CELE

Inteligencia basada en fuentes abiertas (OSINT) en Argentina: un diagnóstico sobre su utilización por parte del Estado

Junio 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) en Argentina: un diagnóstico sobre su utilización por parte del Estado

Morena Schatzky* ***y Nicolás Zara*****
CELE

I. Introducción

La masificación de internet ha transformado drásticamente la manera en que las personas se informan, consumen e interactúan, lo que ha dado lugar a una serie de desafíos de diversa índole. Uno de los cambios más significativos que ha generado internet en las sociedades contemporáneas es el aumento de la capacidad de vigilancia que tienen los Estados sobre sus ciudadanos y ciudadanas.[1]

En la actualidad, utilizar internet implica compartir una gran cantidad de información sobre nuestros gustos, deseos y preocupaciones. En virtud del modelo de negocios de muchas plataformas, esa información es rutinariamente recogida y usada 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 OSINT (acrónimo de *open-source intelligence*) forma parte de un conjunto de términos que hacen alusión a técnicas de inteligencia, así

* Investigadora del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE-UP), 2020-2022. Abogada graduada de la Universidad de Buenos Aires con orientación en derecho público. Maestranda en Derecho Constitucional y Derechos Humanos en la Universidad de Palermo.

** Investigador del 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.

1 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.

como COMINT,[2] SIGINT,[3] HUMINT,[4] GEOINT,[5] etc. Es posible entender a OSINT como la recopilación y el análisis de datos recogidos de fuentes abiertas (y disponibles públicamente) para producir inteligencia accionable. Recién en el momento que a dicha información se le encuentra una utilidad o un propósito, y es asignada a una acción concreta, pasa entonces a convertirse en inteligencia propiamente dicha.[6]

El escenario global actual muestra un crecimiento en el desarrollo, la adquisición y el uso de tecnologías de vigilancia masiva por parte de los Estados.[7] El contexto regional no es diferente.[8] El cuadro se agudizó a partir de la intensificación de su uso a raíz del advenimiento de la pandemia de covid-19.[9]

A más de ello, los Estados se muestran reacios a brindar información acerca del uso de tecnologías de vigilancia. Los casos de espionaje estatal ilegal se han multiplicado en la región, e involucran generalmente a disidentes políticos, defensores de derechos humanos, manifestantes, así como miembros de organizaciones sindicales y periodistas.[10]

---

[2] 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 "COMINT (Communications Intelligence)", Tech Target, disponible en: https://www.techtarget.com/whatis/definition/COMINT-communications-intelligence, último acceso: 19 de mayo de 2023.

[3] 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 "What is SIGINT?", Everything RF, 2022, disponible en: https://www.everythingrf.com/community/what-is-sigint, último acceso: 19 de mayo de 2023.

[4] Human Intelligence (HUMINT) es el término utilizado para la recolección de información por fuentes humanas. Ver más en "Qué es la HUMINT, ejemplos, técnicas y su relación con OSINT", Odin - OSINT y Ciberinteligencia, 2022, disponible en: https://odint.net/humint-osint, último acceso: 19 de mayo de 2023.

[5] 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 "Qué es la GEOINT y para qué se usa la inteligencia geoespacial", Odin - OSINT y Ciberinteligencia, 2022, disponible en: https://odint.net/geoint, último acceso: 19 de mayo de 2023.

[6] Asociación por los Derechos Civiles (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: 19 de mayo de 2023.

[7] ONU, Consejo de Derechos Humanos, *supra* nota 3, § 2.

[8] 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: 19 de mayo de 2023.

[9] En Colombia, las Fuerzas de Seguridad realizarían "ciberpatrullaje", al menos, desde el año 2015, de acuerdo con el art. 15 de la resolución 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_LY5Jde8tH2mQnDbyNZCc2a-/view, último acceso: 19 de mayo de 2023). En Argentina, las resoluciones Nº 31/2018 y Nº 144/2020, hoy derogadas, autorizaban el "ciberpatrullaje".

[10] 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

En este marco se inserta la creciente utilización de OSINT por parte de los Estados con fines de vigilancia. Creemos que esta práctica presenta desafíos específicos en materia de derechos humanos. Se trata de herramientas cuyo empleo puede implicar una vulneración de derechos básicos y que se utilizan, en general, al margen de la legalidad. Su práctica generalmente no se encuentra reglamentada y, allí donde existe regulación, ésta es deficiente.[11] 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.

El presente informe pretende ser una primera aproximación empírica a la utilización de OSINT por parte del Estado en Argentina. Forma parte de una investigación más amplia, de alcance regional, la cual parte de la premisa de que resulta necesario contar con información sobre el uso de las prácticas y las técnicas OSINT, en distintos espacios y por distintos actores. Frente a ello, es necesario realizar un estudio de campo que permita conocer la magnitud del uso de estas técnicas, quiénes son los actores que las utilizan y cuáles han sido, si es posible medirlos, su impacto y su utilidad.

En consecuencia, se propuso un método de entorno analítico-cualitativo para realizar un estudio como el indicado. Es importante resaltar que el método de investigación que se propone no es un análisis cuantitativo, en tanto se trata de un primer estudio que permitirá acercarse al fenómeno OSINT, sin pretensión de abarcarlo en su totalidad. En la preparación de este estudio, se han cursado pedidos formales de acceso a la información pública a diversas reparticiones estatales y se ha entrevistado a diversos actores del sector público y del sector privado.

---

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 y The Citizen Lab, 2022, disponible en: https://tspace.library.utoronto.ca/bitstream/1807/123609/1/Report%23148--project-torogoz.pdf, último acceso: 19 de mayo 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: 19 de mayo de 2023. Ver también el caso de Colombia, que 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: 19 de mayo de 2023.

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

En el apartado II, se analizará el marco legal aplicable a la práctica de OSINT en Argentina, 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 la Ley de Acceso a la Información Pública y la Ley de Protección de Datos Personales. En apartado III se estudiará la compatibilidad de ese marco normativo con los derechos a la privacidad y la libertad de expresión. El apartado IV detallará las prácticas OSINT constatadas en esta investigación. El apartado V versará sobre OSINT en el sector privado. En apartado VI se referirá a casos judiciales recientes relacionados con OSINT. Finalmente, el apartado VII ensayará algunas reflexiones, a modo de conclusión.

II. Marco legal

a. Normativa nacional

i. Leyes nacionales

La actividad de los organismos de inteligencia en Argentina se encuentra regulada por la Ley de Inteligencia Nacional (Nº 25.520).[12] Esta norma dispone en su artículo 5º, que:

> 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.[13]

El artículo 9º de esta norma crea la Dirección Nacional de Inteligencia Criminal, dependiente de la Secretaría de Seguridad Interior, la cual integra el Sistema de Inteligencia Nacional, y a la que asigna la función de producir "inteligencia criminal", entendida como:

> la parte de la Inteligencia referida a las actividades criminales específi-

[12] Información Legislativa (Infoleg), Ministerio de Justicia y Derechos Humanos, Presidencia de la Nación, Ley de Inteligencia Nacional, ley Nº 25.520, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm, último acceso: 22 de mayo de 2023.

[13] El destacado no pertenece al original.

cas que, por su naturaleza, magnitud, consecuencias previsibles, peligrosidad o modalidades, afecten la libertad, la vida, el patrimonio de los habitantes, sus derechos y garantías y las instituciones del sistema representativo, republicano y federal que establece la Constitución nacional.[14]

Por su parte, la Ley de Seguridad Interior (Nº 24.059)[15] pone en cabeza de la Dirección Nacional de Inteligencia Criminal la dirección funcional y la coordinación de la actividad de los órganos de información e inteligencia de la Policía Federal Argentina, la Policía de Seguridad Aeroportuaria, la Gendarmería nacional y la Prefectura Naval Argentina. La Seguridad interior es definida como "la situación de hecho basada en el derecho en la cual se encuentran resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establece la Constitución nacional".

En tanto, la Ley de Defensa Nacional (Nº 23.554)[16] impone como limitación a las actividades de inteligencia de las Fuerzas Armadas que "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). El artículo 2º de la mencionada ley define a la Defensa Nacional como "la integración y la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieran el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva, para enfrentar las agresiones de origen externo". La actividad del Sistema de Defensa Nacional es confinada por el artículo 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". Finalmente, de acuerdo con el artículo 4º, "se deberá tener permanentemente en cuenta la diferencia fundamental que separa

[14] Cfme. art. 2º.

[15] Infoleg, Ministerio de Justicia y Derechos Humanos, Presidencia de la Nación, Seguridad Interior, ley Nº 24.059, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/458/texact.htm, último acceso: 19 de mayo de 2023.

[16] Infoleg, Ministerio de Justicia y Derechos Humanos, Presidencia de la Nación, Defensa Nacional, ley Nº 23.554, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm último acceso: 22 de mayo de 2023.

a la Defensa Nacional de la Seguridad Interior". La ley no establece distinciones relativas a la naturaleza de las tareas de inteligencia que puede llevar adelante, aunque la actuación del Sistema de Defensa se encuentra acotada a la prevención y al manejo de hipótesis de conflicto.

ii. El "protocolo de ciberpatrullaje" del Ministerio de Seguridad

En la actualidad, no existe un protocolo específico seguido por las Fuerzas de Seguridad ni los organismos de inteligencia para la práctica de OSINT. El 26 de julio de 2018, la Secretaría de Seguridad del Ministerio de Seguridad de la Nación emitió la resolución Nº 31/2018,[17] que facultó a las Fuerzas Nacionales de Seguridad Interna a realizar OSINT. Dicha norma dispuso en su artículo 1º:

> Instrúyase a las áreas de investigación de Ciberdelitos de las Fuerzas de Seguridad que se encuentran bajo la órbita de este Ministerio, a tomar intervención, específicamente, en todo lo inherente a los siguientes tópicos: Venta o permuta ilegal de armas por internet.- Venta o permuta de artículos cuyo origen, presumiblemente, provenga de la comisión de un acto o de un hecho ilícito.- Hechos que presuntamente, se encuentren vinculados a la aplicación de la ley Nº 23.737.- Difusión de mensajes e imágenes que estimulen o fomenten la explotación sexual o laboral, tanto de mayores como de menores de edad, y que *prima facie* parecieran estar vinculados a la trata y tráfico de personas.- Hostigamiento sexual a menores de edad a través de aplicaciones o servicios de la web.- Venta o permuta de objetos que, presumiblemente, hayan sido obtenidos en infracción a las disposiciones aduaneras.- Hechos que, presuntamente, transgredan lo normado en los artículos 4º, 5º, 6º, 7º, 8º y 9º de la ley Nº 26.388.

La resolución estableció dos limitaciones a esta práctica. Por un lado, dispuso 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".[18] Por otro lado, estableció que "en ningún momento se permitirán acciones que vulneren o

[17] La investigación tuvo acceso a esta norma, que no se encuentra publicada en el Boletín Oficial.

[18] El resaltado no pertenece al original.

entorpezcan el derecho a la intimidad, ley Nº 25.326 y normativa reglamentaria".

Las tareas de OSINT realizadas al amparo de esta norma debían tener por objetivo reunir los medios probatorios necesarios a fin de realizar una denuncia ante las autoridades judiciales correspondientes.

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 del Ministerio de Seguridad de la Nación,[19] que derogó a 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".[20] Su alcance recaía sobre delitos específicos enumerados en su artículo 3º:

> ARTÍCULO 3º.- DELITOS CONCRETOS OBJETO DE LA PREVENCIÓN. La prevención policial del delito en el espacio cibernético procurará el conocimiento de posibles conductas delictivas cuyo acaecimiento sea previsible en función de la emergencia pública en materia sanitaria establecida por ley Nº 27.541, ampliada por el decreto Nº DECNU-2020-260-APN-PTE del 12 de marzo de 2020 y su modificatorio, en virtud de la Pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con el coronavirus covid-19; atendiendo al desarrollo de la criminalidad vinculada a la comercialización, distribución y transporte de medicamentos apócrifos y de insumos sanitarios críticos; a la venta de presuntos medicamentos comercializados bajo nomenclaturas y referencias al covid-19 o sus derivaciones nominales, sin aprobación ni certificación de la autoridad competente; y a los ataques informáticos a infraestructura crítica –especialmente a hospitales y a centros de salud–; y, también, al desarrollo de indicios relativos a los delitos a los que hace referencia el decreto Nº DECNU-2020-260-APN-PTE del 12 de marzo de 2020 y su modificatorio, previstos en los artículos 205, 239 y concordantes del Código Penal.

[19] 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/anexos/335000-339999/338229/norma.htm, último acceso: 22 de mayo de 2023.

[20] *Ibíd*., art. 1º.

> Asimismo, en tanto se advierta que resulten sensibles al desarrollo de la emergencia pública en materia sanitaria establecida por ley Nº 27.541, ampliada por el decreto Nº DECNU-2020-260-APN-PTE del 12 de marzo de 2020 y su modificatorio, en virtud de la Pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con el coronavirus covid-19, *podrán definirse como objeto de las tareas de prevención policial con uso de fuentes digitales abiertas, posibles conductas delictivas cuyo medio comisivo principal o accesorio incluya la utilización de sistemas informáticos con el fin de realizar acciones tipificadas penalmente como la trata de personas; el tráfico de estupefacientes; el lavado de dinero y terrorismo; conductas que puedan comportar situaciones de acoso y/o violencia por motivos de género, amenaza y/o extorsión de dar publicidad a imágenes no destinadas a la publicación; y delitos relacionados con el grooming y la producción, financiación, ofrecimiento, comercio, publicación, facilitación, divulgación o distribución de imágenes de abuso sexual de niñas, niños y adolescentes.*[21]

En el marco de esta investigación, se efectuó una solicitud de acceso a la información pública al Ministerio de Seguridad de la Nación, cuya respuesta ha indicado que "se dio inicio al procedimiento correspondiente a efectos de la derogación de la resolución Nº 144/2020". En forma concordante con lo informado, en fecha 27 de octubre de 2022, el Ministerio de Seguridad de la Nación dictó la resolución Nº 720/2022,[22] que dispuso en su artículo 1º: "Deróguese la resolución ministerial Nº 144 del 31 de mayo de 2020 y sus complementarias".

La derogación de la resolución Nº 144/2020, que a su vez derogaba la resolución Nº 31/2018, podría generar dudas en torno a la restauración de esta última. No obstante, en respuesta a un nuevo pedido de información pública de esta investigación, el Ministerio de Seguridad de la Nación informó que "si bien es cierto que la resolución Nº 144/2020 –que resuelve derogar la Nº 31/2018– fue posteriormente derogada por la resolución Nº 720/2022 de esta cartera, esta última no resuelve ratificar la vigencia de la previamente derogada, por lo cual la norma continúa extinta".

---

[21] El destacado no pertenece al original.

[22] 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: 22 de mayo de 2023.

De la lectura de los fundamentos de la resolución Nº 720/2022 surge que "sin perjuicio que la criminalidad en el ámbito digital continúa siendo un flagelo para la sociedad, por sus especiales características, requiere que las medidas de investigación sean ejecutadas a petición de las autoridades jurisdiccionales y ya no por tareas preventivas por parte de las Fuerzas de Seguridad", ello porque "la excepcionalidad presente al momento del dictado del decreto Nº 260/2020, en la actualidad se ha visto considerablemente disminuida", que "esta necesidad de realizar tareas investigativas en medios digitales únicamente a requerimiento de la autoridad judicial competente, radica en la tensión existente entre las tareas de prevención en el medio descrito y la protección de los datos personales regulada por la ley Nº 25.326", y que "el hecho de que los datos personales objeto del protocolo en análisis se encuentren en una fuente digital abierta, no implica que quien trate esos datos no deba cumplir con los principios de calidad del dato, de información, de seguridad y de confidencialidad establecidos en la ley Nº 25.326". Por otra parte, los fundamentos también afirman que:

> el artículo 3º del Protocolo establece como parte de objeto la prevención de posibles conductas delictivas (p. ej. trata de personas, lavado de dinero y terrorismo) que tengan como medio comisivo principal o accesorio la utilización de sistemas informáticos para cometer el delito, sin justificar adecuadamente cuál es la vinculación de los mismos con la situación sanitaria atravesada en ese momento. En este orden, se advierte que la finalidad del Protocolo resulta excesivamente amplia.

De los fundamentos surgen cuatro motivos diferentes para la derogación del Protocolo. En primer término, el artículo 1º de la resolución Nº 144/2020 establecía que éste tendría vigencia "durante el plazo de la emergencia pública en materia sanitaria establecida por la ley Nº 27.541". Por ese motivo, concluida dicha emergencia, correspondía su derogación. En segundo lugar, y en estrecha relación con el punto anterior, se plantea que las medidas deben ser ordenadas por la autoridad judicial y no en forma preventiva por las Fuerzas de Seguridad, en razón de que la situación de excepcionalidad que imperaba en marzo de 2020 ya ha cesado. En tercer término, se establece la posibilidad de una tensión entre el Protocolo y la Ley de Protección de Datos Personales. Finalmente, se entendió que el alcance del Protocolo resultaba excesivo, puesto que no se encontraba debidamente justificada la relación entre los delitos nombrados en el párrafo

segundo del artículo 3º del Protocolo (transcrito *supra*) y la situación sanitaria bajo la cual se dictó la normativa de emergencia.

En relación con la Ley de Protección de Datos Personales, es importante destacar que, en julio de 2020, la Agencia de Acceso a la Información Pública (AAIP), autoridad de control de la Ley Nº 25.326 de Protección de los Datos Personales, ya había sugerido al Ministerio de Seguridad de la Nación la suspensión de la aplicación del Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas hasta tanto se revisara su adecuación a la normativa vigente en materia de protección de datos personales.[23] La AAIP efectuó esta sugerencia con base en una serie de defectos que, según entendía, comprometían el derecho a la privacidad. Entre ellos se encontraba el hecho de que la finalidad del Protocolo resultaba demasiado amplia y que la falta de precisiones en su redacción era tal que dificultaba el control por parte de la AAIP de las tareas realizadas; no especificaba si se utilizarían herramientas automatizadas para la recolección de datos, ni los plazos para la revisión y la eliminación del "material prevenido no judicializado"; ni preveía salvaguardas especiales para el caso de transferencia internacional de los datos ni para el tratamiento de datos correspondientes a niñas, niños y adolescentes. Además, dada la gran magnitud de datos que podrían verse involucrados, se sugirió la realización de una evaluación de impacto en materia de datos personales y la adopción de medidas de seguridad para la protección de la confidencialidad y de la integridad de la información que contiene datos de carácter personal en todo el proceso de tratamiento, desde su recolección hasta su destrucción.[24]

iii. Resolución Nº 7/2022 de la Oficina Anticorrupción

El segundo párrafo del artículo 7º del Anexo I de la resolución Nº 7/2022 de la Oficina Anticorrupción manda "monitorear el cumplimiento de la presentación de las Declaraciones Juradas del SISTEMA DE MONITOREO DE ACTIVIDADES PRIVADAS Y PÚBLICAS ANTERIORES Y POSTERIORES AL EJERCICIO DE LA FUNCIÓN PÚBLICA ' MAPPAP' en tiempo y forma por parte de las personas alcanzadas" y:

[23] Del Campo, Agustina y Schatzky, Morena, "¿Ciberpatrullaje o inteligencia?", Blog del Observatorio Legislativo, 2022, disponible en: https://observatoriolegislativocele.com/ciberpatrullaje-o-inteligencia, último acceso: 23 de mayo de 2023.

[24] Agencia de Acceso a la Información Pública (AAIP), nota Nº NO-2020-47326285-APN-AAIP, dirigida al Ministerio de Seguridad de la Nación, firmada el jueves 23 de julio de 2020, disponible en: https://www.argentina.gob.ar/sites/default/files/no-2020-47326285-apn-aaip.pdf, último acceso: 23 de mayo de 2023.

> controlar si se presentan situaciones de incompatibilidad o conflicto de intereses y efectuar las instrucciones y recomendaciones que resulten necesarias para hacer cesar y/o prevenir cualquier situación de incumplimiento. *A tales efectos, podrá cruzar los datos de las declaraciones juradas con información publicada en fuentes abiertas*, así como también dar curso a actuaciones administrativas de oficio o por derivación de la COORDINACIÓN DE ADMISIÓN Y DERIVACIÓN DE DENUNCIAS de esta Oficina.[25]

Luego de ser consultada la Oficina Anticorrupción por la existencia de un protocolo que regule la utilización de técnicas OSINT en el marco de esta normativa, la dependencia contestó que:

> el Sistema MAPPAP actualmente está en una fase de implementación de recolección de datos de las DD.JJ. de las personas obligadas. Todavía no hay información consolidada al respecto, la cual será oportunamente publicada en el sitio web institucional. Por ende aún no se ha realizado ningún cruzamiento de datos.

Además, en su respuesta al pedido de acceso a la información pública de esta investigación, la Oficina Anticorrupción informó que la Coordinación de Admisión y Derivación de Denuncias no recopila información, sino que "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 1.316/2008". Se trata del Reglamento Interno de la Dirección de Investigaciones de la Oficina Anticorrupción. El artículo referido reza:

> ARTICULO 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

[25] El destacado no pertenece al original.

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.

b. Normativa de la Ciudad Autónoma de Buenos Aires

La Ley del Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires[26] (Nº 5.688) establece en su artículo 89 que la Policía de la Ciudad "conforma su organización y desarrolla sus actividades institucionales en función de la prevención, conjuración e investigación de los delitos", y entiende como investigación a "las acciones tendientes a conocer y analizar los ilícitos y hechos que vulneran la seguridad pública, sus modalidades y manifestaciones, las circunstancias estructurales y coyunturales en cuyo marco se produjeron, sus factores determinantes y condicionantes, las personas o grupos que los protagonizaron como autores, instigadores o cómplices y sus consecuencias y efectos institucionales y sociales mediatos e inmediatos". Agrega que "*cuando la investigación se desarrolla en la esfera judicial, comprende la persecución de los delitos y contravenciones consumados a través de las acciones de inteligencia criminal tendientes a constatar su comisión y sus circunstancias de tiempo, lugar y modo de ejecución, individualizar a los responsables y reunir las pruebas para acusarlos*".[27] De allí surge que la atribución de la Policía de la Ciudad de realizar tareas de inteligencia criminal se circunscribe a tareas investigativas en el marco de procesos judiciales. La norma no establece más restricciones que la prohibición de "obtener información, producir inteligencia o almacenar datos sobre personas por el solo hecho de su raza, fe religiosa, orientación sexual o identidad de género, acciones privadas u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción".[28]

---

[26] Ley Nº 5.688 del Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires, disponible en: https://digesto.buenosaires.gob.ar/documento/download/Ley%20Ciudad-5688__68dc0cdd582d3dd01f4f976a796c5cda9d7ab7dd.pdf, último acceso: 29 de mayo de 2023.

[27] El destacado no pertenece al original.

[28] Art. 85.

III. OSINT y derechos humanos

a. Derecho a la privacidad

En Argentina, la privacidad es un derecho asegurado constitucional (arts. 18 y 19 CN) y convencionalmente (art. 11 CADH; art. 17 PIDCP). Que OSINT utilice, por definición, fuentes "abiertas", no implica que su práctica no pueda ser violatoria del derecho a la privacidad.

Para ilustrar este dilema, en primer lugar, es necesario entender qué interpretación de "fuentes abiertas" hacen las normas. Las menciones a fuentes abiertas son escasas en nuestro ordenamiento jurídico. De hecho, del régimen descrito en el apartado II, surge que únicamente el artículo 7º del Anexo I de la resolución Nº 7/2022 de la Oficina Anticorrupción (OA) y la –ya derogada– resolución Nº 144/2020 del Ministerio de Seguridad refieren explícitamente a fuentes abiertas.

En cuanto a la resolución de la OA, el organismo informó que, si bien no existe un protocolo, el sistema MAPPAP actualmente está en una fase de implementación de recolección de datos de las declaraciones juradas de las personas obligadas, por lo que todavía no hay información consolidada al respecto. Por ese motivo, aún no se ha realizado ningún cruzamiento de datos.

La resolución Nº 144/2020 del Ministerio de Seguridad definía el concepto de "fuentes digitales abiertas" como "los medios y plataformas de información y comunicación digital de carácter público, no sensible y sin clasificación de seguridad, cuyo acceso no implique una vulneración al derecho a la intimidad de las personas, conforme lo normado en la Ley de Protección de Datos Personales Nº 25.326 y sus normas reglamentarias". Además, contenía como anexo un protocolo de actuación que sujetaba la actuación de las Fuerzas de Seguridad a una serie de principios: a) legalidad; b) necesidad; c) proporcionalidad; d) razonabilidad; e) protección de la razonable expectativa de privacidad; f) protección de los datos personales; g) protección de la libertad de expresión; h) no criminalización de las protestas en línea; i) restricción de la discrecionalidad en el cumplimiento de las tareas preventoras; j) profesionalización del personal afectado a las tareas de prevención del delito con uso de fuentes digitales abiertas; k) destrucción del material prevenido no judicializado; l) publicidad; m) transparencia y rendición de cuentas; y n) control y responsabilidad por el uso abusivo y violatorio.

Por su parte, el artículo 5º de la Ley de Inteligencia Nacional[29] efectúa distinciones respecto del nivel de acceso de las fuentes. De su redacción surgiría que las comunicaciones, la información, los archivos, los registros y los documentos públicos o "de acceso abierto al público" no son considerados inviolables por esa norma, motivo por el cual no sería necesaria una autorización judicial para acceder a ellos.

La redacción de estas dos últimas normas presenta algunos aspectos problemáticos. La resolución Nº 144/2020 habla de "medios y plataformas de información y comunicación digital *de carácter público*".[30] Para empezar, el "carácter público" no se encuentra claramente definido. A primera vista, difícilmente podría predicarse de entidades multinacionales privadas, tales como las grandes plataformas digitales, que tienen "carácter público".

Haciendo un mayor esfuerzo interpretativo, "carácter público" podría entenderse como asimilable a "accesible al público", en los términos de la Ley de Inteligencia. Incluso de ser así, las dificultades subsisten y son comunes a ambas normas. En primer lugar, el "acceso público" tampoco se encuentra definido en ninguna norma legal. En el caso de la actividad de las personas en internet, puede referirse al hecho de que la persona que sube el contenido no haya limitado su visualización a un conjunto de personas específicas. 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 a través de una URL en un navegador web, y luego a la página de perfil de un usuario o de una usuaria en particular, o localizar el *thread* en el marco del cual la publicación fue realizada. Además, en el caso de algunas plataformas, es necesario tener una cuenta e ingresar las credenciales de autenticación propias para poder visualizar los perfiles de otros usuarios y usuarias.

Finalmente, en algunas plataformas una persona puede elegir que su perfil se mantenga privado, pero no tiene control sobre la visibilidad de sus publicaciones en el perfil de terceros, e incluso podría desconocer si el perfil con el que está interactuando es de "acceso público" o privado. Otro problema del concepto de fuente abierta es que "no depende de cuántas personas hayan realmente accedido

[29] 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 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.

[30] El destacado no pertenece al original.

o supieran de su existencia, sino de cuán hipotéticamente difícil sería para una persona acceder a cierta información (…). Es un ejercicio de conjetura".[31] 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 o un jefe de Estado como un blog de fotos familiares creado para una ocasión específica. Estas cuestiones no parecen ser tenidas en cuenta, en general, cuando se habla de "fuentes abiertas".

Cuando establecen diferenciaciones entre la información disponible en "fuentes abiertas" y el resto, las normas bajo análisis 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 en el párrafo anterior, el usuario o la usuaria ha renunciado a esa expectativa de privacidad.[32]

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 de un centro comercial no deberían ser escuchadas por las Fuerzas de Seguridad fuera del marco de una investigación y sin orden judicial. De igual modo, que sea posible acceder con "relativa

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

[32] 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.

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, la utilización de *scrapers* podría implicar un incumplimiento de los estándares de necesidad y proporcionalidad requeridos por el Derecho Internacional de los Derechos Humanos.[33] Una concepción de internet como espacio público digital compatible con el estado de derecho debe entender que se trata de 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 la 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, por lo que deberían cumplirse las disposiciones de la Ley de Inteligencia Nacional. Al respecto, el artículo 4º de dicha norma prohíbe expresamente a los organismos de inteligencia "realizar tareas represivas, poseer facultades compulsivas, ni cumplir funciones policiales o de investigación criminal".

Por último, la inteligencia criminal sin orden judicial ni una hipótesis delictiva concreta se asemeja menos al "patrullaje" de las calles que a una "excursión de pesca", inadmisible bajo la Constitución nacional y los tratados internacionales de derechos humanos.

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

b. Derecho a la libertad de expresión

Las implicancias de la práctica de OSINT en el derecho a privacidad están intrínsecamente relacionadas con las potenciales afectaciones que podría tener en la libertad de expresión. 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,[34] sobre todo si creen que su discurso podría ser objeto de persecución penal.

En el caso específico de las interacciones en internet, creemos que la autocensura podría ocurrir de alguna de estas formas: 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; o iv) participar de las discusiones con acceso restringido –por ejemplo, al 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 ciudadanas en los asuntos comunes. El derecho a obtener información sobre asuntos de interés público se verá conculcado, lo que afectaría 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",[35] 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

[34] 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.

[35] Organización de los Estados Americanos (OEA), Comisión Interamericana de Derechos Humanos (CIDH), "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: 23 de mayo de 2023.

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".

IV. Pedidos de acceso a la información y prácticas constatadas

En el marco de la presente investigación, se cursaron pedidos formales de información pública a diversas dependencias del Gobierno nacional en el ámbito de los procedimientos normados por la ley nacional Nº 27.275, y a los organismos de seguridad de la Ciudad Autónoma de Buenos Aires en los términos de la ley Nº 104 de esa ciudad. En el contexto de las respuestas recibidas a esos pedidos, de entrevistas que fueron llevadas adelante a especialistas en la materia y a personas que practican o han practicado OSINT, y publicaciones en los medios de prensa, se han podido constatar diversas instancias en las que el Estado ha practicado OSINT.

a. Ministerio de Seguridad de la Nación

En su respuesta al pedido de acceso a la información pública, el Ministerio de Seguridad afirmó que no realiza recolección de datos personales en fuentes abiertas. Ante la consulta en torno a si han surgido casos a raíz de las tareas de prevención policial del delito en internet, cuántos de ellos fueron judicializados y bajo qué tipos penales, desde la entrada en vigencia del Protocolo aprobado por la resolución Nº 144/2020, el Ministerio de Seguridad se negó a informar, al aducir que "las Fuerzas Federales de Seguridad se ciñen estrictamente a los términos de la ley Nº 25.520, por tanto no existen casos para reportar públicamente".

No obstante, se ha constatado el uso de técnicas OSINT por parte del Ministerio de Seguridad en varias oportunidades. De hecho, en abril de 2020, la entonces ministra de seguridad, Sabina Frederic, se refirió públicamente durante la pandemia de covid-19 a la existencia de un plan de "ciberpatrullaje" destinado a "medir el humor social", basado fundamentalmente en el monitoreo de fuentes

abiertas, particularmente de redes sociales.[36] Sin embargo, los ejemplos abundan y se remontan incluso más atrás en el tiempo.

En 2016, Nicolás Lucero, de 19 años, llegó a su casa en la localidad de José León Suárez, en la provincia de Buenos Aires, y advirtió la presencia de efectivos policiales que lo aguardaban. Luego de allanar su domicilio, los agentes lo condujeron a la comisaría, requisaron su celular y los de su familia y la netbook de su hermana.[37] Había sido acusado por el delito de intimidación pública a raíz de un tuit en el que se refería al entonces presidente de la Nación:[38]

Nicolás fue sobreseído en sede judicial en el año 2018, tras transitar una causa judicial en su contra.[39]

En una situación similar, en abril de 2020, Kevin Guerra, un joven de 20 años oriundo de la localidad de Junín, en la provincia de Buenos Aires, escribió un tuit en el que ironizaba 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:[40]

---

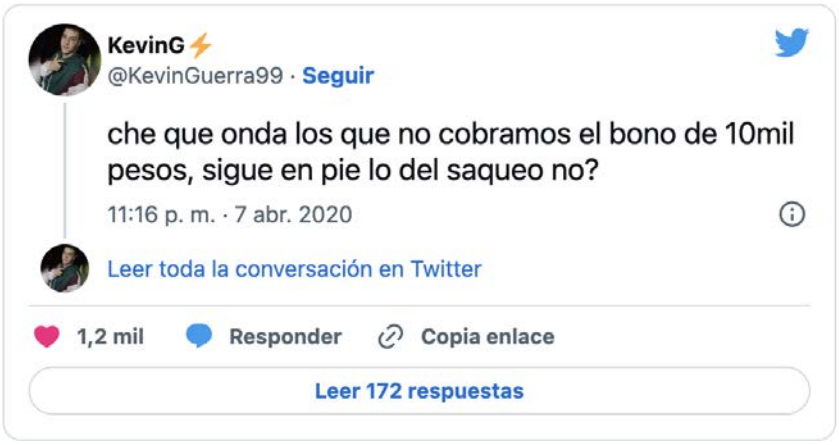
[36] Ver, "Polémica revelación: la ministra de Seguridad admitió que las fuerzas a su cargo realizan ciberpatrullaje en redes sociales para 'detectar el humor social'", Diario Infobae, 2020, disponible en: https://www.infobae.com/politica/2020/04/09/polemica-revelacion-la-ministra-de-seguridad-admitio-que-las-fuerzas-a-su-cargo-realizan-ciberpatrullaje-en-redes-sociales-para-detectar-el-humor-social, último acceso: 23 de mayo de 2023.

[37] 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: 23 de mayo de 2023.

[38] Disponible en: https://twitter.com/nicolucero69/status/765936986217668608, último acceso: 23 de mayo de 2023.

[39] "Declaran 'inocente' al joven que estuvo preso por un tuit contra Mauricio Macri", Diario Perfil, 2018, disponible en: https://www.perfil.com/noticias/sociedad/declaran-inocente-al-joven-que-escribio-un-tuit-contra-macri.phtml, último acceso: 23 de mayo de 2023.

40 Disponible en: https://twitter.com/KevinGuerra99/status/1247709948554903554, último acceso: 23 de mayo de 2023.



El tuit fue detectado por la Gendarmería nacional –dependiente del Ministerio de Seguridad– en el contexto de "tareas de ciberpatrullaje en redes sociales" y Kevin fue denunciado penalmente por esa fuerza. La causa judicial fue caratulada como "intimidación pública".[41] Finalmente, Kevin fue sobreseído. Según lo que informó el Centro de Estudios Legales y Sociales (CELS), que asumió su defensa, el tuit en cuestión surgió de una búsqueda realizada por la Gendarmería nacional al utilizar los términos "saquear, cuarentena, Argentina". Además, Gendarmería fundó su actuación en la habilitación conferida por la resolución Nº 31/2018 del Ministerio de Seguridad de la Nación.[42]

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.[43]

[41] "Habló Kevin Guerra, detenido por twittear: 'Todo esto fue un chiste'", Diario Ámbito, 2020, disponible en: https://www.ambito.com/informacion-general/bono/hablo-kevin-guerra-detenido-twittear-todo-esto-fue-un-chiste-n5095854, último acceso: 23 de mayo de 2023.

[42] "La justicia federal sobreseyó a Kevin Guerra por sus expresiones en Twitter", Centro de Estudios Legales y Sociales (CELS), 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: 23 de mayo de 2023.

[43] "En medio de la pandemia por coronavirus, se realizaron 20 allanamientos contra agitadores en las redes sociales", A24, 2020, disponible en: https://www.a24.com/policiales/medio-pandemia-coronavirus-realizaron-20-allanamientos-agitadores-redes-sociales-09042020_umqdiP2qx, último acceso: 23 de mayo de 2023.

b. Ministerio de Defensa

El Ministerio de Defensa respondió el pedido de acceso a la información pública del CELE al comunicar que no recopila información de fuentes abiertas ni se han realizado ni aprobado estudios, regulaciones, propuestas de regulaciones ni documentos para los cuales se hayan recopilado datos de fuentes abiertas.

c. Oficina anticorrupción

En su respuesta al pedido de acceso a la información pública, la Oficina Anticorrupción informó que la Coordinación de Admisión y Derivación de Denuncias "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 1.316/2008", que 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.

d. Ministerio de Relaciones Exteriores

En respuesta al pedido de acceso a la información pública del CELE, el Ministerio de Relaciones Exteriores informó que no realiza recolección de información mediante fuentes abiertas. Frente a la requisitoria, más específica, de si a los fines de las convocatorias a eventos o reuniones realizados en el marco del Ministerio, se lleva a cabo previamente una búsqueda de información en fuentes abiertas sobre las personas a invitar, este contestó que:

> todo evento, conferencia o convocatoria que sea realizada por este Ministerio se encuentra debidamente coordinada por el área sustantiva o primaria. En este sentido, las personas a invitar dependen enteramente de la característica del evento a realizarse y de las consideraciones que estime el área oportuna. Por estos motivos, y en virtud de las particularidades que cada reunión requiera, es que las invitaciones se extienden sin un protocolo de actuación predeterminado.

No obstante lo informado, se ha denunciado que en los meses previos a las reuniones de la OMC y del G20 que se llevaron a cabo en el país en los años 2017 y 2018, la Agencia Federal de Inteligencia, a requerimiento del Ministerio de Relaciones Exteriores, realizó perfilamientos ilegales de periodistas, académicos y miembros de la sociedad civil que pretendían acreditarse o concurrir a esas reuniones, con el fin de determinar si su participación sería aceptada.[44] Con base en esos perfilamientos, se rechazaron sesenta y cinco acreditaciones, e incluso se deportó a algunos extranjeros que decidieron ingresar al país a pesar de que su acreditación hubiera sido rechazada.[45] 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".[46] De las propias afirmaciones del Ministerio, se sigue que se realizó inteligencia con base en fuentes abiertas para llevar a cabo perfilamientos políticos, explícitamente prohibidos por la Ley de Inteligencia.

[44] "Piden la indagatoria de Arribas y Majdalani por espionaje ilegal en las cumbres de la OMC y el G20", Diario Ámbito, 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: 23 de mayo de 2023.

[45] "Reunión de la OMC en la Argentina: acreditaciones rechazadas y deportaciones", CELS, 2017, disponible en: https://www.cels.org.ar/web/2017/12/wto-meeting-in-argentina-rejected-accreditations-and-deportations, último acceso: 23 de mayo de 2023.

[46] 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: 26 de mayo de 2023.

e. AFIP

La AFIP ha contestado la solicitud de información al referir que "según lo informado por las áreas de sistemas del Organismo, no se tiene información para brindar respecto de su consulta relativas a la regulación interna sobre la recolección de datos personales de fuentes 'abiertas' o 'semiabiertas'". La agencia recaudadora aportó que:

> conforme al marco legal establecido por las leyes Nº 11.683 (t.o. en 1998 y sus modificaciones) y Nº 27.430 y normas reglamentarias, esta Administración Federal de Ingresos Públicos cuenta con determinados regímenes de información (generales y específicos) que constituyen herramientas para optimizar las funciones de fiscalización y control de los gravámenes a cargo del Organismo, evitar maniobras de evasión, como así también inducir a una mayor transparencia en las operaciones respectivas.

Sin embargo, trascendió que en noviembre de 2022 y tras una investigación publicada en la prensa,[47] la AFIP realizó una denuncia ante una fiscalía especializada en ciberdelincuencia en relación con la actividad de personas que, presuntamente,

[47] 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: 23 de mayo de 2023.

se encontraban ofreciendo 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 realizar 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".[48]

f. 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.[49] 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".[50] Muchas de ellas 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. En ese entorno, la Agencia entregó las carpetas de inteligencia producidas a los damnificados.

El periodista Rodis Recalt, de la editorial Perfil, compartió el contenido de la carpeta que respecto suyo la AFI había confeccionado.[51] Allí se puede observar la utilización de OSINT y otras formas de inteligencia para construir su perfil.

---

[48] 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: 23 de mayo de 2023.

[49] 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: 23 de mayo de 2023.

[50] 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: 23 de mayo de 2023.

[51] 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: 23 de mayo de 2023.

g. Policía de la Ciudad

En el marco de su respuesta a la solicitud de información pública formulada por esta investigación, la Policía de la Ciudad informó 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". En julio del 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 por entonces secretario de Seguridad del Gobierno porteño, Marcelo D'Alessandro, expresó a la prensa que los dos 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".[52] 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.

El CELE consiguió entrevistar a una persona que trabajaba en esta Fuerza de Seguridad y ha realizado tareas de OSINT.[53] Expresó que las búsquedas se realizaban 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 de la persona y después se fijan en todas las redes sociales hasta dar cuenta de quién es, con quién se junta, etc.". Finalmente, informó que la Policía de la Ciudad entiende como una habilitación a la práctica de OSINT lo normado en el artículo 10 de la Ley Nº 5.847 de 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, a través de la Policía de la Ciudad, prestará colaboración para impedir el acceso a los predios y la permanencia

[52] "Amenazaron con mensajes en árabe que iban a atentar contra Macri", Diario Clarín, 2016, disponible en: https://www.clarin.com/policiales/amenazaron-mensajes-arabe-atentar-macri_0_SJNELzqO.html, último acceso: 23 de mayo de 2023.

[53] Entrevista realizada el 27 de octubre de 2022. La persona entrevistada solicitó mantener en reserva su identidad por no tener autorización para conversar públicamente sobre sus funciones.

> en los mismos, de aquellas personas que se encuentren incluidas en la Base de Antecedentes sobre Violencia en Eventos Futbolísticos de la CABA. 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, 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.

En cuanto a los límites de las búsquedas, la persona entrevistada informó que "existen criterios de búsqueda, depende de la orientación del Poder Judicial".

V. Sector privado

En una entrevista realizada en el marco de esta investigación, una especialista en protección de datos y privacidad, con 25 años de trayectoria en consultoría privada, así como en distintas áreas del sector público, incluidas áreas vinculadas a las Fuerzas de Seguridad, expresó que:

> *el sector privado hace muchísimo uso de fuentes abiertas* (…). Hay sitios que te dan todas las herramientas para realizar OSINT, por ejemplo, el sitio https://ciberpatrulla.com, que tiene guías sobre cómo ciberpatrullar, o los cursos que dan en OSINT Latam Group. Después hay herramientas que hacen análisis de fuentes abiertas que tienen versiones gratis y versiones pagas, como Maltego (uno de los más conocidos), Social Links y Shodan. Todos estos hacen análisis de fuentes abiertas.[54]

La elaboración de este apartado, no obstante, resultó particularmente desafiante debido a que las empresas que proveen servicios de OSINT no necesariamente lo indican explícitamente en sus sitios web. Muchas empresas indican que realizan consultorías en temas de ciberseguridad. Es posible que esto incluya herramientas y usos de OSINT, pero no es posible asegurarlo según la información de sus

[54] El resaltado no pertenece al original.

sitios web.[55] También resultó desafiante en tanto no se ha conseguido entrevistar a representantes de empresas que quisieran compartir su visión sobre el uso de herramientas OSINT para este reporte.

Algunas empresas indican que ofrecen servicios de *threat intelligence* o inteligencia de amenazas en español, sin indicación de qué implica esto. Es el caso, por ejemplo, de Sonda,[56] cuyo sitio web indica que tiene oficinas en Argentina y en otros países de la región. Se encontraron empresas que ofrecen servicios de OSINT, pero no están basadas en Argentina, como por ejemplo Social Links[57] y Factal,[58] ambas basadas en Estados Unidos; o Maltego[59] y Shodan,[60] las cuales no indican tener oficinas físicas en sus sitios web.

En Argentina existen sitios web que ofrecen descargar herramientas para OSINT de forma gratuita. Es el caso de Digitalmente Seguro[61] (sin oficinas físicas, desarrolló Argentosint,[62] una app con herramientas de fuentes abiertas de información disponible en Google Play Store), OSINT Latam Group[63] (sin oficinas) y OSINT.com.ar[64] (sin oficinas, ofrece herramientas para realizar OSINT, recomendaciones y otros datos; también dice ofrecer servicios de ciberseguridad), y OSINT Latinoamérica[65] (centro especializado en el diseño y la impartición de programas de capacitación en inteligencia y seguridad, basado en México, que ofrece cursos sobre OSINT).

Finalmente, de las averiguaciones realizadas en el marco de esta investigación, no han surgido protocolos específicos para centros de investigación académica que permitan o limiten las prácticas de OSINT.

---

55 Se puede encontrar un listado de empresas que ofrecen servicios de ciberseguridad en Argentina en https://ciberseguridad.com/empresas/argentina, último acceso: 23 de mayo de 2023.

56 Disponible en: https://www.sonda.com/soluciones/ciberseguridad, último acceso: 23 de mayo de 2023.

57 Disponible en: https://sociallinks.io, último acceso: 23 de mayo de 2023.

58 Disponible en: https://www.factal.com/about, último acceso: 23 de mayo de 2023.

59 Disponible en: https://www.maltego.com, último acceso: 23 de mayo de 2023.

60 Disponible en: https://www.shodan.io, último acceso: 23 de mayo de 2023.

61 Disponible en: https://digitalmenteseguro.com.ar, último acceso: 23 de mayo de 2023.

62 Disponible en: https://digitalmenteseguro.com.ar/app-de-osint-para-argentina, último acceso: 23 de mayo de 2023.

63 Disponible en: https://twitter.com/osintlatamgroup?lang=en, último acceso: 23 de mayo de 2023.

64 Disponible en: https://osint.com.ar, último acceso: 23 de mayo de 2023.

65 Disponible en: https://osintlatinoamerica.com, último acceso: 23 de mayo de 2023.

VI. Jurisprudencia relevante

a. Caso "Bejarano"[66]

El 10 de marzo de 2013 en la Ciudad de Buenos Aires, Elvio Sosa Ruiz se encontraba durmiendo en la vía pública cuando Alexis Ezequiel Bejarano, junto con otro individuo aún no identificado, lo rociaron con una lata que contenía algún tipo de combustible, y prendieron fuego. Sosa Ruiz falleció en el hospital al día siguiente producto de sus quemaduras. Los testigos del hecho apuntaron a un sujeto apodado "Chucky" como autor del hecho. A través de la red social Facebook, la Policía consiguió atribuir tal apodo a Alexis Ezequiel Bejarano.

El Tribunal Oral en lo Criminal Nº 20 de la Ciudad de Buenos Aires condenó a Alexis Ezequiel Bejarano por el delito de homicidio calificado por haber sido cometido con alevosía a la pena de prisión perpetua. El acusado planteó la nulidad de esta resolución al alegar la violación a los artículos 234 del Código Procesal Penal de la Nación[67] y 153 del Código Penal[68] sobre la inviolabilidad de la correspondencia. Se refirió a las impresiones obtenidas de su perfil de Facebook que fueron incorporadas a la causa. Sostuvo que "al ser equiparado el correo electrónico y las redes sociales a la correspondencia epistolar, tal información para que tenga valor probatorio debe ser obtenida por medio de la orden judicial correspondiente, de conformidad con lo establecido en el artículo 234 del CPPN". Alegó que las impresiones de Facebook se obtuvieron sin orden judicial y por lo tanto los funcionarios policiales y judiciales habían incurrido en el tipo penal del artículo 153 del Código Penal.

---

66 "Bejarano, Alexis Ezequiel s/Recurso de Casación", Sala IV de la Cámara Federal de Casación Penal, sentencia del 4 de diciembre de 2015. "La Cámara Federal de Casación Penal confirma condena por homicidio cometido con alevosía", Centro de Información Judicial (CIJ), disponible en: https://www.cij.gov.ar/nota-19281-La-C-mara-Federal-de-Casaci-n-Penal-confirma-condena-por-homicidio-cometido-con-alevos-a.htm, último acceso: 23 de mayo de 2023.

67 "Intercepción de correspondencia. Art. 234. - Siempre que lo considere útil para la comprobación del delito el juez podrá ordenar, mediante auto fundado, la intercepción y el secuestro de la correspondencia postal o telegráfica o de todo otro efecto remitido por el imputado o destinado a este, aunque sea bajo nombre supuesto".

68 "Art. 153. - Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena".

La Sala IV de la Cámara Federal de Casación Penal confirmó la sentencia. En el voto de mayoría, el juez Hornos sostuvo que:

> a partir de sus características públicas, la página de Facebook propiedad del imputado no goza de la protección de la privacidad como la clásica vía postal. Ello así, desde que si bien para su funcionamiento y utilización se requiere indispensablemente de un prestador del servicio, el nombre de usuario y clave de acceso destinados a impedir que terceros extraños se entrometan en los datos y contenidos que se emiten y reciben, lo cierto es que el perfil de BEJARANO en la red social en cuestión era público y casi toda la información que compartía podía ser vista por cualquier persona que accediera a través de internet a la página.[69]

En consecuencia, entendió que Facebook no puede ser considerada como análoga a la "correspondencia epistolar" protegida en el artículo 18 de la Constitución Nacional, y en este sentido el modo en que han sido obtenidas las capturas e incorporadas como prueba no violan dicha garantía. Continúa su voto al indicar que:

> el procedimiento por el cual se obtuvo e incorporó como prueba la página de Facebook mediante la cual se pudo corroborar que el sujeto apodado "Chucky" se correspondía con el nombre y fotografía que figuraban en ese perfil de la red social fue realizado conforme a las disposiciones legales vigentes sin afectar la garantía que prohíbe intromisiones arbitrarias en la intimidad y privacidad del imputado y por ello propongo rechazar el presente agravio.[70]

El Tribunal Oral en lo Criminal Nº 20 de la Capital Federal condenó a Bejarano por el delito de homicidio calificado por haber sido cometido con alevosía a la pena de prisión perpetua. La Sala IV de la Cámara Federal de Casación Penal, con fecha 4 de diciembre de 2015, rechazó el recurso de casación interpuesto por Bejarano.

Esta jurisprudencia habilita el uso de información obtenida en redes sociales (al menos en perfiles públicos de Facebook) como prueba, incluso cuando su obtención no haya sido ordenada judicialmente. No se refiere específicamente a la de-

[69] "Bejarano, Alexis Ezequiel s/Recurso de Casación", *supra* nota 68, p. 5.

[70] *Ibíd*.

finición de fuente abierta, pero sí indica que si un perfil de Facebook se encuentra "abierto" (visible sin necesidad de "solicitar amistad"), el mismo es "público", en tanto cualquier usuario o usuaria de internet podría ver sus publicaciones.

b. "La gorra leaks"

En 2017, mediante una práctica de *phishing*, un hacker que se presentaba bajo el seudónimo "[S]", y que aún no pudo ser identificado, logró acceder a la base de datos de la Policía Federal Argentina. Bajo el usuario "La gorra leaks", en 2019, se publicaron más de 700 gigabytes de archivos con información sensible de esa fuerza en Github, en la Deep Web, en un canal de Telegram y en una cuenta de Twitter. En el marco de la investigación, se utilizaron las redes sociales y el análisis de tuits de sospechosos, que terminaron con una acusación al desarrollador de software Javier Smaldone, en una causa repleta de irregularidades.

En el dictamen del 22 de marzo de 2021, emitido por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), a cargo del fiscal Horacio Azzolin, se señaló que entre los motivos por los que señalaron a Smaldone en la causa estuvieron su conocimiento en lenguajes informáticos, el "señalamiento realizado por terceros en redes sociales y otras plataformas de internet, su 'hostigamiento' a la Policía vía redes sociales, sus tuits sobre este y otros ataques informáticos que tuvieron lugar en el país y, finalmente, sus publicaciones en las que cuestionaba el sistema de voto electrónico".[71] El dictamen expuso que "desde nuestro punto de vista es un conjunto de apreciaciones sin rigor científico ni anclaje concreto en elementos objetivos del caso que pretenden vincular a un perfil determinado de persona con un hecho".

Finalmente, el fiscal remarcó que se intentó vincular a una persona con un hecho con base en "un posible perfil de persona inferido de las expresiones públicas en una red social concreta que tiene una lógica comunicacional específica", y que "las apreciaciones [de la investigación] parecen ser propias de otras épocas, colisionan con el derecho a la libertad de expresión y no deberían ser tomadas en cuenta como premisas para construir un caso".[72] Los quince acusados fueron sobreseídos y la causa archivada en el mes de noviembre de 2021.

---

[71] Dictamen de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público Fiscal (UFECI), subido a internet por el propio Smaldone, disponible en: https://ia804605.us.archive.org/27/items/dictamen_ufeci_ocr/dictamen_ufeci_ocr.pdf, último acceso: 23 de mayo de 2023.

[72] *Ibíd*.

VII. Conclusiones

La historia de la reglamentación de OSINT en Argentina es una de avances temerarios y retrocesos tardíos ante la evidencia de que los intentos regulatorios no cumplían con estándares internacionales de derechos humanos ni legislación interna. En un primer momento, se otorgó una habilitación amplia a las Fuerzas de Seguridad para practicar OSINT en la investigación de determinados delitos, sin prácticamente limitaciones, y todo ello por medio de una resolución ministerial (la Nº 31/2018) que ni siquiera fue publicada en el Boletín Oficial. Luego vino la Resolución 144/2020, que reconoció los defectos de su predecesora, a la que derogó, para establecer algunas limitaciones fundadas en estándares insuficientemente definidos. Finalmente, el Ministerio de Seguridad, mediante resolución Nº 720/2022, se hizo eco de algunas de estas deficiencias y derogó el mencionado protocolo, más de dos años después de haber recibido advertencias, por parte de la Agencia de Acceso a la Información Pública, acerca de algunas de las potenciales afectaciones de la resolución Nº 144/2020 al derecho a la privacidad de los ciudadanos y las ciudadanas. Hoy no existe en el país una normativa que regule la utilización estatal de OSINT.

La práctica de OSINT por parte del Estado sin sujeción a reglamentaciones específicas ni a estándares generales tiene implicancias negativas en derechos humanos, principalmente en lo que respecta a privacidad y libertad de expresión. Si bien la mayoría de las dependencias públicas consultadas han señalado que no realizan OSINT, a lo largo de esta investigación se han identificado instancias concretas en las que diferentes agencias estatales argentinas han practicado OSINT con fines de vigilancia. De allí que, aunque no se pueda afirmar que la práctica se lleva adelante en forma sistemática, sí puede decirse que las autoridades recurren a ella al menos esporádicamente.

Existe una enorme opacidad en la forma en la que la administración pública realiza inteligencia de fuentes abiertas sobre sus ciudadanos y ciudadanas. Ello, a su vez, dificulta en extremo el control de la actividad en varios sentidos. Por una parte, la naturaleza de la actividad y sus potenciales afectaciones en derechos humanos requerirían la puesta en funcionamiento de un sistema de rendición de cuentas mediante el cual el Estado reporte periódicamente la actividad OSINT que lleva adelante. Por otra parte, el reconocimiento de que el Estado se involucra en actividades de esta índole facilitaría la imposición de obligaciones de transparencia respecto de la contratación con terceros de servicios relacionados

con esta actividad. Finalmente, otro aspecto derivado de la práctica de OSINT por fuera de las normas es que se hace con informalidad, sin guías claras ni entrenamiento especializado a los sujetos que la llevan adelante.

En la legislación argentina, el concepto de "fuentes abiertas" no se encuentra claramente definido. En tanto, la Ley de Inteligencia asume, erróneamente, que la información accesible públicamente no se encuentra al amparo de la protección constitucional y convencional del derecho a la privacidad.

Este equívoco podría surgir de la noción de entender a internet –o al menos cierto contenido allí existente– como un "espacio público digital" que puede patrullar libremente. Sin embargo, ello no es así por varios motivos. En primera instancia, no es de titularidad estatal. En segundo lugar, el concepto de fuente abierta podría requerir una revisión y la disponibilidad "libre" de los contenidos debe ser matizada, en tanto no todos los contenidos calificados como tal son igualmente accesibles, y no todos fueron concebidos para ser vistos por el público en general (los blogs personales o familiares son fuente abierta de la misma forma que un portal de noticias). Por otro lado, 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. A diferencia de lo que ocurre en el espacio público, las personas cuando interactúan en internet no están esperando ser observadas por agentes estatales.

A más de ello, las tecnologías de *scraping* y otras hoy existentes permiten extraer gran cantidad de información de la web a una gran velocidad y a un costo radicalmente menor al que se incurriría de otro modo. La utilización de ese tipo de programas es mucho más invasiva que el "patrullaje" de las calles y extrae mucha más información que la estrictamente necesaria para los fines estatales buscados, por lo que podría no satisfacer los estándares de necesidad y proporcionalidad requeridos por el Derecho Internacional de los Derechos Humanos.[73]

El –mal llamado– "ciber patrullaje" se lleva adelante en forma secreta, sin que los agentes que la realizan se identifiquen, a diferencia de la actividad de prevención policial en las calles. Por lo que no se trata de patrullaje, sino de lisa y llana inteligencia. Por ello, deberían cumplirse, al menos, las disposiciones de la Ley de Inteligencia Nacional, cuyo artículo 4º prohíbe expresamente las tareas de

[73] Art. 17 PIDCP, *supra* nota 35.

inteligencia criminal por fuera del requerimiento judicial específico en el marco de un proceso judicial, o a través de autorización legal. Cuando se lleva adelante sin orden judicial ni una hipótesis delictiva concreta, adquiere los rasgos de una "excursión de pesca" policial y la legalidad del procedimiento se vuelve endeble.

Por todo lo anterior, resulta necesario reconocer legalmente la existencia y el alcance de la expectativa de privacidad online de la que gozan los ciudadanos y las ciudadanas, de acuerdo con los tratados y la Constitución nacional. Para ello, es importante que la definición legal del concepto de "fuentes abiertas" tenga esto en cuenta.

La actividad de OSINT por parte del Estado debe ser reglamentada legalmente, de acuerdo con criterios respetuosos de los derechos humanos. En primer lugar, debe dejarse de lado el concepto de "ciberpatrullaje" y encuadrarse la actividad como una de inteligencia. En el caso de la inteligencia criminal, solamente debería ser practicada en virtud de una orden judicial previa, fundada y específica, lo más restrictiva posible, y únicamente cuando la intervención resulte estrictamente conducente para la investigación. Respecto de la información obtenida, debería conservarse aquella que resulte relevante para la finalidad requerida en el expediente, y eliminar el resto. Es esencial que el personal que practica esta tarea sea capacitado en derechos humanos y protección de datos personales. Vale dejar a salvo que lo anterior aplica a la actividad estatal, y que de ninguna manera debería afectar la actividad de periodistas e investigadores, ni el derecho de toda la comunidad a acceder a la información.

Por último, es necesario implementar mecanismos especialmente rigurosos de transparencia y publicidad en la adquisición del software utilizado por las dependencias estatales para estas tareas –o su contratación con privados en caso de que se tercericen– y de rendición de cuentas en su utilización.