible en: https://www.policia.gov.co/file/32305/download?token=OA0OIAOJ, último acceso: 17 de agosto de 2023.

[42] Ley Nº 1.621/2013, art. 3º.

[43] *Ibíd*., art. 4º.

losófica, pertenencia a una organización sindical, social o de derechos humanos, o para promover los intereses de cualquier partido o movimiento político o afectar los derechos y garantías de los partidos políticos de oposición".[44] El artículo 5º manda a que la actividad de inteligencia se sujete a estándares de necesidad, idoneidad y proporcionalidad.[45]

III.4. México

Las acciones de "ciberpatrullaje" estaban contempladas en el "Modelo homologado de las unidades de policía cibernética", del acuerdo 06/XLI/16, aprobado el 20 de diciembre de 2016 por el Consejo Nacional de Seguridad Pública. El modelo, que funciona como guía para las policías cibernéticas de los Estados de la unión, integra el eje "detección y atención oportuna de los delitos cibernéticos" del Programa Nacional de Seguridad Pública (2013-2018) del gobierno de Enrique Peña Nieto. Allí se detallan las tareas de "patrullaje cibernético" como tendientes 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, instituciones de los tres órdenes de gobierno (municipal, estatal, federal) y autoridades competentes.[46]

Tras la llegada al poder de Andrés Manuel López Obrador en 2018, la Policía Federal fue reemplazada por la Guardia Nacional (GN). En su ley orgánica se indica que esta tiene la facultad de "*vigilar, identificar, monitorear y rastrear* la red pública de internet sobre sitios web, bajo el supuesto de prevenir conductas delictivas".[47]

Asimismo, en octubre de 2020 la Secretaría de Seguridad y Protección Ciudadana (SSPC), a través del Secretariado Ejecutivo del Sistema Nacional de Segu-

---

[44] *Ibíd*.

[45] Ley Nº 1.621/2013, art. 5º.

[46] El destacado no pertenece al original. Gobierno de México, "Modelo homologado de unidades de policía cibernética", disponible en: https://www.gob.mx/cms/uploads/attachment/file/189189/Modelo_homologado_unidades_policia_cibernetica.pdf, último acceso: 9 de agosto de 2023.

[47] El destacado no pertenece al original. Art. 9º, fracción XXXVIII de la Ley de la Guardia Nacional, aprobada el 27 de mayo de 2019.

ridad Pública (SESNSP) y el Centro Nacional de Información (CNI)[48] presentó el "Sistema Multi-fuente para la estimación de la incidencia delictiva orientada a la inteligencia policial" (en adelante "sistema multi-fuente"), como parte del fortalecimiento del "Modelo nacional de Policía y Justicia Cívica".[49] El sistema multi-fuente se diseñó con la finalidad de reducir la cifra negra del crimen y contribuir a la inteligencia policial a través de "diez fuentes sólidas y complementarias" entre las que se cuenta el uso de datos y la inteligencia operable de fuentes abiertas (OSINT).[50]

No obstante las habilitaciones legales, las entidades que realizan "ciberpatrullaje" no publican información sobre la actividad. Por ello, no existe transparencia a propósito de qué información se busca y se recolecta, bajo qué supuestos, y qué tratamiento se hace de ella.

III.5. Uruguay

El funcionamiento de los organismos de inteligencia en Uruguay se rige por la ley Nº 19.696 del Sistema Nacional de Inteligencia del Estado (Ley del SNIE).[51] En su artículo 3º, esta norma define a las fuentes abiertas como "aquellas de las cuales se puede obtener un determinado informe, sin más restricción que la tarea que demanda su obtención", a diferencia de las cerradas, a las que define como "aquellas cuyo acceso es restringido y que para la obtención de la información es necesario el uso de medios y procedimientos especiales".

El artículo 3º literal E de la Ley del SNIE define a la inteligencia policial como la "actividad que comprende lo relativo a la obtención, procesamiento, análisis y distribución de información relativa a la prevención y eventual represión del delito común y el crimen organizado en su calidad de auxiliar de la Justicia, a través de la prevención y represión del delito". Se trata de una definición que funde

[48] "El Centro Nacional de Información (CNI) es un órgano desconcentrado de la SSPC; realiza tareas de inteligencia en pro de preservar la integridad, estabilidad y permanencia del Estado mexicano" (art. 19, Ley de Seguridad Nacional).

[49] El modelo nacional de Policía y Justicia Cívica fue aprobado el 8 de julio de 2019. Gobierno de México, "Modelo nacional de Policía y Justicia Cívica", 2020, disponible en: https://www.gob.mx/sesnsp/articulos/modelo-nacional-de-policia-y-justicia-civica-238637, último acceso: 9 de agosto de 2023.

[50] Gobierno de México, "Presentan SSPC-SESNSP Sistema Multifuente para la incidencia delictiva", 2020, disponible en: https://www.gob.mx/sspc/prensa/presentan-sspc-sesnsp-sistema-multifuente-para-la-incidencia-delictiva, último acceso: 9 de agosto de 2023.

[51] Centro de Información Oficial, Normativa y Avisos Legales Uruguay, ley Nº 19.696, 2018, disponible en: https://www.impo.com.uy/bases/leyes/19696-2018, último acceso: 9 de agosto de 2023.

el concepto de inteligencia policial con las actividades de represión del delito y de investigación criminal, lo que implica un potencial riesgo de expansión de la utilización de los informes y las tecnologías de inteligencia en las actividades de prevención y represión del delito, y en la esfera de los procesos penales.

A su vez, el artículo 20 de la Ley del SNIE[52] establece que ciertas operaciones de búsqueda de información constituyen "procedimientos especiales que pued[en] afectar la libertad y privacidad de los ciudadanos", y requieren previa autorización del Poder Judicial. La ley considera procedimientos especiales a "los que permiten el acceso a antecedentes relevantes contenidos en fuentes cerradas o que provienen de ellas". De esta forma encontramos que el concepto de "procedimientos especiales" se relaciona únicamente con fuentes "cerradas", por lo que no sería necesario requerir autorización judicial previa para realizar OSINT.

Por su parte, la Ley de Inteligencia autoriza a que el personal de los órganos que integran el Sistema Nacional de Inteligencia de Estado realice actividades en forma encubierta "para la obtención de antecedentes e informaciones" con previa autorización escrita de sus autoridades. Esto incluye "la eventual emisión de los documentos necesarios para proteger la identidad del personal involucrado". De lo anterior surge que la Ley de Inteligencia uruguaya tampoco exigiría orden judicial para crear perfiles falsos (artículo 21 de la Ley de Inteligencia); bastaría solamente con la autorización escrita de la autoridad administrative de un órgano que integra el SNIE. Tampoco existe una regulación legal de los procedimientos y plazos de actuación, del sistema de control y del reporte de información de este agente encubierto.

Finalmente, en el artículo 7º de dicha ley se encuentra la prohibición de los organismos de realizar por sí actividades de represión o investigación criminal, "salvo que dicha actividad se encuentre dentro de sus cometidos legales específicos".[53] De esta forma, las prohibiciones del artículo 7º no solucionan los problemas que genera la definición amplia y ambigua de inteligencia policial.

En tanto, la definición de "fuentes públicas" de la Ley de Protección de Datos Personales (Nº 18.331) no incluye internet.[54] La Unidad Reguladora y de Control de

---

[52] *Ibíd*.

[53] "Ningún órgano de inteligencia tendrá facultades compulsivas y les estará especialmente prohibido: 1) realizar tareas represivas; cumplir, por sí, funciones policiales o de investigación criminal, salvo que dicha actividad se encuentre dentro de sus cometidos legales específicos o mediante requerimiento judicial en el marco de una causa concreta".

[54] "Artículo 9º bis (…) se consideran como públicas o accesibles al público las siguientes fuentes o documentos: a) el Diario Oficial y las publicaciones oficiales, cualquiera sea su soporte de registro o canal de comunicación. b) Las publicaciones en medios masivos de comunicación, entendiendo por tales los provenientes de la prensa, cualquiera sea el soporte en el que

Datos Personales (URCDP) no considera a internet como fuente pública.[55] Pero este alcance limitado que la Ley de Protección de Datos Personales otorga al concepto de "fuentes públicas" no sería aplicable al tratamiento de estos datos con fines de inteligencia y seguridad pública. Esto es así porque los artículos 3º literal B[56] y el artículo 25[57] de la misma ley excluyen de su alcance al "tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las Fuerzas Armadas, organismos policiales o inteligencia" siempre que "resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas para la defensa nacional, la seguridad pública o para la represión de los delitos".

El profesor Rodrigo Rey plantea serias críticas a la Ley del SNIE y destaca que "es pasible de serias objeciones (entendemos que existen argumentos en favor de posibles inconstitucionalidades de algunas disposiciones) en cuanto a la técnica legislativa, y particularmente, estos cuestionamientos se trasladan a las fronteras porosas entre la producción de información de inteligencia y la actividad de investigación o instrucción".[58] Además de las deficiencias relacionadas con la definición misma de inteligencia policial, Rey también critica la falta de regulación sobre el diseño de los procedimientos de obtención de información, su gestión y posibilidad de acceso a esos datos:

---

figuren o el canal a través del cual se practique la comunicación. c) Las guías, anuarios, directorios y similares en los que figuren nombres y domicilios, u otros datos personales que hayan sido incluidos con el consentimiento del titular. d) Todo otro registro o publicación en el que prevalezca el interés general en cuanto a que los datos personales en ellos contenidos puedan ser consultados, difundidos o utilizados por parte de terceros. En caso contrario, se podrá hacer uso del registro o publicación mediante técnicas de disociación u ocultamiento de los datos personales".

[55] La URCDP en su dictamen Nº 10/020 del 23 de junio de 2020 expresa que "el artículo 9º bis de la ley Nº 18.331 no incluye a internet dentro del listado de fuentes públicas o accesibles al público, por lo que los datos de empresas provenientes de páginas amarillas o de otras páginas webs no son datos públicos o accesibles al público por el hecho de encontrarse allí publicados". Ver Gobierno de Uruguay, Unidad Reguladora y de Control de Datos Personales, dictamen Nº 10/020, 2020, disponible en: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/dictamen-n-10020, último acceso: 9 de agosto de 2023.

[56] "Artículo 3º. (…) No será de aplicación a las siguientes bases de datos: (…) b) Las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito".

[57] "Artículo 25. Base de datos correspondientes a las Fuerzas Armadas, organismos policiales o de inteligencia. (…) El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las Fuerzas Armadas, organismos policiales o inteligencia, sin previo consentimiento de los titulares, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquellos para la defensa nacional, la seguridad pública o para la represión de los delitos. Las bases de datos, en tales casos, deberán ser específicas y establecidas al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".

[58] Rey, Rodrigo, "La regulación del Sistema Nacional de Inteligencia de Estado, y una lectura introductoria sobre los procedimientos especiales de obtención de información", en: *Revista de Derecho Penal*, Nº 27, 2019, pp. 19-41, disponible en: https://revistas.fcu.edu.uy/index.php/penal/article/view/1915, último acceso: 9 de agosto de 2023.

Esto lleva a que sean las agencias administrativas quienes definan los eventos que dan lugar a la labor de inteligencia y no el legislador. En otras palabras, no existe un estándar legal mínimo de fundamentación y ese punto puede dar lugar a serias arbitrariedades. Tampoco se registran términos o plazos para la resolución y los posibles recursos y tampoco se prevé la posibilidad de prórroga, que justamente podría operar como control (efectivo, sobre los contenidos específicamente relevados y su pertinencia) sobre la ejecución de estos procedimientos.[59]

IV. Solicitudes de acceso a la información y prácticas constatadas

IV.1. Argentina

De las respuestas a los pedidos de acceso a la información pública cursados en Argentina a diversas dependencias públicas surge que solamente la Policía de la Ciudad de Buenos Aires y la Oficina Anticorrupción, dependiente del Poder Ejecutivo nacional, manifestaron utilizar herramientas OSINT. La Policía de la Ciudad de Buenos Aires refirió que "cuenta con una dependencia denominada Ciberpatrullaje, la cual realiza por orden judicial distintas tareas de análisis de fuentes abiertas en redes sociales de acceso público".

La Oficina Anticorrupción informó que la Coordinación de Admisión y Derivación de Denuncias no recopila información, sino que "se accede a información a través de bases abiertas o semiabiertas, a los efectos de resolver cada uno de los casos traídos a estudio, los cuales son debidamente agregados a los expedientes electrónicos que motivan las búsquedas". El organismo hizo saber que "dicha actividad investigativa se encuentra respaldada en el inciso e) del artículo 2º del Anexo I de la resolución MJSyDH Nº 1.316/08".[60]

Las demás dependencias consultadas –a excepción de la Agencia Federal de Inteligencia, que no contestó los pedidos de acceso a información– respondieron

[59] *Ibíd*.

[60] El art. 2º de la res. MJSyDH Nº 1.316/08 (reglamento interno de la Dirección de Investigaciones de la Oficina Anticorrupción) reza: "Artículo *2º.- Una vez formada una actuación, el* fiscal de Control Administrativo decidirá, en ejercicio de la facultad otorgada por el artículo 8º, inciso e) del decreto Nº 102/99: (…) e) previo a decidir en alguno de los sentidos precedentes, tanto el fiscal de Control Administrativo como el director de Investigaciones, o alguno de los investigadores administrativos (con conocimiento del fiscal de Control Administrativo), podrán realizar medidas probatorias preliminares con el fin de precisar la descripción de algún hecho, para verificar si ingresa dentro del ámbito de competencia fijado por el artículo 1º del decreto Nº 102/99 o si supera los criterios de significación determinados por el Plan de Acción de la Oficina".

que no realizan OSINT y que no han suscrito tampoco contratos con empresas privadas para contratar servicios de OSINT ni software que facilite esa tarea. No obstante, de la consulta de publicaciones en medios de prensa y de entrevistas a especialistas en la materia y a personas que practican o han practicado OSINT, se han podido constatar diversas instancias en las que el Estado ha practicado OSINT con fines de vigilancia.

IV.1.a. Ministerio de Seguridad de la Nación

En abril de 2020, durante la pandemia de covid-19, la entonces ministra de Seguridad, doctora Sabina Frederic, se refirió públicamente a la existencia de un plan de "ciberpatrullaje" destinado a "medir el humor social", basado fundamentalmente en el monitoreo de fuentes abiertas, particularmente redes sociales,[61] que derivó en la sanción de la resolución Nº 144/2020.

En 2016, la Policía Federal argentina allanó el domicilio de Nicolás Lucero, de 19 años, en la localidad de José León Suárez (provincia de Buenos Aires). Tras el allanamiento, Nicolás fue conducido a una comisaría, y agentes de esa fuerza requisaron su celular y los de su familia, y la netbook de su hermana.[62] Había sido acusado por el delito de intimidación pública a raíz de un tuit[63] –de evidente tono sarcástico– en el que refería al entonces presidente de la Nación. Nicolás debió transitar una causa penal en su contra, en la que fue sobreseído en sede judicial en el año 2018.[64]

En una situación similar, en abril de 2020, Kevin Guerra, un joven de 20 años oriundo de la localidad de Junín (provincia de Buenos Aires), escribió un tuit ironizando acerca de la demora en la percepción de las ayudas de emergencia proporcionadas por el Estado nacional en el marco de la pandemia del covid-19.[65] El tuit fue detec-

[61] Ver Diario Infobae, "Polémica revelación: la ministra de Seguridad admitió que las fuerzas a su cargo realizan ciberpatrullaje en redes sociales para 'detectar el humor social'", 2020, disponible en: https://www.infobae.com/politica/2020/04/09/polemica-revelacion-la-ministra-de-seguridad-admitio-que-las-fuerzas-a-su-cargo-realizan-ciberpatrullaje-en-redes-sociales-para-detectar-el-humor-social, último acceso: 9 de agosto de 2023.

[62] Lamas, Federico, "La increíble historia detrás del tuit contra Macri que terminó en la Justicia", Diario Popular, 2017, disponible en: https://www.diariopopular.com.ar/general/la-increible-historia-detras-del-tuit-contra-macri-que-termino-la-justicia-n327253, último acceso: 9 de agosto de 2023.

[63] Ver https://twitter.com/nicolucero69/status/765936986217668608, último acceso: 18 de agosto de 2023.

[64] Diario Perfil, "Declaran 'inocente' al joven que estuvo preso por un tuit contra Mauricio Macri", 2018, disponible en: https://www.perfil.com/noticias/sociedad/declaran-inocente-al-joven-que-escribio-un-tuit-contra-macri.phtml, último acceso: 9 de agosto de 2023.

[65] Disponible en: https://twitter.com/KevinGuerra99/status/1247709948554903554, último acceso: 9 de agosto de 2023.

tado por la Gendarmería Nacional –dependiente del Ministerio de Seguridad– en el marco de "tareas de ciberpatrullaje en redes sociales" y Kevin fue denunciado penalmente por esa fuerza. La causa judicial fue caratulada como "intimidación pública".[66] Finalmente, Kevin fue sobreseído. Según lo que informó el Centro de Estudios Legales y Sociales (CELS), que asumió su defensa, el tuit surgió de una búsqueda realizada por la Gendarmería Nacional al utilizar los términos "saquear, cuarentena, Argentina". Gendarmería fundó su actuación en la habilitación conferida por la resolución Nº 31/2018 del Ministerio de Seguridad de la Nación.[67]

Finalmente, debe destacarse el caso de los allanamientos a los "agitadores en redes" realizados en abril de 2020 en simultáneo y en diversas localidades de la provincia de Buenos Aires. En esa oportunidad se allanaron viviendas y se secuestraron teléfonos celulares y computadoras de diferentes personas que, según había detectado el Ministerio de Seguridad, habrían "incitado a la comisión de delitos" mediante el uso de perfiles falsos en redes sociales.[68]

IV.1.b. Ministerio de Relaciones Exteriores

Se ha denunciado que, en los meses previos a las reuniones de la Organización Mundial de Comercio (OMC) y del Grupo de los Veinte (G20) que se llevaron adelante en el país en los años 2017 y 2018, la Agencia Federal de Inteligencia (AFI) –a requerimiento del Ministerio de Relaciones Exteriores– realizó perfilamientos ilegales de periodistas, académicos, académicas y miembros de la sociedad civil que pretendían acreditarse o concurrir a esas reuniones, con el fin de determinar si su participación sería aceptada.[69] Con base en esos perfilamientos, se rechazaron 65 acreditaciones, e incluso algunos ciudadanos extranjeros, que decidieron ingresar al país a pesar de que su acreditación había sido rechazada, fueron deportados.[70]

66 Diario Ámbito, "Habló Kevin Guerra, detenido por twittear: 'Todo esto fue un chiste'", 2020, disponible en: https://www.ambito.com/informacion-general/bono/hablo-kevin-guerra-detenido-twittear-todo-esto-fue-un-chiste-n5095854, último acceso: 9 de agosto de 2023.

67 Centro de Estudios Legales y Sociales (CELS), "La justicia federal sobreseyó a Kevin Guerra por sus expresiones en Twitter", 2021, disponible en: https://www.cels.org.ar/web/2021/01/la-justicia-federal-sobreseyo-a-kevin-guerra-por-sus-expresiones-en-twitter, último acceso: 9 de agosto de 2023.

68 A24, "En medio de la pandemia por coronavirus, se realizaron 20 allanamientos contra agitadores en las redes sociales", 2020, disponible en: https://www.a24.com/policiales/medio-pandemia-coronavirus-realizaron-20-allanamientos-agitadores-redes-sociales-09042020_umqdiP2qx, último acceso: 9 de agosto de 2023.

69 Diario Ámbito, "Piden la indagatoria de Arribas y Majdalani por espionaje ilegal en las cumbres de la OMC y el G20", 2021, disponible en: https://www.ambito.com/politica/espionaje/piden-la-indagatoria-arribas-y-majdalani-ilegal-las-cumbres-la-omc-y-el-g20-n5180581, último acceso: 9 de agosto de 2023.

70 CELS, "Reunión de la OMC en la Argentina: acreditaciones rechazadas y deportaciones", 2017, disponible en: https://

Según un comunicado oficial de Cancillería, las personas a quienes se les denegó su acreditación "habían hecho explícitos *llamamientos a manifestaciones de violencia a través de las redes sociales*, expresando su vocación de generar esquemas de intimidación y caos".[71] De las propias afirmaciones del Ministerio se sigue que se llevó a cabo inteligencia con base en fuentes abiertas para realizar perfilamientos políticos, explícitamente prohibidos por la Ley de Inteligencia.

IV.1.c. Administración Federal de Ingresos Públicos

En noviembre de 2022 y tras una investigación publicada en la prensa,[72] trascendió que la Administración Federal de Ingresos Públicos (en adelante, AFIP) –la agencia recaudadora del Gobierno nacional– denunció ante una fiscalía especializada en ciberdelincuencia la actividad de personas que, presuntamente, ofre-

www.cels.org.ar/web/2017/12/wto-meeting-in-argentina-rejected-accreditations-and-deportations, último acceso: 9 de agosto de 2023.

[71] El destacado no pertenece al original. No fue posible acceder al comunicado original. El texto citado corresponde a la captura que se muestra, la cual fue obtenida del sitio web del CELS, y se encuentra en Ministerio de Relaciones Exteriores, Comercio Internacional y Culto, Argentina, "Sobre la acreditación de ONG's a la Conferencia Ministerial de la OMC en Buenos Aires", 2017, disponible en: https://cancilleria.gob.ar/es/actualidad/comunicados/sobre-la-acreditacion-de-ongs-la-conferencia-ministerial-de-la-omc-en-buenos, último acceso: 9 de agosto de 2023.

[72] Martínez, Belkis, "'Estafa': venden por $500.000 un documento clave de la AFIP", Diario La Nación, 2022, disponible en: https://www.lanacion.com.ar/economia/campo/estafa-venden-por-500000-un-documento-clave-de-la-afip-nid29112022, último acceso: 9 de agosto de 2023.

cían cartas de porte (un documento electrónico obligatorio emitido por la propia AFIP que ampara el transporte de granos automotor y ferroviario) apócrifas en redes sociales. Al recibir la información y en forma previa a efectuar la denuncia, "la División Penal Tributaria [de la AFIP] realizó tareas de investigación en redes sociales abiertas pudiendo dar con diferentes perfiles y publicaciones en la red social Facebook donde se ofrecían estos documentos con el fin de simular operaciones", pero advirtieron que no pudieron obtener datos".[73]

IV.1.d. Agencia Federal de Inteligencia

La Agencia Federal de Inteligencia no contestó el pedido de acceso a la información pública cursado en el marco de esta investigación. Sin embargo, se ha constatado la realización de tareas OSINT por parte de esta dependencia.

En 2020, la entonces interventora de la AFI denunció haber encontrado, en la sede de la Agencia, carpetas que contenían fichas de inteligencia sobre periodistas, políticos, asociaciones de la sociedad civil y académicos.[74] Una fuente de la Agencia Federal de Inteligencia expresó a la prensa que "aunque *las fichas de los periodistas están hechas en base a fuentes abiertas, como las redes sociales*, la recopilación de esa información está prohibida por la Ley de Inteligencia".[75] Muchas habían sido generadas en el ya descrito contexto del proceso de acreditación previo a las reuniones de la OMC y el G20 en Argentina, en los años 2017 y 2018, respectivamente. Tras el cambio de administración, la Agencia entregó las carpetas de inteligencia a los damnificados.[76] Allí se puede observar la utilización de OSINT y otras formas de inteligencia para construir sus perfiles.

---

[73] Martínez, Belkis, "La AFIP presentó una denuncia por la supuesta venta ilegal y millonaria de un documento clave", Diario La Nación, 2022, disponible en: https://www.lanacion.com.ar/economia/campo/la-afip-presento-una-denuncia-por-la-supuesta-venta-ilegal-y-millonaria-de-un-documento-clave-nid05122022/, último acceso: 9 de agosto de 2023.

[74] Pizzi, Nicolás, "La AFI denunció ante la Justicia que durante el gobierno de Mauricio Macri se hizo inteligencia ilegal contra organizaciones sociales y periodistas", Diario Infobae, 2020, disponible en: https://www.infobae.com/politica/2020/06/05/la-afi-denuncio-ante-la-justicia-que-durante-el-gobierno-de-mauricio-macri-se-hizo-inteligencia-ilegal-contra-organizaciones-sociales-y-periodistas, último acceso: 9 de agosto de 2023.

[75] El resaltado no pertenece al original. Pizzi, Nicolás, "Las fichas de inteligencia que elaboró la AFI durante el gobierno de Macri sobre las personas que asistieron a las cumbres del G20 y la OMC", Diario Infobae, 2020, disponible en: https://www.infobae.com/politica/2020/06/07/que-dicen-las-fichas-que-armaba-la-afi-en-la-previa-del-g20-y-la-reunion-de-la-omc-en-buenos-aires, último acceso: 9 de agosto de 2023.

[76] Un periodista de la Editorial Perfil compartió el contenido de la carpeta que respecto suyo la AFI había confeccionado. Ver Recalt, Rodis, "Exclusivo: las carpetas del espionaje", Revista Noticias, 2021, disponible en: https://noticias.perfil.com/noticias/politica/exclusivo-las-carpetas-del-espionaje.phtml, último acceso: 9 de agosto de 2023.

IV.1.e. Policía de la Ciudad de Buenos Aires

Aunque en su respuesta a la solicitud de información pública formulada por esta investigación, la Policía de la Ciudad informó que la división "Ciberpatrullaje" de esa fuerza sólo realiza OSINT por orden judicial, se ha constatado su empleo en al menos dos instancias que exceden el contexto referido.

En julio de 2016, la Policía de la Ciudad de Buenos Aires detuvo a dos jóvenes que habían posteado amenazas al entonces presidente de la Nación Mauricio Macri en la red social Twitter. La publicación consistía en la leyenda "Nos vemos pronto, @mauriciomacri" acompañada de una imagen de explosivos e inscripciones en árabe. El entonces secretario de Seguridad del Gobierno porteño, Marcelo D'Alessandro, expresó a la prensa que los detenidos por estos mensajes "son un ejemplo de que estamos atentos a este tipo de hechos, que intentan llevar temor a la población, y que contamos con la tecnología y la decisión necesarias para ir buscar a los responsables sin perder tiempo".[77] La nota de prensa de la que fue extraída esta información indica que también participó de la investigación personal del Ministerio de Seguridad de la Nación.

Por otra parte, esta investigación consiguió entrevistar a una persona que trabajó en esta fuerza de seguridad, quien ha realizado tareas de OSINT.[78] Expresó que las búsquedas se ejecutaban a solicitud del Poder Judicial, y que en ellas se recababa "información sobre personas en general", lo cual incluye información sobre personas individualizadas. En cuanto al procedimiento, hizo saber que "existe un procedimiento informal que depende un poco del criterio de la Justicia. El protocolo es igual que cuando mi hijo quiere averiguar con quién anda su ex. Ven la cara del chico y después se fijan en todas las redes sociales hasta dar cuenta de quién es, con quién se junta, etc.". Finalmente, hizo saber que la Policía de la Ciudad también entiende como una habilitación a la práctica de OSINT lo normado en el artículo 10º de la ley Nº 5.847 "Régimen integral para eventos futbolísticos de la Ciudad Autónoma de Buenos Aires", que crea la Base de Antecedentes sobre Violencia en Eventos Futbolísticos de la CABA y dispone que:

> la autoridad competente, en uso de facultades preventivas, y en ocasión del evento, deberá impedir el acceso a los predios y la permanencia en los mismos de las personas de las que, por razonables pautas objetivas,

[77] Diario Clarín, "Amenazaron con mensajes en árabe que iban a atentar contra Macri", 2016, disponible en: https://www.clarin.com/policiales/amenazaron-mensajes-arabe-atentar-macri_0_SJNELzqO.html, último acceso: 9 de agosto de 2023.

[78] Entrevista realizada el 27 de octubre de 2022. La persona entrevistada solicitó mantener en reserva su identidad.

se presuma que puedan alterar el orden en el marco de un evento futbolístico. Dicha determinación preventiva deberá notificarse a la entidad involucrada a fin de que manifieste su voluntad de ejercer el derecho de admisión en eventos futbolísticos futuros.

IV.2. Brasil

En la realización de este estudio se cursaron diversos pedidos de acceso a la información pública a múltiples dependencias del Estado brasileño. El Centro de Inteligencia de la Marina, la Agencia Brasileña de Inteligencia (ABIN) y la Policía Federal declinaron contestar; se ampararon en la naturaleza de las actividades de inteligencia, o alegaron motivos de seguridad.

IV.2.a. Ministerio Público Federal

El Ministerio Público Federal hizo saber que todas las áreas de la Secretaria de Perícia, Pesquisa e Análise (SPPEA, por su nombre en portugués) recolectan datos de fuentes abiertas. En ese sentido, la sociedad civil ya ha alertado acerca de la utilización de OSINT en el marco de investigaciones realizadas por ministerios públicos federales y estatales.[79]

IV.2.b. Policía Militar

La Policía Militar también ha efectuado vigilancia de redes sociales mediante técnicas OSINT. Así lo atestigua el caso de João Reginaldo da Silva Júnior, de 24 años, oriundo de Uberlândia, quien, en el marco de la visita a su ciudad del entonces presidente Jair Bolsonaro, escribió en su cuenta de Twitter: "Gente, Bolsonaro mañana en Udia… ¿Hay alguien que busca convertirse en héroe nacional?". João fue detenido luego de que la Policía Militar catalogara su publicación como "propaganda e incitación a cometer delitos contra la integridad física y la vida del Hon. Presidente de la República Jair Messias Bolsonaro con promesas que tales amenazas se materializarían durante su paso por esta ciudad de Uberlândia en

[79] Asociación para el Progreso de las Comunicaciones, Artículo 19 Brasil y América del Sur, Derechos Digitales e Intervozes, Examen Periódico Universal del Consejo de Derechos Humanos de la ONU, 41º período de sesiones, "Contribución conjunta de las partes interesadas", 2022, § 28, disponible en: https://www.apc.org/sites/default/files/upr_brazil-sp-final.pdf, último acceso: 14 de agosto de 2023.

la fecha de hoy".[80] Aunque fue liberado a las pocas horas,[81] la causa judicial en su contra siguió su curso. Según fue reportado en la prensa, el Ministerio Público Federal (MPF) propuso un acuerdo de transacción criminal para João –y otras seis personas que publicaron mensajes sobre Bolsonaro en Twitter durante su visita a Uberlândia–. La propuesta prevé una multa de veinte mil reales (R$20.000) para los involucrados que, de ser aceptada, evitaría la prosecución del proceso judicial en su contra. Los abogados de João informaron que desestimarían la propuesta.[82]

IV.2.c. Ministerio de Defensa

El Ministerio de Defensa manifestó haber encontrado en sus registros contratos con terceros que les proveen servicios OSINT. Entre otros, refirió al contrato 01/2021 suscripto con la empresa Supernova Serviços de Informação LTDA, con el objeto de la "prestación de servicios de monitoreo de redes sociales". Los términos del contrato establecen que se trata de un monitoreo permanente "(24x7)", por el período de un año, de "la imagen del organismo en las redes sociales, incluyendo blogs", y que "el resultado de la acción debe indicar repercusión (qué), perfiles de influencia (quién), medios (dónde, cuándo), reputación y polarización (cómo), tendencia, escenario brasileño y otras informaciones estratégicas oportunas para la toma de decisiones, como el *engagement* negativo".[83]

IV.2.d. Presidencia de la Nación

Se ha denunciado que la Secretaría de Comunicaciones de la Presidencia firmó un contrato con una empresa privada en virtud del cual se realizó el perfilamiento de 77 periodistas e influenciadores en redes sociales. Los objetivos perfilados fueron clasificados en tres grupos, con base en la simpatía de sus publicacio-

[80] Rodrigues, Fabiano, "Jovem é preso em flagrante após publicação sobre visita de Bolsonaro a Uberlândia", G1 Triângulo e Alto Paranaíba, 2021, disponible en: https://g1.globo.com/mg/triangulo-mineiro/noticia/2021/03/04/jovem-e-preso-apos-publicacao-sobre-vinda-de-bolsonaro-a-uberlandia.ghtml, último acceso: 14 de agosto de 2023.

[81] *Ibíd*.

[82] Borge, Luis Fellipe, "MPF propõe multa de R$ 20 mil a jovem detido por publicação sobre visita de Bolsonaro em MG", G1 Triângulo e Alto Paranaíba, 2023, disponible 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, último acceso: 14 de agosto de 2023.

[83] Disponible para su descarga en Gobierno de Brasil, Ministerio de Defensa, "Contratos formalizados na administração central do Ministério da Defesa (ACMD)", 2019, disponible en: https://www.gov.br/defesa/pt-br/acesso-a-informacao/licitacoes-e-contratos-1/contratos-vigentes-na-administracao-central-do-ministerio-da-defesa-acmd-1/contratos-formalizados-na-administracao-central-do-ministerio-da-defesa-acmd, último acceso: 14 de agosto de 2023.

nes respecto del Gobierno: "favorable", "neutral informativo" y "detractor". Este "mapa de influenciadores" contenía también la recomendación acerca de las "acciones a seguir" respecto de cada persona perfilada.[84] El documento contenía además los teléfonos y las direcciones de correo electrónico de los objetivos observados.[85]

IV.2.e. Ministerio de Justicia

El Ministerio de Justicia informó que no realiza OSINT. Sin embargo, es importante señalar el caso del llamado "dosier antifascista". El dosier era un documento confidencial elaborado por la Secretaría de Operaciones Integrales (SEOPI) del Ministerio de Justicia, que mapeaba y vigilaba a 579 funcionarios federales y estatales de diversas áreas de seguridad, burocracia estatal y universidades que fueron identificados como miembros del "movimiento antifascismo".[86] El dosier contenía, además de información de los funcionarios, una serie de datos tomados de fuentes abiertas, como nombre, dirección, fotografía, URL de redes sociales y otros datos. El documento fue circulado entre los organismos de seguridad pública y de inteligencia.

Un documento similar, producido por Douglas García, diputado estatal por San Pablo, que contenía información y datos personales de más de mil personas consideradas "terroristas", fue entregado al Gobierno estadounidense por Eduardo Bolsonaro, diputado federal e hijo del expresidente, según lo reportado por la prensa.[87] El 19 de agosto de 2020, el Supremo Tribunal Federal de Brasil suspendió la elaboración del dosier y, en mayo de 2022, el pleno de ese tribunal lo declaró inconstitucional.[88]

---

[84] Valente, Rubens, "Relatório do governo separa em grupos jornalistas e influenciadores", UOL, 2020, disponible en: https://noticias.uol.com.br/colunas/rubens-valente/2020/12/01/governo-bolsonaro-jornalistas-redes-sociais.htm, último acceso: 14 de agosto de 2023.

[85] Valente, Rubens, "Veja a lista de jornalistas e influenciadores em relatório do governo", UOL, 2020, https://noticias.uol.com.br/colunas/rubens-valente/2020/12/01/lista-monitoramento-redes-sociais-governo-bolsonaro.htm, último acceso: 14 de agosto de 2023.

[86] Valente, Rubens, "Ação sigilosa do governo mira professores e policiais antifascistas", UOL, 2020, disponible en: https://noticias.uol.com.br/colunas/rubens-valente/2020/07/24/ministerio-justica-governo-bolsonaro-antifascistas.htm, último acceso: 14 de agosto de 2023. Observatorio Legislativo CELE, boletín de junio de 2022, disponible en: https://observatoriolegislativocele.com/boletin-mensual-observatorio-legislativo-junio-2022, último acceso: 14 de agosto de 2023.

[87] Carta Capital, "Eduardo Bolsonaro entregou dossiê de antifascistas aos EUA, diz deputado à Justiça", 2020, disponible en: https://www.cartacapital.com.br/politica/eduardo-bolsonaro-entregou-dossie-de-antifascistas-aos-eua-diz-deputado-a-justica, último acceso: 14 de agosto de 2023.

[88] El contenido de la sentencia se encuentra en Supremo Tribunal Federal, "Rede Sustentabilidade c. Bruno Lunardi Goncalves y otros", 2020, disponible en: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5967354, último acceso: 14 de agosto de 2023.

En cuanto a la adquisición de software para la práctica de OSINT, el 19 de mayo de 2021, el Ministerio de Justicia lanzó el aviso de licitación Nº 03/2021, con el objetivo de atender las necesidades operativas de la Dirección de Inteligencia de la SEOPI. El objeto del concurso implicaba "la adquisición de una solución de inteligencia en fuentes abiertas, social media, deep y dark web, que comprende el suministro, la instalación y la configuración, así como el apoyo técnico, en respuesta a las necesidades operativas de la Dirección de Inteligencia de la Secretaría de Operaciones Integradas (DINT/SEOPI)". La ganadora del concurso fue la empresa Harpia Tech. Según la información suministrada por la propia empresa durante el concurso, "el programa que ofrece la compañía monitorea 5.722 fuentes, repartidas en 112 países". Por su parte, la propuesta explicaba que "por fuente se entiende: red social, canal en un grupo de mensajes, foro en la dark web, etc." y que entre las fuentes que el programa monitorea se encontraban "fuentes que reflejan los siguientes fenómenos: hacktivismo, delitos cibernéticos, publicaciones académicas, *exploits*, *scripts*, herramientas de ataque, espionaje cibernético, datos abiertos publicados por empresas de seguridad, grupos de comunicación e instituciones de investigación".[89] En el año 2021, un grupo de organizaciones de la sociedad civil habían logrado una medida cautelar que frenó el proceso de contratación del Ministerio de Justicia con esta empresa, pero en 2022 el Tribunal de Cuentas de la Unión dejó sin efecto la medida y liberó su contratación.[90]

IV.3. Colombia

De los términos de la resolución Nº 5.839/2015 de la Policía Nacional surge que solo el Centro Cibernético Virtual de la Policía Nacional está habilitado a realizar "ciberpatrullaje", y "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 vulneración a la disponibilidad, integridad y confidencialidad de la información que circulan por el ciberespacio". No obstante, se ha detectado que bajo el amparo de la mencionada normativa se llevan a cabo acti-

[89] Zanatta, Rafael A., "O que sabemos sobre o Harpia Tech?", Data Privacy BR, 2022, disponible en: https://www.dataprivacybr.org/o-que-sabemos-sobre-a-harpia-tech, último acceso: 14 de agosto de 2023.

[90] Hirabahasi, Gabriel, "TCU libera contrato do Ministério da Justiça para sistema de inteligência", CNN Brasil, 2022, disponible en: https://www.cnnbrasil.com.br/nacional/tcu-libera-contrato-do-ministerio-da-justica-para-uso-de-sistema-espiao-pegasus, último acceso: 14 de agosto de 2023.

vidades OSINT en supuestos diferentes al habilitado por la norma (investigación de ciberdelitos),[91] e incluso por entidades diferentes a la Policía Nacional.

IV.3.a. Fiscalía General de la Nación

La Fiscalía General de la Nación informó a esta investigación que, si bien no cuenta con una dependencia específicamente encargada de la tarea, hace consultas de fuentes abiertas, en el marco de lo preceptuado en el artículo 244 del Código de Procedimiento Penal, que establece que "la Policía Judicial, en desarrollo de su actividad investigativa, podrá realizar las comparaciones de datos registradas en bases mecánicas, magnéticas u otras similares, siempre y cuando se trate del simple cotejo de informaciones de acceso público".

IV.3.b. Policía Nacional

De las respuestas a los pedidos de acceso a la información enviados por esta investigación, surge que la Policía Nacional ha suscrito "contratos con entidades que proveen servicios para la realización de actividades de ciberpatrullaje en fuentes abiertas".

Sumado a ello, según surge de las respuestas a pedidos de acceso a la información radicados por la Fundación para la Libertad de Prensa (FLIP) y Fundación Karisma, "las actividades de ciberpatrullaje comprenden la consulta, observación y recolección de información en línea sobre datos y contenidos abiertos y públicos en internet y redes sociales".[92] Además, en una declaración pública en 2021, el exdirector de la Policía, Jorge Luis Vargas, se refirió al asunto y señaló que el ciberpatrullaje es como el patrullaje ordinario, pero llevado a cabo en internet, y que "en ese espacio público, en donde la ley lo permite, la autoridad debe ejercer ese servicio de vigilancia".[93]

---

[91] Ello en contra de la posición de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos en la materia, que propone evitar englobar, bajo el concepto de "ciberseguridad", conductas criminales que no están dirigidas a atentar contra la integridad de las redes y la infraestructura de internet. Ver CIDH, "Libertad de expresión e internet", informe de la Relatoría Especial para la Libertad de Expresión, OEA/Ser.L/V/II, CIDH/RELE/INF.11/13, 31 diciembre 2013, §§ 118 y 119, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf, último acceso: 14 de agosto de 2023.

[92] Camacho Gutiérrez, Lucía, Ospina Celis, Daniel y Upegui Mejía, Juan Carlos, *Inteligencia estatal en internet y redes sociales: el caso colombiano*, Bogotá, Dejusticia, 2022, p. 31, disponible en: https://www.dejusticia.org/wp-content/uploads/2022/12/InteligenciaEstatalEnInternet-Web-Dic23.pdf, último acceso: 14 de agosto de 2023.

[93] Revista Semana, "¿Qué es el ciberpatrullaje?", 2021, disponible en: https://ne-np.facebook.com/RevistaSemana/videos/qu%C3%A9-es-el-ciberpatrullaje/438397297775230/?__so__=permalink&__ rv__=related_videos, último acceso: 14 de agosto de 2023.

Durante las jornadas del paro nacional de 2021, se reportó que las autoridades colombianas se encontraban realizando monitoreo masivo de internet, tendiente a identificar "contenidos presuntamente falsos sobre el desarrollo de las protestas, desprestigio de la imagen de las fuerzas públicas, así como la instigación al odio público. Estas medidas tendrían como fin determinar qué información es falsa o verdadera y, de esta manera, combatir supuestas actividades de 'terrorismo digital' que pudieran tener el potencial de exacerbar la violencia".[94] El Estado colombiano informó a la Comisión Interamericana de Derechos Humanos (CIDH) que, en ese marco, se llevaron adelante "21.675 horas de ciberpatrullaje y que se identificaron al menos 154 noticias falsas y más de 2.300 publicaciones que contienen amenazas a la vida o la integridad física".[95] También durante el paro nacional, la Policía recolectó información sobre los manifestantes a través del monitoreo de sus redes sociales. Este monitoreo llevó a la individualización y la detención de varios de ellos.[96]

Por todo lo anterior, la CIDH formuló al Gobierno la recomendación de "cesar las actividades de categorización policial de contenidos como 'falsos' o 'verdaderos' y abstenerse de asignar calificaciones estigmatizantes o tendientes a la criminalización de quienes se expresan a través de internet sobre las protestas".[97]

IV.3.c. Ejército de Colombia

En el año 2020, trascendió en la prensa que el Ejército había llevado adelante un programa de seguimiento informático sobre más de 130 objetivos de inteligencia, entre los que se contaban políticos, dirigentes sindicales y organizaciones de la sociedad civil. En el marco de ese programa, "por medio de herramientas informáticas y de software, realizaron búsquedas y recolectaron masiva e indiscriminadamente toda la información posible de sus objetivos para elaborar informes de inteligencia militar. Teléfonos, direcciones de residencia y trabajo, correos electrónicos, amigos, familiares, hijos, colegas, contactos, infracciones

[94] CIDH, Organización de los Estados Americanos (OEA), "Visita de trabajo a Colombia: observaciones y recomendaciones. Visita: junio 2021", 2021, § 176, disponible en: https://www.oas.org/es/cidh/informes/pdfs/ObservacionesVisita_cidh_Colombia_spA.pdf, último acceso: 14 de agosto de 2023.

[95] Reporte escrito del Estado a la CIDH, 8 de junio de 2021, p. 64, citado en CIDH-OEA, *supra* nota 94, § 176.

[96] Fundación Karisma, "Sobre la estigmatización a integrantes de la 'primera línea' y a creadores de contenido", 2022, disponible en: https://web.karisma.org.co/sobre-las-recientes-capturas-a-integrantes-de-la-primera-linea-y-a-creadores-de-contenido, último acceso: 14 de agosto de 2023.

[97] Reporte escrito del Estado a la CIDH, 8 de junio de 2021, p. 64, citado en CIDH-OEA, *supra* nota 94, recomendación Nº 40.

de tráfico y hasta lugares de votación forman parte de estos perfiles".[98] Algunos funcionarios del Ejército habrían intentado justificar este accionar bajo la premisa de que se trataba de información que había sido recopilada de fuentes abiertas.

También en 2020, el Ejército Nacional creó una lista de usuarios[99] en su cuenta oficial de Twitter (@col_ejercito), a la que tituló "Oposición", y en la que incluyó 33 cuentas de medios de comunicación, periodistas, organizaciones sociales, militantes y dirigentes políticos (incluido, por ejemplo, Gustavo Petro), activistas de derechos humanos, organizaciones internacionales (entre ellas, la cuenta de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos), e incluso la cuenta de la Jurisdicción Especial para la Paz de Colombia. Luego de que la situación tomara estado público, el Ejército emitió un comunicado en el que refirió que se trató de una decisión equivocada, y borró (u ocultó) la lista.[100]

IV.3.d. Detección de noticias falsas en el marco de la pandemia

Durante el año 2020, el Puesto de Mando Unificado de Ciberseguridad[101] relevó la actividad en internet en busca de "noticias falsas". En la respuesta a un pedido de acceso a la información formulado por la FLIP,[102] esa fuerza indicó que "logra la identificación de noticias falsas a partir de la información publicada en fuertes abiertas". Entre el 30 de marzo y el 26 de abril de ese año, la Policía Nacional publicó diariamente los reportes acerca de las *fake news* que identificó en internet.[103]

[98] Revista Semana, "Las carpetas secretas", 2020, disponible en: https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616, último acceso: 14 de agosto de 2023.

[99] Respecto de las listas de usuarios, ver Centro de Ayuda Twitter, "Cómo usar las listas de Twitter", disponible en: https://help.twitter.com/es/using-twitter/twitter-lists, último acceso: 14 de agosto de 2023.

[100] Ver https://twitter.com/cuestion_p/status/1237382254952763392, último acceso: 14 de agosto de 2023, y https://twitter.com/flip_org/status/1237499772069711874, último acceso: 14 de agosto de 2023.

[101] El Puesto de Mando Unificado de Ciberseguridad estaba integrado por la Presidencia de la República (CSIRT Presidencia), el Ministerio de Defensa (COLCERT), el Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC), la Fiscalía General de la Nación, las Fuerzas Militares (CCOCI), la Policía Nacional y la Dirección General de Inteligencia.

[102] Ministerio de Defensa Nacional, Policía Nacional, Dirección de Investigación Criminal e Interpol, Nº GS-2021, DIJIN-CE-CIP-1.10, 2021, disponible en: https://drive.google.com/file/d/1Z7AKesIM_LY5Jde8tH2mQnDbyNZCc2a-/view, último acceso: 14 de agosto de 2023.

[103] Reportes en República de Colombia, Policía Nacional, "Reporte de noticias falsas detectadas por CAI virtual", 2020, disponible en: https://www.policia.gov.co/reporte-fakenews, último acceso: 14 de agosto de 2023.

IV.3.e. Presidencia de la República

Durante el año 2020, la Fundación para la Libertad de Prensa (FLIP) publicó un informe en el cual se advirtió que la Presidencia de la República habría contratado a la firma de marketing Du Brands para hacer un seguimiento a más de 450 cuentas de influenciadores en redes sociales. Cada uno de ellos fue perfilado como "positivo", "neutro" o "negativo" en función de si su contenido era favorable o no a las posiciones políticas del Gobierno.[104] Una de las personas perfiladas interpuso una acción de tutela contra el Gobierno por entender que en la confección de la lista se había violado su derecho al hábeas data. El caso llegó a la Corte Suprema, que falló a favor del demandante, en tanto su inclusión –sin autorización previa, en una lista en virtud de un dato sensible como su filiación política– viola su derecho fundamental de hábeas data. Ello, sin perjuicio de que el dato en cuestión hubiera sido hecho público por el accionante.[105]

IV.4. México

En ausencia de información pública detallada y transparente sobre el uso de inteligencia de fuentes abiertas, se enviaron solicitudes de acceso a la información a la Secretaría de Seguridad y Protección Ciudadana (SSPC), a la Guardia Nacional (GN) y al Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP). Todas las dependencias citadas respondieron que no cuentan con los datos pertinentes respecto de las prácticas de recolección de datos e información a través de fuentes abiertas ni contratos con empresas privadas para la realización de OSINT. Sin embargo, se han podido constatar que al menos las siguientes dependencias estatales han practicado OSINT con fines de vigilancia.

IV.4.a. Centro Nacional de Inteligencia

El Sistema Multi-fuente del Centro Nacional de Inteligencia (CNI) tiene por ob-

[104] El Espectador, "La lista de influenciadores a los que la Presidencia les pone el ojo", 2020, disponible en: https://www.elespectador.com/politica/la-lista-de-influenciadores-a-los-que-la-presidencia-les-pone-el-ojo-article, último acceso: 14 de agosto de 2023. Revista Semana, "Positivo, negativo, neutro: lista de influenciadores perfilados por el Gobierno", 2020, disponible en: https://www.semana.com/nacion/articulo/positivo-negativo-neutro-lista-de-influenciadores-perfilados-por-el-gobierno/697304, último acceso: 14 de agosto de 2023.

[105] República de Colombia, Corte Suprema de Justicia, sentencia Nº STP9319-2020 del 27 de octubre de 2020, Sala de Casación Penal, Sala de Decisión de Tutelas Nº 1, disponible en: https://cortesuprema.gov.co/corte/index.php/2021/02/22/derecho-al-habeas-data, último acceso: 14 de agosto de 2023.

jeto que las unidades de análisis de las instituciones de seguridad pública puedan integrar la información de manera efectiva y eficiente.[106] Ello no obsta a que el sistema utilice información disponible en las redes sociales para "conocer el comportamiento de las personas y las estructuras sociales que se forman en comunidad" y detectar "conductas delictivas y antisociales" mediante el "monitoreo constante de las redes sociales", para que las autoridades se puedan "anticipar a probables hechos delictivos que pongan en riesgo la seguridad de la población" e "implementar acciones preventivas y, con ello, evitar que los riesgos detectados escalen".[107] El Sistema también es utilizado para "analizar las redes de vínculos entre actores o agentes relevantes para alguna investigación".[108]

Entrevistada por esta investigación, una persona cercana al CNI manifestó que esa entidad entiende como fuentes abiertas "por ejemplo, [lo] que las personas suben a las redes sociales: un video, o la descripción de un hecho. Básicamente, es información pública que está en las redes sociales que sube alguna persona". Hizo saber además que el Sistema no prevé protocolos específicos que lo regulen o que limiten las prácticas OSINT.[109]

Sumado a lo anterior, una nota periodística[110] reveló que uno de los Centros Regionales de Fusión de Inteligencia (CERFI), ubicado en el 27º Batallón de Infantería en Iguala, Guerrero, realiza actividades de monitoreo e intervención de comunicaciones privadas. Allí también se señala que el CERFI efectúa intercepción de llamadas, geolocalización, acceso a redes sociales y recuperación de datos. Se destaca, además, una plataforma integral de inteligencia que opera con un módulo de OSINT, con el cual recolectan datos de las plataformas de redes sociales.

IV.4.b. Guardia Nacional

De conformidad con el Censo Nacional de Seguridad Pública Federal 2021, durante el año 2020 la División Científica de la Guardia Nacional, a través del "mo-

[106] Modelo Nacional de Policía y Justicia Cívica, "Sistema multi-fuente para la estimación de la incidencia delictiva orientada a la inteligencia policial", 2020, p. 15, disponible en: https://www.gob.mx/cms/uploads/attachment/file/590581/sistema_multi-fuente_PP.pdf, último acceso: 14 de agosto de 2023.

[107] *Ibíd*., p. 28.

[108] *Ibíd*., p. 28.

[109] Artículo 19, entrevista a colaborador del CNI, 20 de octubre de 2022.

[110] Ocampo Torres, Lenin, "En Iguala funciona un centro regional de espionaje del Ejército, revela el hackeo del grupo Guacamaya", El Sur, 2022, disponible en: https://suracapulco.mx/en-iguala-funciona-un-centro-regional-de-espionaje-del-ejercito-revela-el-hackeo-del-grupo-guacamaya, último acceso: 14 de agosto de 2023.

nitoreo cibernético" de internet, identificó y desactivó 5.920 sitios web por actividades ilegales; entre ellos 342 sitios por robo de datos financieros y personales.[111] Adicionalmente, el 3 de octubre de 2022, la Guardia Nacional presentó la convocatoria IA-036H00998-E267-2022, para la contratación del "servicio de capacitación para realizar el curso de Inteligencia en Fuentes Abiertas (Open Source Intelligence, OSINT)",[112] que atendería los temas de: i) teoría de la inteligencia y conceptos metodológicos; y ii) herramientas y bases de datos. El curso sería impartido, tentativamente, en la Ciudad de México durante el mes de noviembre y diciembre de 2022. La existencia de esta convocatoria, que fue eliminada del portal web, contradice la respuesta de la Guardia Nacional a la solicitud de acceso a la información cursada por esta investigación, en la que esa dependencia había informado que no existía información respecto de prácticas de OSINT.

IV.4.c. Entidades Federativas

Se ha conocido que los estados de Guerrero, Chihuahua y Veracruz han adquirido software relacionado con OSINT. El Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública de Guerrero registró durante los períodos de enero a junio de los años 2021 y 2022, respectivamente, gastos por el monto de $387.000 pesos mexicanos (19.903,41 dólares), correspondientes a un "software para realizar la búsqueda de información sensible e investigaciones por medio de OSINT".[113]

Por su parte, el estado de Chihuahua señaló en el documento "Evaluación del Programa para el Fortalecimiento del Estado de Fuerza y las Capacidades Institucionales",[114] publicado en octubre de 2020, la creación de una policía cibernética dotada con "tecnología que permite el ciberpatrullaje" y cuyo personal cuenta con un perfil especializado en conocimientos técnicos de OSINT, dedicado a

[111] Instituto Nacional de Estadística y Geografía (INEGI), "Censo Nacional de Seguridad Pública Federal. Presentación de resultados generales", 2021, actualizado el 11 de abril de 2022, disponible en: https://www.inegi.org.mx/contenidos/programas/cnspf/2021/doc/cnspf_2021_resultados.pdf, último acceso: 14 de agosto de 2023.

[112] La convocatoria fue eliminada del portal, aunque el documento (pdf) sigue disponible en Secretaría de la Defensa Nacional (SEDENA) y Guardia Nacional (GN), "Convocatoria para la invitación nacional a cuando menos tres personas, electrónica", 2022, disponible en: https://www.gob.mx/cms/uploads/attachment/file/765949/Convocatoria_IA-E267-2022_Curso_de_Inteligencia_en_Fuentes_Abiertas.pdf, último acceso: 14 de agosto de 2023.

[113] La información referente al software se encuentra disponible en los datos abiertos de la Plataforma Nacional de Transparencia, bajo el término "OSINT", disponible en: https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=OSINT&coleccion=5, último acceso: 14 de agosto de 2023.

[114] Gobierno del Estado de Chihuahua, "Evaluación del Programa para el Fortalecimiento del Estado de Fuerza y las Capacidades Institucionales", 2020, disponible en: https://www.gob.mx/cms/uploads/attachment/file/604448/DIAGNO_STICO_CHIHUAHUA_2020.pdf, último acceso: 14 de agosto de 2023.

"recabar información de distintos sitios, páginas, blogs, redes sociales y cualquier otro medio virtual".[115] Los datos obtenidos durante el ciberpatrullaje son procesados y analizados para generar "productos de inteligencia para la identificación de perfiles simulados con *modus operandi* o situaciones inusuales que vulneren la seguridad y/o situaciones inusuales que vulneren la seguridad de los cibernautas".[116] Al respecto, se envió una solicitud de acceso a la información a la Secretaría de Seguridad Pública del estado de Chihuahua, que no fue contestada.

A su turno, en el Informe Estatal de Evaluación 2021 del estado de Veracruz, surge que este adquirió y renovó licencias de software especializado para tareas de la Policía Científica Preventiva –entre ellas OSINT–,[117] con el objetivo de "fortalecer y mejorar el desempeño de la Policía Científica, y combatir la ciberdelincuencia". Como respuesta a un pedido de acceso a la información de esta investigación, la Secretaría de Seguridad Pública de ese estado informó que "se entiende por inteligencia de fuentes abiertas a la búsqueda de información pública en internet, según lo dispuesto en el artículo 143,[118] de la Ley Nº 875 de Transparencia y Acceso a la Información Pública para el estado de Veracruz". Vale decir que esa norma define a la información pública como aquella "en posesión de los sujetos obligados, con excepción de la que tenga el carácter de confidencial o reservada",[119] es decir, en el sentido que usualmente recibe el término en las leyes de transparencia, y no en referencia a su nivel de acceso.

IV.5. Uruguay

IV.5.a. Centro Nacional de Respuesta a Incidentes de Seguridad Informática

De las respuestas a los pedidos de acceso a la información enviados por esta investigación surge que el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTUY) contrató, en 2020, una licencia de Threat Intelligence de

[115] *Ibíd*.

[116] *Ibíd*., p. 11.

[117] Gobierno del Estado de Veracruz, Secretaría de Seguridad Pública (SSP) y Secretaría Ejecutiva del Sistema y del Consejo Estatal de Seguridad Pública (SESCESP), "Evaluación integral del fondo de aportaciones para la Seguridad Pública (FASP) del estado de Veracruz, ejercicio fiscal 2021", informe estatal de evaluación, 2021, disponible en: http://ftp2.fiscaliaveracruz.gob.mx/WEB%20FGE/FASP/2021/Evaluacion-Integral-FASP-Veracruz-2021.pdf, último acceso: 14 de agosto de 2023.

[118] Congreso del Estado de Veracruz, Secretaría General, Dirección de Registro Legislativo y Publicaciones Oficiales, "Ley de Transparencia y Acceso a la Información pública para el estado de Veracruz de Ignacio de la Llave", 2022, disponible en: https://www.legisver.gob.mx/leyes/LeyesPDF/LTRANSPARENCIA20122022.pdf, último acceso: 15 de agosto de 2023.

[119] *Ibíd*.

la empresa ITSEC S.A. por un monto de $170.800 dólares. La contratación se dio a través de un llamado a licitación[120] y tuvo lugar en el marco del Programa de Fortalecimiento de la Ciberseguridad en Uruguay, suscrito en 2019 con el Banco Interamericano de Desarrollo (BID), cuyo objetivo era mejorar la prevención, la detección y la respuesta a los ataques informáticos.

Del propio llamado a licitación pueden inferirse las características del sistema. Allí se establecía, entre otras cosas, la obligatoriedad de que el sistema adquirido contara "con acceso a múltiples fuentes de información de amenazas, como mínimo las siguientes: redes sociales, *hacker message boards* y foros, IRC, *paste sites*, blogs, y dark webs". Debía contar, además, con "acceso a publicaciones en redes sociales, incluyendo como mínimo: Twitter, Facebook y Reddit". También debía "proporcionar acceso a los foros de acceso especial (páginas Onion) de la dark web", entre otras cosas.[121]

IV.5.b. Ministerio Público Fiscal

De la entrevista a una fuente calificada en el ámbito de la Fiscalía General de la Nación surge que en el marco de las investigaciones criminales se recolecta información de personas individualizadas y que la figura del "agente encubierto" puede ser utilizada para la creación de perfiles falsos. Además, hizo saber que no existen protocolos para la recolección y el tratamiento de información recolectada en fuentes abiertas.[122]

El informante calificado de la Fiscalía resalta que hoy no existen garantías suficientes en cuanto a la aplicación de OSINT por parte de la Policía en Uruguay y que también hay otros problemas a tener en cuenta como son la corrupción policial y la falta de preparación de los funcionarios policiales (y de la misma Fiscalía) al momento de manejar información. Expresa que son de público conocimiento algunos casos de filtraciones de información o el uso de la información del sistema policial para fines privados.[123]

---

[120] Gobierno de Uruguay, Agencia Reguladora de Compras Estatales, "PFI - Licitación pública nacional 3/2020", 2020, disponible en: https://www.comprasestatales.gub.uy/consultas/detalle/id/818602/mostrar-llamado/1, último acceso: 14 de agosto de 2023.

[121] Uruguay Presidencia, Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC), "Documentos de licitación para adquisición de licencia de Threat Intelligence", 2020, disponible en: https://docs.google.com/document/d/1Ygz2fYqqqcS3QKX6i5Sh_gvwa68Yi5CuUUvWxbJXBKg/edit, último acceso: 14 de agosto de 2023.

[122] Entrevista realizada el 6 de diciembre de 2022.

[123] Ver Diario Ámbito, "Caso Astesiano: los chats del ex custodio que complican a policías y funcionarios", 2022, disponible en: https://www.ambito.com/uruguay/caso-astesiano-los-chats-del-ex-custodio-que-complican-policias-y-funcionarios-n5603158, último acceso: 14 de agosto de 2023.

IV.5.c. Ministerio del Interior

Luego de varios meses de haber vencido el plazo para contestar y luego de una denuncia ante la Unidad de Acceso a la Información Pública de Uruguay, el Ministerio del Interior declaró como reservada la información solicitada para esta investigación respecto del uso de técnicas de OSINT y la existencia de protocolos de uso, y utilizó criterios de clasificación de la información que la Unidad de Acceso a la Información Pública ya ha considerado ilegales en sus dictámenes.[124]

En la Memoria Anual del año 2020,[125] el Ministerio del Interior uruguayo declaró que el Observatorio Nacional sobre 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". UCINET es un software utilizado en apoyo a las actividades de OSINT, se usa para el análisis y la graficación de redes sociales, e incluye una gran cantidad de medidas estadísticas e indicadores a partir de matrices de relaciones entre individuos o casos. Vale la pena aclarar que la terminología "análisis de redes sociales" se utiliza de forma amplia por lo que no refiere necesariamente a su uso en redes sociales digitales (como Twitter, Facebook, Instagram), sino a la detección de patrones y relaciones entre individuos de cualquier tipo de red. Consultado sobre los fines y los protocolos del uso de este software, el Ministerio del Interior de Uruguay declaró reservada la información.

IV.5.d. Caso de pedido de acceso a la información sobre ciberpatrullaje

En junio de 2020, el periódico departamental *Salto al Día* publicó que, según una fuente del área de Delitos Informáticos de la Policía de Uruguay, alrededor de 200.000 personas habrían sido identificadas por participar en grupos en redes sociales con características políticas, fundamentalmente de orientación de

[124] Ver Uruguay Presidencia, AGESIC, Unidad de Acceso a la Información Pública (UAIP), "Dictamen Nº 17/013 sobre información reservada y matrices de criterios", 2013, disponible en: https://www.gub.uy/unidad-acceso-informacion-publica/institucional/normativa/dictamen-n-17013-sobre-informacion-reservada-matrices-criterios, último acceso: 14 de agosto de 2023. Ver Uruguay Presidencia, AGESIC, UAIP, "Consejo Ejecutivo de la Unidad de Acceso a la Información Pública", resolución Nº 13/22, 2022, disponible en: https://www.gub.uy/unidad-acceso-informacion-publica/sites/unidad-acceso-informacion-publica/files/2022-06/RESUAIP22013-%20AA%20con%20MI.pdf, último acceso: 14 de agosto de 2023.

[125] Uruguay Presidencia, "Memoria anual 2020", tomo II, disponible en: https://medios.presidencia.gub.uy/tav_portal/2021/noticias/AH_438/Tomo%20II_FINAL%20web.pdf, último acceso: 14 de agosto de 2023.

izquierda.[126] Gustavo Gómez, director de la organización de derechos humanos Observacom, presentó una solicitud de acceso a la información pública para saber si se "realiza un monitoreo sistemático de oficio en redes sociales para identificar expresiones de odio".[127] El Ministerio del Interior desestimó la solicitud "en razón de que la información solicitada por el mismo tiene la calidad de 'reservada'".[128]

V. OSINT y derechos humanos

V.1. Afectación a la privacidad

La privacidad es un derecho asegurado constitucionalmente en muchos países de la región (Argentina, Bolivia, Brasil, Chile, Colombia, México, Uruguay, Venezuela, entre otros) y cuya protección está prevista tanto en el Sistema Universal de Protección de los Derechos Humanos (SUDH) como en el Sistema Interamericano de Protección a los Derechos Humanos (SIDH). Que el "derecho a la privacidad" no aparezca mencionado explícitamente en esos instrumentos no implica que no sea un derecho humano fundamental previsto en los tratados.[129]

A nivel universal, el artículo 12 de la Declaración Universal de Derechos Humanos (DUDH) y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP) prescriben que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. En el ámbito de la protección regional, el artículo 11 de la Convención Americana sobre Derechos Humanos (CADH), sobre la protección de la honra y de la dignidad es el que resulta relevante, en igual sentido. La Corte Interamericana de Derechos Humanos (en adelante, CtIDH) ha expresado que la intimidad referida en ese artículo comprende, entre otras dimensiones, la de tomar decisiones libremente relacionadas con diversas áreas de la propia vida, tener un espacio de tranquilidad personal, mantener reservados ciertos aspectos de la vida privada y controlar la difusión de información personal hacia el

[126] Salto al Día, "Delitos Informáticos tendría identificado a más de 200 mil personas por expresiones de odio en redes sociales", 2020, disponible en: https://web.archive.org/web/20200811033653/https://saltoaldia.com.uy/delitos-informaticos-tendria-identificado-a-mas-de-200-mil-personas-por-expresiones-de-odio-en-redes-sociales, último acceso: 14 de agosto de 2023.

[127] Ver https://twitter.com/gusgomezgermano/status/1311650905134166017, último acceso: 14 de agosto de 2023.

[128] Ver https://mobile.twitter.com/gusgomezgermano/status/1311650940458536960, último acceso: 14 de agosto de 2023.

[129] Bertoni, *supra* nota 21.

público.[130] No obstante, los derechos incluidos en el artículo 11 no son derechos absolutos y se encuentran sujetos a la aplicación del test de proporcionalidad:[131]

> El derecho a la vida privada no es un derecho absoluto y, por lo tanto, puede ser restringido por los Estados siempre que las injerencias no sean abusivas o arbitrarias; por ello, las mismas deben estar previstas en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y [estricta] proporcionalidad, es decir, deben ser necesarias en una sociedad democrática.[132]

Sobre la relación entre privacidad y comunicaciones, ese tribunal tiene dicho que "aunque las conversaciones telefónicas no se encuentran expresamente previstas en el artículo 11 de la Convención, se trata de una forma de comunicación que, al igual que la correspondencia, se encuentra incluida dentro del ámbito de protección del derecho a la vida privada".[133] Es preciso resaltar que para la CtIDH las violaciones de la privacidad pueden provenir tanto del Estado como de privados.[134]

Asimismo, en el caso "Pavez Pavez vs. Chile", la CtIDH interpretó el concepto de "vida privada" de forma amplia, al establecer que su protección "no se limita al derecho a la privacidad, pues abarca una serie de factores relacionados con la dignidad de la persona, incluyendo, por ejemplo, la capacidad para desarrollar su propia personalidad, aspiraciones, determinar su identidad y definir sus relaciones personales".[135] Por su lado, el Tribunal Europeo de Derechos Humanos

---

[130] Corte Interamericana de Derechos Humanos (CtIDH), "Fontevecchia y D'amico vs. Argentina", sentencia del 29 de noviembre de 2011, Fondo, Reparaciones y Costas, Serie C, Nº 238, § 48, disponible en: https://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=191, último acceso: 14 de agosto de 2023.

[131] Bertoni, *supra* nota 21.

[132] CtIDH, "Tristán Donoso vs. Panamá", sentencia del 27 de enero de 2009, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, N° 193, § 56, disponible en: https://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=253, último acceso: 14 de agosto de 2023.

[133] *Ibíd*., § 55, citado en Bertoni, *supra* nota 21.

[134] Bertoni, *supra* nota 21.

[135] "58. Por otra parte, el Tribunal ha precisado que la protección del derecho a la vida privada no se limita al derecho a la privacidad, pues abarca una serie de factores relacionados con la dignidad de la persona, incluyendo, por ejemplo, la capacidad para desarrollar su propia personalidad, aspiraciones, determinar su identidad y definir sus relaciones personales. El concepto de vida privada engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior. La efectividad del ejercicio del derecho a la vida privada es decisiva para la posibilidad de ejercer la autonomía personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona. Asimismo, la vida privada comprende la forma en que la persona se ve a sí misma y cómo decide proyectarse hacia los demás, siendo esto una condición indispensable para el libre desarrollo de la personalidad". CtIDH, "Pavez Pavez vs. Chile", sentencia del 4 de febrero de 2022, Fondo, Reparaciones y Costas, disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_449_esp.pdf, último acceso: 14 de agosto de 2023.

(TEDH) en el caso "Peck vs. United Kingdom"[136] reconoció que hay una expectativa de privacidad incluso cuando las personas interactúan en espacios públicos.[137] Estos criterios expansivos y generosos sobre el derecho a la privacidad nos llevan a considerar como una posibilidad que el mismo se extienda, incluso, a entradas públicas en redes sociales cuyo alcance puede ser restringido por los usuarios y las usuarias, aun en los casos en los que –por cualquier razón– no lo hayan hecho.

Así, el hecho de que OSINT utilice, por definición, fuentes "abiertas" no implica que su práctica no pueda ser violatoria del derecho a la privacidad. Como se ha dicho, la definición de "fuente abierta" que se establezca por ley será fundamental para dilucidarlo.

En el caso de las fuentes abiertas online, estas suelen ser generalmente entendidas como aquellas "accesibles al público en general". Ello no está exento de problemas. El "acceso público" es un concepto brumoso. En el caso de la actividad en internet, puede referirse al hecho de que el usuario o la usuaria que sube el contenido haya decidido que su visualización no se encuentre limitada únicamente a sus contactos. En ese sentido, podría entenderse que una publicación está "abierta al público". Sin embargo, esta afirmación puede –y debe– ser matizada. Para lograr acceder a una publicación determinada, es necesario ingresar a una plataforma, sea mediante una aplicación o tipeando una URL en un navegador web, y luego, dentro de la plataforma, ubicar la página de perfil de un usuario determinado, o localizar el *thread* en el marco del cual la publicación fue realizada. La posibilidad de publicar contenido en forma reservada para algunas personas no es una función que se encuentre disponible en toda plataforma ni que todos los usuarios y usuarias conozcan o implementen regularmente.

Por lo demás, no todo material publicado es potencialmente accesible. En el caso de algunas plataformas, es necesario poseer una cuenta e ingresar las credenciales de autenticación propias para poder visualizar el contenido disponible. En esos casos, el contenido no se encuentra accesible a todo el público, sino solamente a quienes poseen una cuenta, a veces paga. Es el caso de muchas publicaciones académicas e incluso medios de comunicación o archivos periodísticos. Es decir, no todo material publicado es accesible o irrestricto.[138] Finalmente, en el

[136] Ver Corte Europea de Derechos Humanos, "Peck vs. The United Kingdom", sentencia del 28 de enero de 2003, disponible en: https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22peck%22],%22itemid%22:[%22001-60898%22]}, último acceso: 14 de agosto de 2023.

[137] Bertoni, *supra* nota 21.

[138] Medios como *Clarín* (Argentina), *Folha de S. Paulo* (Brasil), *El Mercurio* (Chile), *El Espectador* (Colombia), *Reforma* (México)

caso de las redes sociales, aunque una persona disponga que las publicaciones de su perfil se mantengan privadas, podría no tener control sobre la visibilidad de sus interacciones en publicaciones ubicadas en el perfil de terceros (por ejemplo, comentarios a fotografías de terceros), e incluso podría desconocer si el perfil con el que está interactuando es de "acceso público" o privado.[139]

Otro problema del concepto de fuente abierta es que "no depende de cuántas personas hayan realmente accedido o supieran de su existencia, sino de cuán hipotéticamente difícil sería para una persona acceder a cierta información (…). Es un ejercicio de conjetura".[140] Ese ejercicio hipotético pone en pie de igualdad a situaciones que, en los hechos, no lo están: es tan "público" un tuit de un deportista mundialmente famoso, una celebridad televisiva o un jefe de Estado como un blog de fotos familiares creado para una ocasión específica. Las diferentes legislaciones reseñadas no tienen esto en cuenta cuando definen las "fuentes abiertas".

Las normas que distinguen en forma tajante entre la información disponible en "fuentes abiertas" y el resto parten de la misma premisa: si la información es de "acceso público", su titular no tiene sobre ella ninguna expectativa de privacidad respecto del Estado. En el caso de internet, ello importa asumir que, al elegir que sus interacciones sean "públicas" en el sentido señalado anteriormente, el usuario o la usuaria ha renunciado a esa expectativa de privacidad.[141] Sin embargo, ello no debe ser necesariamente así. Al publicar en internet, las personas no están contemplando que ese contenido será objeto de escrutinio estatal. Ello es especialmente cierto cuando no existen normas que lo autoricen específicamente. A diferencia de lo que ocurre con las personas físicas, el accionar estatal se encuentra circunscrito al ámbito de su competencia, esto es, a aquellas potestades que el sistema jurídico le asigna. Por otro lado, los derechos constitucionales no pueden ser dejados de lado por los términos y las condiciones de las plataformas o por la propia arquitectura de internet.

Como se ha visto, existe una tendencia a englobar, bajo las categorías de "fuente abierta" o "acceso público", toda clase de información diferente. El único denominador común es que se trata de fuentes de relativamente "fácil" acceso. Ni

y *El País* (Uruguay) limitan el acceso a contenido de los usuarios y las usuarias que no posean una cuenta. Servicios académicos como JSTOR o HeinOnline hacen lo propio con el acceso a piezas de investigación.

[139] Es el caso, por ejemplo, de los comentarios en perfiles de terceros en Facebook e Instagram.

[140] Hartzog, Woodrow, "The Public Information Fallacy", en: *Boston University Law Review*, vol. 99, Nº 459, 2019, p. 498.

[141] Kerr, Orin S., "Applying the Fourth Amendment to the Internet: A General Approach", en: *Stanford Law Review*, vol. 62, Nº 1.005, 2009, p. 1.030-1.031.

siquiera se suele distinguir entre la información publicada libremente por una persona sobre sí misma y la información sobre ella –disponible en internet– publicada por otra, con o sin su consentimiento.

Esta concepción parece responder a una noción de "espacio público digital" bajo la cual se asimila a internet (o al menos a la parte de internet accesible por todos y todas) a un espacio público, como si se tratara de un parque o la vía pública. Si internet, o al menos su contenido "de acceso público", es asimilable a la vía pública, entonces el Gobierno puede "patrullar" en ella, preventivamente y sin autorización judicial, con el objetivo legítimo de proteger la seguridad de los ciudadanos y las ciudadanas. No obstante, la premisa es errónea. Internet no es el equivalente funcional de la vía pública. La característica de esta que hace que sea legítimo para el Estado "patrullar" con fines de seguridad ciudadana es su calidad de bien de dominio público del Estado, lo cual implica no solamente su libre acceso, sino también su titularidad estatal, de donde se desprende asimismo el deber de seguridad respecto de las personas que allí transitan. Es por eso que la policía no podría patrullar en un museo o centro comercial privado de acceso libre al público, que son de titularidad de terceros. La expectativa de privacidad del público frente al Estado dentro de estos establecimientos es mayor a aquella que tienen en la vía pública; las interacciones entre los clientes y las clientas de un centro comercial no deberían ser escuchadas por las fuerzas de seguridad fuera del marco de una investigación y sin una orden judicial. De igual modo, que sea posible acceder con "relativa facilidad" al contenido de las publicaciones en internet (siempre y cuando se cuente con una URL) no implica que vigilarlas sin una orden judicial no constituya una afectación al derecho a la privacidad.

Incluso, si se aceptara este encuadre –equívoco– del espacio público digital, el "patrullaje" en internet no reviste las mismas características que el realizado por agentes de las fuerzas de seguridad en la vía pública. En primer lugar, hoy existen herramientas de *scraping* que permiten extraer gran cantidad de información de la web a una gran velocidad y a un costo radicalmente menor al que se incurriría si se hiciera manualmente. La utilización de ese tipo de programas es mucho más invasiva que el "patrullaje" de las calles, ya que extrae mucha más información que la estrictamente necesaria para los fines estatales buscados. De esta forma, el uso de *scrapers* podría implicar un incumplimiento con los estándares de necesidad y proporcionalidad requeridos por el derecho internacional de los

derechos humanos.[142] Una concepción de internet como espacio público digital compatible con el estado de derecho debe entenderlo como un espacio cívico valioso, donde los derechos tienen plena vigencia, y que debe ser protegido de interferencias indebidas.

Por lo demás, el –mal llamado– "ciber patrullaje" se lleva adelante en forma secreta, sin que los agentes que lo realizan se identifiquen, a diferencia de la actividad de prevención policial en las calles. Prácticamente cualquier actividad en internet podría estar siendo observada por las autoridades con fines de seguridad y los sujetos vigilados nunca serían notificados, de tal modo que la actividad se asimila mucho más a la de los servicios de inteligencia que a la de las agencias de seguridad interior.

Otra potencial afectación a los derechos humanos puede ocurrir cuando, en el caso de procesos penales, se obtiene mediante OSINT más información sobre una persona que aquella que resulta relevante y estrictamente necesaria para la investigación. La información disponible online no debe utilizarse para construir un "perfil" del imputado. En caso contrario, existe la posibilidad de que, mediante la introducción de elementos extraños al hecho que se investiga, se afecte la imparcialidad del juzgador, y se vulnere así el debido proceso.

Por último, creemos que la producción de inteligencia criminal sin orden judicial ni una hipótesis delictiva concreta se asemeja menos al "patrullaje" de las calles que a una "excursión de pesca", prohibida por las constituciones y los tratados internacionales.

V.2. Afectación a la libertad de expresión

Las implicancias de la práctica de OSINT en el derecho a privacidad están intrínsecamente relacionadas con potenciales afectaciones en el ejercicio del derecho a la libertad de expresión. La Relatoría Especial de la Comisión Interamericana de Derechos Humanos para la Libertad de Expresión ha dicho que "el respeto de la libertad de expresión en línea presupone la privacidad de las comunicaciones. En efecto, sin un espacio privado, libre de injerencias arbitrarias del Estado o de particulares, el derecho a la libertad de pensamiento y expresión no puede ser ejercido plenamente".[143]

[142] Art. 17 PIDCP, observación general Nº 16 del Comité de Derechos Humanos de las Naciones Unidas.

[143] CIDH, *supra* nota 91, p. 130, y CIDH, "Estándares para una internet libre, abierta e incluyente", informe de la Relatoría Es-

El artículo 13 de la Convención Americana de Derechos Humanos y el artículo 19 del Pacto Internacional de los Derechos Civiles y Políticos establecen el derecho de toda persona a la libertad de expresión, el que comprende "la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección".[144] Sus disposiciones resultan plenamente aplicables a las comunicaciones, ideas e informaciones que se difunden y acceden a través de internet.[145]

Internet, en general, y las redes sociales, en particular, no pueden ser vistos como meras "fuentes de información" (como es el caso de otras fuentes abiertas como libros, publicaciones académicas, revistas, etc., concebidas con esa finalidad). Por el contrario, se trata de espacios cívicos valiosos de deliberación democrática y de ejercicio de otros derechos, como la libertad de educación y de asociación,[146] que es necesario proteger y no reprimir.

Existen estudios que demuestran el efecto disuasorio que las prácticas de OSINT tienen sobre el discurso. Las personas tienden a callar si saben que están siendo vigiladas, especialmente al publicar contenido en redes sociales,[147] sobre todo si creen que su discurso podría ser objeto de persecución penal.

En el caso específico de las interacciones en internet, podemos imaginar algunas formas en las que la autocensura podría funcionar: i) dejar de participar en las discusiones o de expresar sus ideas; ii) participar en las discusiones y expresar sus ideas, aunque con el cuidado de no exponer sus pensamientos en forma cándida por temor a represalias ante expresiones impopulares; iii) dejar de participar en las discusiones "públicas" y pasar a tenerlas en el ámbito privado, por ejemplo, mediante intercambios privados en lugar de en foros de discusión de acceso abierto o comentarios a publicaciones; y iv) participar de las discusiones con acceso

pecial para la Libertad de Expresión, OEA/Ser.L/V/II, CIDH/RELE/INF.17/17, 15 de marzo 2017, p. 183, disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf, último acceso: 14 de agosto de 2023.

[144] Art. 13.1 CADH, art. 19 PICP.

[145] CIDH, *supra* nota 91, § 2. ONU, Consejo de Derechos Humanos, "Promoción, protección y disfrute de los derechos humanos en internet", A/HRC/20/L.13, 29 de junio de 2012, § 1, disponible en: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf, último acceso: 14 de agosto de 2023.

[146] ONU, Asamblea General, "Promoción y protección del derecho a la libertad de opinión y de expresión", A/66/290, 10 de agosto de 2011, § 61, disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/449/81/PDF/N1144981.pdf, último acceso: 14 de agosto de 2023, citado en CIDH, *supra* nota 91, § 2.

[147] Ver, por ejemplo, Stoycheff, Elizabeth, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring", en: *Journalism & Mass Communication Quarterly*, vol. 93, Nº 2, 2016, pp. 296-311.

restringido, por ejemplo, modificar el acceso a su perfil en redes sociales a "privado", de forma tal que solamente ciertas personas puedan leer sus intervenciones.

Los efectos mediatos de esta situación son aún más preocupantes. Si actualmente internet es el lugar donde discurre gran parte del debate público, entonces, un efecto de autocensura de las características referidas desincentivará la deliberación y el involucramiento de los ciudadanos y las ciudadanas en los asuntos comunes. El derecho a obtener información sobre asuntos de interés público se verá conculcado, lo que afectará seriamente la amplitud y la robustez necesarias en el debate en una sociedad democrática.

En esa línea, en su declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión,[148] la Relatoría Especial de las Naciones Unidas para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos expresaron que es "preocupante que la legislación en materia de inteligencia y seguridad haya permanecido inadecuada frente a los desarrollos de las nuevas tecnologías en la era digital. Preocupan de manera especial los efectos intimidatorios que el acceso indiscriminado a datos sobre la comunicación de las personas pueda generar sobre la libre expresión del pensamiento, búsqueda y difusión de información en los países de la región". Es por eso que instaron a los Estados a "que revisen la legislación pertinente y modifiquen sus prácticas, con la finalidad de asegurar su adecuación a los principios internacionales en materia de derechos humanos". A su vez, las afectaciones de OSINT en la libertad de expresión tienen incidencia directa en el ejercicio de los derechos políticos como la libertad de asociación, de afiliación política y sindical y el derecho de protesta, y afectan particularmente la capacidad de organización y resistencia de defensores de derechos humanos, disidentes políticos, organizaciones de la sociedad civil, etc.

Lo dicho hasta aquí no debe ser interpretado de forma tal que el derecho de acceso a la información o el derecho a la libertad de expresión, en su faz colectiva, se vean afectados. En este sentido, es importante establecer un régimen diferenciado para la actividad de OSINT realizada por el Estado (o por terceros

[148] CIDH, OEA, "Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión", informe del Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y de la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, 2013, disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2, último acceso: 14 de agosto de 2023.

para aquel). Específicamente, es relevante no afectar la actividad de periodistas, investigadores e investigadoras, y centros académicos.

VI. Conclusiones

Como se ha visto, en los últimos años se ha observado en la región una tendencia de las autoridades a intentar monitorear, de diversas formas, la actividad de las personas en internet, con fines de vigilancia. Una de ellas, que cobró especial notoriedad, fue la realización de inteligencia con base en fuentes abiertas (OSINT).

A pesar de haber sido presentada bajo el nombre de "ciberpatrullaje", se trata de una actividad de inteligencia. Incluso si la finalidad de esta actividad es proveer a la seguridad ciudadana, implica la obtención, el procesamiento y el análisis de información. Además, a diferencia del patrullaje de las calles, se lleva adelante en secreto por agentes no identificados, o de incógnito. Finalmente, a diferencia del patrullaje que se lleva a cabo sobre espacios, este seguimiento digital se ha realizado sobre personas concretas, es decir, objetivos de inteligencia.

Una segunda observación sobre OSINT a nivel regional es que se está ejecutando por fuera de la ley o con sustento en normas de jerarquía infralegal. En ninguno de los Estados estudiados existe una norma que establezca límites a esta actividad, que prescriba en qué oportunidad es legítimo hacerlo, con qué alcance y con orden de quién. Donde existen normas habilitantes, estas no cumplen con los estándares de legalidad ni han sido fruto de un debate legislativo previo. Además, se han utilizado herramientas OSINT para el perfilamiento de periodistas, manifestantes, defensores de derechos humanos, activistas, políticos, líderes sociales, académicos e influenciadores de internet.

Algunos Gobiernos de la región han adquirido software de OSINT para vigilancia. Así, bajo el pretexto de "patrullar" internet, los Estados han aumentado sus capacidades tecnológicas de control y vigilancia. Lo que no ha aumentado a la par de ello son los recursos y las capacidades estatales para controlar esas actividades.

Una dificultad adicional para controlar la actividad OSINT radica en la opacidad con la que es llevada adelante por los Estados. Tal opacidad adquiere diversas formas. En primer lugar, puede ocultarse por completo la realización de la actividad, e incluso la existencia de normas habilitantes. En otros casos, los contratos de adquisición de servicios de OSINT o del software para ejecutarlo

pueden ser secretos o reservarse, generalmente por razones de seguridad nacional. Finalmente, es difícil para las personas defenderse de las instancias específicas de OSINT que se realizan sobre ellas cuando estas no son publicadas por las autoridades. De esta forma, la actividad se lleva a cabo a espaldas de la sociedad y del escrutinio público, e incluso de los propios afectados.

En algunos Estados, se ha observado que la actividad OSINT con fines de vigilancia se realiza con sistematicidad, mientras que en otros casos se ha efectuado en forma aislada. En otros, esto es difícil de afirmar con certeza debido a la falta de transparencia. En cualquiera de esos supuestos, su realización en ausencia de leyes que adecúen su práctica a estándares internacionales tiene el potencial de incidir en los derechos humanos de la población. El avance incontrolado de los Estados sobre la actividad de las personas en internet pone en jaque el rol de la red como un espacio cívico de deliberación popular y su eficacia como herramienta para grupos activistas y comunidades vulnerabilizadas. Por todo lo anterior, es importante iniciar un diálogo que permita debatir esta temática de forma abierta entre todas las partes involucradas, con miras a procesos legislativos que busquen encauzar la práctica dentro del marco del derecho constitucional y del derecho internacional de los derechos humanos.

A modo de recomendaciones específicas para evitar la vulneración de derechos a través de las prácticas OSINT, resulta imprescindible que toda acción del Estado en la materia cumpla el test tripartito desarrollado en el Sistema Internacional de Derechos Humanos para que cualquier medida de vigilancia sea legal, necesaria y proporcionada. La actividad de OSINT, incluso desde el Estado, puede tener usos legítimos, como los periodísticos o de investigación criminal. Sin embargo, la falta de claridad respecto a las funciones que se ejercen al hacer OSINT desde el Estado (investigación, vigilancia preventiva o inteligencia) hace más posibles las violaciones de derechos. En ese sentido, es necesario definir de forma clara las facultades del Estado y establecer mecanismos de control para el uso de tecnologías como el OSINT.

La regulación de la actividad debe contemplar la creación –por ley– de protocolos específicos que rijan la recolección, el procesamiento y la eliminación de información obtenida de fuentes abiertas. Dicha reglamentación deberá incluir qué tipo de datos se pueden recolectar en fuentes abiertas, y qué fines cumplirá la recolección; además, procurará proteger la privacidad de las personas usuarias y tolerar todas las expresiones permitidas por el marco jurídico local e internacional en materia de libertad de expresión.

Los protocolos deberán instaurar principios de rendición de cuentas, como la publicación de reportes periódicos que señalen las prácticas que se realizaron en fuentes abiertas digitales. De la misma forma, el protocolo debe cumplir con los principios previstos por las leyes de protección de datos personales en los casos aplicables, para que los y las titulares de los datos puedan ejercer sus derechos de acceso, rectificación, cancelación y oposición.

Para evitar las violaciones de derechos en el uso de las técnicas OSINT son necesarios mecanismos de control. Algunos de ellos deben ser la notificación posterior a los ciudadanos y las ciudadanas que fueron vigilados y vigiladas con tecnologías y el uso que se dio a esa información, el control previo de jueces, y el establecimiento de sanciones claras para quienes cometan abusos.

En forma concomitante con la reglamentación de los usos de OSINT para evitar la afectación de derechos humanos, es importante establecer obligaciones de transparencia y apertura también en la contratación de tecnología o servicios de terceros que incluyen esta práctica. En ese sentido, es necesario conocer los contratos existentes entre Estados y empresas privadas proveedoras de servicios OSINT, los cuales deberían ser ampliamente difundidos y encontrarse fácilmente disponibles, así como la información acerca de la asignación de recursos y el gasto realizado para esas tareas. Además, es exigible que se publiquen estadísticas acerca de las instancias específicas en las que se efectuó OSINT sobre particulares y, cuando ello sea posible, los motivos que las justificaron. Otro aspecto a mejorar en la transparencia de los Gobiernos es el recurrente uso de las razones de seguridad nacional como valla para el acceso a la información.

Por último, se impone requerir a aquellos Estados que contratan sistemas o servicios de OSINT que realicen estudios de impacto en materia de privacidad, y que sus resultados sean también ampliamente difundidos.