CELE

# Las prácticas OSINT, ¿son amigas o enemigas de los derechos humanos?

*Noviembre 2023*

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

UP
Universidad
de Palermo

# Las prácticas OSINT, ¿son amigas o enemigas de los derechos humanos?*

***Eduardo Bertoni*****
***CELE***

## I. Introducción

La revisión bibliográfica sobre la inteligencia en fuentes abiertas (OSINT, por sus siglas en inglés) da cuenta de que es difícil encontrar el origen de este concepto. Se trata de una práctica que tiene cientos de años de antigüedad que, como su nombre lo indica, se refiere a la recolección de información disponible en fuentes abiertas con el objeto de realizar tareas de inteligencia.

Así descripto, parece un concepto autoevidente. Sin embargo, definir OSINT de una sola forma no es tarea sencilla. El concepto esconde implicancias que intentaremos abordar en el presente trabajo, relacionadas con las interpretaciones de "fuentes abiertas" y de "inteligencia".

"Fuentes abiertas" puede implicar que "es accesible para cualquier persona sin necesidad de contar con credenciales especiales de acceso de ningún tipo, en contraposición a información que se encuentra detrás de una capa de protección, por ejemplo, usuario y contraseña".[1] Sin embargo, esta libertad en el acceso puede verse limitada por distintos motivos, por ejemplo, si los datos que allí se encuentran no debieran ser objeto de "tratamiento", en concordancia con las leyes de protección de datos personales.

---

* El presente trabajo fue realizado por Eduardo Bertoni a solicitud del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Artículo 19 México y Centroamérica, Artigo 19 y Fundación Karisma, con el apoyo de la oficina de Democracia, Derechos Humanos y Trabajo (DRL) del Departamento de Estado de los Estados Unidos. El autor agradece la colaboración de Agustina del Campo, Ramiro Álvarez Ugarte y Morena Schatzky por sus comentarios y sugerencias.

** Doctor en Derecho (Universidad de Buenos Aires). Representante de la Oficina Regional de Sudamérica del Instituto Interamericano de Derechos Humanos (IIDH). Exdirector de la Agencia de Acceso a la Información Pública (AAIP) de Argentina en el período 2017-2020. Fundador y exdirector (2009-2016) del Centro de Estudios en Libertad de Expresión (CELE) de la Universidad de Palermo. Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) de la OEA para el período 2002-2005. Profesor en la Facultad de Derecho de la Universidad de Buenos Aires y de la Universidad de Nueva York (NYU).

[1] 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, p. 5, disponible en: https://adc.org.ar/wp-content/uploads/2019/06/045-seguidores-que-no-vemos-10-2018.pdf, último acceso: 23 de agosto de 2023.

El concepto de "inteligencia", por su parte, también merece algunas precisiones ya que comprende distintos significados. El más obvio de ellos es el uso que le damos a "inteligencia" al referirnos a una persona como "inteligente", es decir, relacionada con la capacidad de entender o comprender, o la capacidad de resolver problemas.[2] Ahora bien, cuando en el lenguaje coloquial las personas se refieren a la palabra "inteligencia" como actividad, esta aparece inmediatamente ligada a tareas que realizan las fuerzas de seguridad de los Estados con el objeto de prevenir tanto ataques que provengan del exterior, como delitos que puedan ocurrir en un determinado territorio, o –en general– a la captura de información valiosa para la toma de decisiones, a veces a través de métodos subrepticios. Pero, como veremos en este trabajo, hoy en día las "tareas de inteligencia" pueden perseguir otros objetivos no relacionados con la prevención de delitos, ya sea para perseguir fines comerciales, llevar a cabo investigaciones científicas o académicas, u otros.

Existen, entonces, distintos usos posibles de OSINT de la mano de múltiples y diversos actores. En algunos casos se trata de una práctica que implementan las fuerzas de seguridad con fines de vigilancia y prevención de delitos;[3] en otros, es una práctica que utilizan sectores académicos con fines de investigación académica. OSINT también se ha convertido en un servicio prestado por empresas privadas –a veces a solicitud de los Estados–, cuyos fines pueden ser variados.

Esta investigación entenderá a OSINT como la recolección y el análisis de datos de fuentes abiertas –sean o no personales– con una determinada finalidad. Esa finalidad puede ser con o sin fines de lucro; con fines de vigilancia, de investigación científica o académica; o tratarse de fines exclusivamente personales y, en este sentido, cualquier persona puede realizar esta práctica.

El presente trabajo procurará servir como diagnóstico inicial para aportar claridad conceptual a la definición de OSINT, a través de la elaboración de un análisis acerca de las posibles vulneraciones sobre derechos fundamentales, especialmente aquellas que afectan el derecho a la privacidad. Además, incluirá los

[2] Ver definición de la Real Academia Española (RAE), disponible en: https://dle.rae.es/inteligencia, último acceso: 23 de agosto de 2023. Según la misma fuente, es necesario aclarar que, cuando la referencia es a "servicios de inteligencia", se los define como "organización del Estado que proporciona al Poder Ejecutivo análisis e información para mejorar la toma de decisiones estratégicas orientadas a prevenir o neutralizar amenazas y a defender los intereses nacionales". De allí es que, comprendemos, se entienda que OSINT está referido únicamente a ello, y de allí que se lo confunde con ciberbatrullaje o vigilancia, aunque, como se explica en este trabajo, OSINT incluya prácticas que nada tienen que ver con ello y cuyas regulaciones pueden ser distintas.

[3] En ciertos casos, como veremos con la situación de un protocolo para las fuerzas de seguridad de Argentina, las prácticas OSINT se las llama directamente "ciberpatrullaje".

estándares internacionales que dan contenido tanto al derecho a la privacidad, como al acceso a la información que resultan útiles para el análisis de la problemática. Como conclusión preliminar y núcleo de esta investigación, se destaca el carácter claroscuro del concepto: OSINT es una práctica problemática desde el punto de vista de la protección de los datos personales, pero también es una herramienta clave para fortalecer el ejercicio de la libertad de expresión en su contracara: tanto para el derecho de "acceso" a la información como para el derecho a "buscar" información. El acceso a la información de fuentes abiertas constituye una condición necesaria para la investigación y la producción de conocimiento, una tarea valiosa en todo tipo de sectores.

A tal fin, el trabajo se ordenará de la siguiente manera: en primer lugar, se echará luz sobre el concepto y sus diferentes interpretaciones, al analizar por separado los conceptos de "fuentes abiertas" e "inteligencia", y sus implicancias. Seguidamente, se abordará la multiplicidad de actores que realizan OSINT, desde agencias de inteligencia, fuerzas de seguridad y otros organismos del sector público, hasta empresas privadas e individuos. Una vez planteado el concepto y sus usos, se analizarán los diversos dilemas conceptuales que OSINT presenta. Entre ellos, el trabajo hará énfasis en torno al dilema de que si bien los datos de fuentes abiertas están disponibles para cualquier persona, eso no significa que puedan ser objeto de "tratamiento" desde el punto de vista de las regulaciones en materia de protección de datos personales. Por último, se enfatizará otra disyuntiva que OSINT plantea con respecto al acceso a la información: si bien puede implicar vulneraciones al derecho a la privacidad y a la protección de datos personales, las actividades comprendidas en las prácticas OSINT se encuentran inherentemente relacionadas con el ejercicio del derecho de acceso a la información y, en este sentido, con el derecho a buscar información. La conclusión hará hincapié en esa contradicción, al afirmar que las prácticas de recolección de datos en fuentes abiertas son una herramienta que fortalece el ejercicio de la libertad de expresión.

## II. OSINT(s)

De acuerdo a definiciones usuales, OSINT involucra la recolección de información disponible en fuentes accesibles de manera sencilla con el objeto de realizar tareas de inteligencia. Pero, como vimos en la introducción, el concepto tiene un carácter polisémico.

## *II.1. Sobre fuentes abiertas (open source)*

Como su nombre lo indica, OSINT tiene una directa relación con el concepto de "fuente abierta". Esta es aquella "accesible para cualquier persona sin necesidad de contar con credenciales especiales de acceso de ningún tipo, en contraposición a información que se encuentra detrás de una capa de protección, por ejemplo, usuario y contraseña".[4]

Las prácticas OSINT se caracterizan por la recolección de datos de fuentes abiertas accesibles tanto en el mundo offline como online. Los datos y la información pueden estar disponibles en medios de prensa tradicionales (televisión, radio, periódicos); en publicaciones académicas en revistas y bibliotecas; y en internet, donde hoy en día se hace mayormente la recolección de datos e información mediante OSINT.

Según diversos autores, es posible distinguir las fuentes de información en tres niveles: en el primer nivel se encuentran aquellas de acceso libre, sin ningún tipo de restricción para acceder a los datos allí alojados (por ejemplo, el Boletín Oficial); en el segundo nivel, en cambio, la fuente es de carácter semipúblico y no pago, en el sentido de que se exige una registración previa del usuario o de la usuaria a la plataforma como requisito para acceder a los datos (por ejemplo, LinkedIn); el tercer y último nivel también es de carácter semipúblico, el cual exige una registración previa, pero además es pago, donde el usuario o la usuaria debe abonar un importe para acceder a los datos que busca (por ejemplo, a través de Nosis).[5]

A pesar de lo útil que pueda resultar hacer esta clasificación de las fuentes de información, es necesario tener presente la ambigüedad que existe en los alcances de lo que puede considerarse como "información pública" o "información privada", ya que dentro de cada uno de estos niveles también pueden encontrarse datos de carácter tanto público como privado. Veremos esto en detalle más adelante.

La recolección en fuentes abiertas puede realizarse de diferentes maneras, pero la forma que más se utiliza para OSINT es la que denominan "recopilación pasiva". En este tipo de recolección se utilizan recursos disponibles públicamente y el ti-

---

4 ADC, *supra* nota 2, p. 5.

5 Monte, Martina y Sánchez, Santiago I., "Tensiones constitucionales entre el derecho a la intimidad y el ciberpatrullaje en la investigación criminal. Análisis del Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas", Academia, 2020, disponible en: https://www.academia.edu/47689666/Tensiones_constitucionales_entre_el_derecho_a_la_intimidad_y_el_ciberpatrullaje_en_la_investigaci%C3%B3n_criminal_An%C3%A1lisis_del_Protocolo_General_para_la_Prevenci%C3%B3n_Policial_del_Delito_con_Uso_de_Fuentes_Digitales_Abiertas, último acceso: 23 de agosto de 2023.

tular de los datos no es notificado ni alertado respecto de la búsqueda. La misma es altamente anónima y en secreto, un aspecto esencial para OSINT.[6]

## *II.2. Sobre inteligencia*

La inteligencia se entiende, por un lado, como la simple tarea de investigar, de buscar información para ganar un conocimiento profundo de algún tema con base en información, recursos y fuentes. En este sentido, las tareas de inteligencia pueden perseguir otros objetivos comerciales, o informar investigaciones científicas o académicas, llevadas adelante por actores privados. Sin embargo, cuando en el lenguaje coloquial se hace referencia a inteligencia como actividad, esta aparece inmediatamente ligada a tareas que realizan las fuerzas de seguridad de los Estados con el objeto de prevenir tanto ataques que provengan del exterior, como delitos que puedan ocurrir en un determinado territorio. Desde este punto de vista, la inteligencia es una actividad acotada a las fuerzas de seguridad de un Estado.

Si bien estos conceptos son diferentes entre sí, OSINT puede implicar todas estas acepciones: existen usos del término OSINT que refieren a prácticas de investigación dentro de la primera versión de inteligencia, y también hay usos de OSINT vinculado a investigaciones que realizan agentes estatales con fines de investigación, vigilancia y prevención de delitos –este, podría decirse, es el sentido tradicional del término "inteligencia"–.

De esta forma, parece interesante destacar la definición de OSINT dada por el Departamento de Defensa de los Estados Unidos: "La inteligencia de fuente abierta (OSINT) es una inteligencia que se produce a partir de información disponible públicamente y se recopila, explota y difunde de manera oportuna a una audiencia adecuada con el fin de abordar un requisito de inteligencia específico".[7]

Según algunos autores,[8] la inteligencia en fuentes abiertas cobra relevancia du-

---

[6] Hassan, Nihad A. y Hijazi, Rami, *Open Source Intelligence. Methods and Tools. A Practical Guide to Online Intelligence*, Nueva York, Apress, 2018, pp. 14-15.

[7] La traducción es propia. Ver U.S. Government, "National Defense Authorization Act For Fiscal Year 2006", Public Law 109-163, 109th Congress, Subtitle D - Intelligence-Related Matters, disponible en: https://www.govinfo.gov/content/pkg/PLAW-109publ163/html/PLAW-109publ163.htm, último acceso: 23 de agosto de 2023.

[8] Hassan y Hijazi, *supra* nota 7.

rante la segunda guerra mundial, cuando en los Estados Unidos se creó el Servicio de Información de Transmisiones Extranjeras (FBIS, por sus siglas en inglés), dedicado principalmente al monitoreo de información pública que pudiera estar relacionada con el apoyo a las operaciones militares durante la guerra.

El FBIS siguió activo luego de terminada la segunda guerra mundial. Décadas más tarde, a raíz del ataque terrorista a las Torres Gemelas en la ciudad de Nueva York, la Comisión que investigó el ataque (9/11 Commission, en inglés) sugirió la creación de una agencia especializada en recolección de información disponible en fuentes abiertas. En consecuencia, el director nacional de Inteligencia de ese país creó el Centro Nacional de Inteligencia con Fuentes Abiertas (National Intelligence Open Source Center, en inglés) que tomó todas las actividades que había realizado hasta ese momento el FBIS. Posteriormente, se creó una oficina dentro de la Agencia Central de Inteligencia (CIA, por sus siglas en inglés) bajo el título de Open Source Enterprise.[9]

De acuerdo a la definición dada por el Manual sobre Inteligencia de Fuentes Abiertas de la Organización del Tratado del Atlántico Norte (NATO), publicado a finales de 2001:

> OSINT es información que ha sido deliberadamente descubierta, discriminada, destilada y difundida a una audiencia *selecta*, generalmente al comandante y su personal inmediato, para abordar una pregunta *específica*. OSINT, en otras palabras, aplica el proceso probado de inteligencia a la amplia diversidad de fuentes abiertas de información y *crea inteligencia*.[10]

Estos ejemplos sirven para visualizar la íntima relación que comúnmente se da al concepto OSINT con las actividades de los servicios de inteligencia en su acepción tradicional.

### *II.3. Necesidad de claridad conceptual sobre OSINT*

Sin perjuicio de estos múltiples usos de OSINT, como se adelantó en la introducción, en este trabajo abordaremos OSINT como la recolección y el análisis de datos de fuentes accesibles públicamente –sean o no personales– siempre que esto

[9] Hassan y Hijazi, *supra* nota 7, p. 2.

[10] La traducción es propia. Los destacados no pertenecen al original. "NATO Open Source Intelligence Handbook", 2001, disponible en: https://archive.org/details/NATOOSINTHandbookV1.2, último acceso: 23 de agosto de 2023.

cuente con una determinada finalidad –no necesariamente vinculada con la vigilancia, la prevención de delitos, la investigación científica o académica u otra en particular–. En otras palabras, no cualquier recolección de datos de fuentes abiertas es OSINT. Por esta razón se sostiene que "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".[11] Esta aclaración parece necesaria porque muchas veces puede confundirse OSINT con una mera tarea de recolección de datos, sin un fin específico o predeterminado.

Una forma posible para demarcar el concepto de OSINT es entenderlo como un *output* al que se llega luego de un proceso de recolección específica de *inputs* o datos crudos de información existente: una vez recolectados, los *inputs* son analizados con el objetivo particular de brindar información nueva. Supongamos, por ejemplo, el siguiente caso hipotético. Un ministerio de salud solicita que el personal de un determinado departamento recolecte todos los datos disponibles en fuentes abiertas sobre personas que han sido tratadas con un determinado medicamento y sus resultados (esto constituiría el *input*). Obtenidos los datos, se procede a analizar si los resultados pueden estar vinculados con alguna franja etaria de las personas a las que se les suministraron esos tratamientos (lo que constituiría el *output*). Este es el momento en el que la práctica pasa de ser solamente una recolección de datos a convertirse en OSINT.

Como vimos en el ejemplo, la finalidad de OSINT puede involucrar alguna cuestión general, pero también puede involucrar conocer algo específico sobre una persona determinada. Ello puede ocurrir si, por ejemplo, previo a ofrecer un cargo a una persona a la directiva de una institución se recogen datos sobre esa persona en fuertes abiertas, se los analiza y se emite un resumen de lo encontrado a fin de entender si el candidato o la candidata tiene el perfil adecuado para el puesto.

Al mismo tiempo, debe mencionarse que, cuando mediante OSINT se recolecta información de las redes sociales en internet, esta práctica tiene una denominación diferente: "inteligencia de redes sociales" (o Social Media Intelligence –SOCMINT–, por sus siglas en inglés). SOCMINT puede darse mediante diferentes técnicas entre las que se incluyen la revisión manual del contenido publicado por usuarios y usuarias, búsquedas específicas (de usuarios y usuarias, grupos, hashtags, etc.). Puede involucrar, además, herramientas de *scraping* o cualquier otro software que extraiga información de sitios web.[12]

[11] ADC, *supra* nota 2, p. 5.

[12] ADC, *supra* nota 2, p. 7.

## *II.4. OSINT(ers)*

En virtud de que los sujetos que practican OSINT son múltiples y diversos, en este apartado destacaremos algunos casos a modo de ejemplo. Es posible separar a los actores que realizan OSINT en dos grupos. Por un lado, están aquellos que realizan OSINT de forma "esporádica". En este grupo se incluyen desde organizaciones de la sociedad civil y oficinas gubernamentales, hasta empresas del sector privado, sectores de investigación académica e individuos, pues –al seguir la definición de OSINT de este trabajo– esta alcanza a cualquier organismo o individuo que recolecte y analice datos de fuentes accesibles públicamente –sean o no personales– con una determinada finalidad.

Por el otro, están aquellos actores que se "dedican" a OSINT, en el sentido de que no podrían ejercer sus funciones o cumplir con sus objetivos de otra manera. Amerita profundizar sobre el alcance de este segundo grupo. ¿Quiénes lo componen? Aquí se incluyen agencias de inteligencia y fuerzas de seguridad, como también empresas del sector privado.

Con respecto a las agencias de inteligencia, las dos que se consideran más "tradicionales" en este campo globalmente por sus actividades de OSINT son el ya mencionado Open Source Enterprise que está dentro de la CIA de los Estados Unidos; y el BBC Monitoring[13] en el Reino Unido. Ambos organismos tienen roles y actividades similares, y realizan OSINT para cumplir con sus funciones.

Entre los departamentos dependientes de las fuerzas de seguridad encontramos a algunos que están dedicados exclusivamente a la recolección y al análisis de fuentes abiertas en internet, y redes sociales en particular. Es el caso, por ejemplo, de las áreas especializadas en tareas de vigilancia que, con el advenimiento de internet y la vida digital, llevan sus tareas al plano virtual. Veremos más adelante que replicar las tareas de vigilancia analógicas al plano virtual puede ser problemático tanto por aspectos jurídicos como éticos.

Dentro de las organizaciones que realizan OSINT en el sector privado, y que entrarían en la segunda categoría de actores, es posible mencionar, por ejemplo,

[13] En el sitio web de BBC Monitoring se indica lo siguiente: "Antes del estallido de la segunda guerra mundial, el Gobierno británico solicitó a la BBC que estableciera una organización para monitorear el uso de los medios por parte de las potencias del Eje, y especialmente el nuevo y poderoso medio: la radio. Durante los últimos 80 años, BBC Monitoring ha innovado y desarrollado, y ahora monitorea más de 3.000 fuentes en radio, televisión, prensa, en línea y redes sociales, en 100 idiomas. Nuestro propósito sigue siendo observar, comprender y explicar los medios del mundo para ayudar a nuestros usuarios a interpretar eventos clave" (la traducción es propia). BBC Monitoring, "What is BBC Monitoring?", disponible en: https://monitoring.bbc.co.uk/about, último acceso: 23 de agosto de 2023.

a Janes Information Group;[14] Economist Intelligence Unit;[15] Oxford Analytica;[16] Factiva[17] y Lexis Nexis.[18] En algunos casos estas organizaciones prestan servicios de OSINT a agencias gubernamentales, pero en muchos otros sus servicios son prestados a otros actores interesados en obtener información debidamente analizada, como pueden ser las organizaciones internacionales[19] que tercerizan o realizan directamente actividades de OSINT.

Al mismo tiempo, parte del sector privado, principalmente el sector de negocios, recurre a empresas que realizan OSINT tanto para la investigación de posibles nuevos mercados como para monitorear actividades de los competidores, entre otros fines. En el pasado, OSINT era requerido únicamente por grandes corporaciones, pero a medida que se abarataron los costos de recolección de datos e información gracias a internet, también pequeñas empresas recurren a proveedoras de servicios de OSINT con similares propósitos.

Para esta investigación, se entrevistó a empleados[20] de empresas que recurren a servicios de OSINT por parte de empresas de la segunda categoría. Señalaron las que más se utilizan: Pipl,[21] Spokeo[22] y Been Verified.[23] En síntesis, las tres empresas ofrecen poner a disposición de sus clientes un análisis de datos de personas en base a información disponible públicamente en internet. En general, para poder recopilar la información utilizan un software que "rastrea" la web en busca de nombres, ubicaciones, edades, hechos y cualquier otra información relevante.

---

[14] Ver Janes, "About Janes", disponible en: https://www.janes.com/about-janes/what-we-do, último acceso: 23 de agosto de 2023.

[15] Ver Economist Intelligence, "Global Insights and Market Intelligence", disponible en: https://www.eiu.com/n, último acceso: 23 de agosto de 2023.

[16] Ver Oxford Analytica, "Who We Are", disponible en: https://www.oxan.com/about/values, último acceso: 23 de agosto de 2023.

[17] Ver Dow Jones, "Factiva", disponible en: https://www.dowjones.com/professional/factiva, último acceso: 23 de agosto de 2023.

[18] Ver Lexis Nexis, disponible en: https://www.lexisnexis.com/en-us/home.page, último acceso: 23 de agosto de 2023. Hassan y Hijazi, *supra* nota 7, pp. 7-10.

[19] Es posible encontrar ejemplos de OSINT en organizaciones como la Cruz Roja, la Organización del Tratado del Atlántico Norte (OTAN), o la Organización para la Seguridad y Cooperación Europea, que incluso ofrece cursos de prácticas OSINT. Ver Organization for Security and Co-operation in Europe, "OSCE Organizes Training Course on Internet Investigations and Open Source Intelligence in Central Asia", 2021, disponible en: https://www.osce.org/secretariat/507764, último acceso: 23 de agosto de 2023.

[20] En todos los casos pidieron reserva de su identidad y de la empresa donde trabajaban.

[21] Ver Pipl, disponible en: https://pipl.com, último acceso: 23 de agosto de 2023.

[22] En su sitio web, Spokeo indica que "hemos organizado más de 12 mil millones de registros de miles de fuentes en informes fáciles de entender para que esté mejor informado sobre las personas que lo rodean. Simplemente ingrese un nombre, número de teléfono, correo electrónico o ubicación para buscar disponibles" (la traducción es propia). Ver Spokeo, disponible en: https://www.spokeo.com, último acceso: 23 de agosto de 2023.

[23] Ver Been Verified, disponible en: https://www.beenverified.com, último acceso: 23 de agosto de 2023.

Vale la pena destacar un ejemplo real: para esta investigación, se ingresó mi nombre y apellido en Spokeo. La información obtenida estaba totalmente desactualizada y se refería a información de teléfonos y domicilios cuando residía en Estados Unidos, hace casi más de 15 años. Para saber más información, el sitio ofrece una tarifa adicional. Sin perjuicio de que la información obtenida estaba desactualizada, evidentemente la búsqueda hizo posible arrojar algunos datos.

Resulta interesante la explicación dada en Spokeo sobre su "política de privacidad", donde detalla las diferentes categorías de información públicamente disponible que recopila, desde índices de consumidores, directorios telefónicos, registros de propiedad y registros judiciales (información que surge de registros públicos, en manos del Estado), hasta redes sociales.[24] Catalogan esa información como "información pública". La pregunta que surge es si ello es realmente así o es simplemente un recurso publicitario para justificar la práctica.[25]

## III. Estándares sobre privacidad en el Sistema Internacional de Derechos Humanos

Previo a profundizar en el análisis sobre los dilemas que trae OSINT, amerita hacer un breve repaso sobre los estándares mínimos de protección a la privacidad que establecen los tratados que protegen los derechos humanos. La protección a la privacidad está prevista tanto a nivel del Sistema Universal de Protección de los Derechos Humanos (SUDH) como del Sistema Interamericano de Protección a los Derechos Humanos (SIDH). Si bien el "derecho a la privacidad" no aparece mencionado de esta manera, de ello no se puede inferir que no sea un derecho humano fundamental previsto en los tratados.

A nivel universal, se destaca el artículo 12 de la Declaración Universal de Derechos Humanos (DUDH) y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), los que 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.

---

[24] Ver Spokeo, "Privacy Policy", disponible en: https://www.spokeo.com/privacy-policy, último acceso: 23 de agosto de 2023.

[25] En el sitio de Been Verified se provee una explicación sobre qué son los datos públicos que es absolutamente reveladora para esta investigación: "¿Recuerdas cuando te registraste para esa tarjeta de crédito gratis? ¿O esos reembolsos de teléfonos celulares y suscripciones a revistas? ¿O incluso multas por exceso de velocidad, escrituras de hipotecas, perfil de redes sociales y publicaciones en blogs? Todos revelan información sobre usted, que se conoce como registro público" (la traducción es propia). Been Verified, *supra* nota 24.

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, 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 público.[26] Los derechos incluidos en el artículo 11 no son derechos "absolutos": las injerencias sobre el derecho a la vida privada deben sujetarse a la aplicación del conocido test de proporcionalidad.[27]

En cuanto al eje que relaciona la protección de la vida privada con las comunicaciones, la CtIDH expresó que, aunque las conversaciones telefónicas no se encuentren expresamente previstas en el artículo 11 de la Convención, de todos modos son una forma de comunicación que, al igual que la correspondencia, se encuentra incluida dentro del ámbito de protección del derecho a la vida privada.[28]

En palabras de la Corte, "el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública. En este sentido, el domicilio y la vida privada [están] intrínsecamente ligados, ya que el domicilio se convierte en un espacio en el cual se puede desarrollar libremente la vida privada".[29] Nótese que, al interpretar este artículo, para la CtIDH es claro que la violación puede provenir tanto del Estado como de privados.

Es pertinente resaltar que, hasta el presente, la CtIDH ha abordado problemáticas relacionadas con la vida privada y la inviolabilidad del domicilio, la vida privada y la inviolabilidad de las comunicaciones, la vida privada y la sexualidad, y la vida privada y la autonomía reproductiva. No obstante, no ha resuelto ningún

---

[26] 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.

[27] En palabras de la CtIDH, "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". CtIDH, "Tristán Donoso vs. Panamá", sentencia del 27 de enero de 2009, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, Nº 193, § 56, disponible en: https://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=253, último acceso: 14 de agosto de 2023.

[28] *Ibíd*., § 55.

[29] CtIDH, "Caso de las Masacres de Ituango vs. Colombia", sentencia del 1º de julio de 2006, Serie C, Nº 148, §§ 193-194, disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_148_esp.pdf, último acceso: 23 de agosto de 2023.

caso que se refiera a la vulneración de datos personales con relación a la protección de la vida privada, ya sea en el mundo analógico o digital.[30]

Asimismo, vale la pena destacar la amplitud de la interpretación del concepto de "vida privada" que dio la CtIDH en su reciente sentencia del 4 de febrero de 2022 en el caso "Pavez Pavez vs. Chile". El tribunal estableció que la protección del derecho a la vida privada abarca factores que van más allá del derecho a la privacidad, como la dignidad, la capacidad de desarrollar una personalidad y la determinación de identidad, entre otros.[31] Por su lado, el Tribunal Europeo de Derechos Humanos (TEDH) en el caso "Peck vs. United Kingdom"[32] reconoció que hay una expectativa de privacidad incluso cuando las personas interactúan en espacios públicos.

Hasta aquí podemos ver cómo la protección del derecho a la privacidad está determinada en el ámbito de los sistemas universales y regionales de protección de los derechos humanos. También vemos que, por la amplitud que se da al concepto de "privacidad", la protección de los datos personales se encuentra incluida dentro de ella.

## IV. Dilemas conceptuales

De todo lo expresado hasta aquí podemos advertir que la técnica OSINT plantea diversos dilemas conceptuales. Principalmente, el término "fuente abierta" merece un análisis más detallado: ¿acaso todos los datos de libre acceso pueden ser "tratados"? Esta pregunta como disparadora nos obliga a analizar las dispo-

[30] Comentario de Carlos Zelada al art. 11, ver Andreu-Guzmán, Federico y otros, *Convención Americana sobre Derechos Humanos. Comentario*, Steiner, Christian y Fuchs, Marie (eds.), Berlín-Bogotá, Konrad Adenauer Stiftung, 2º ed., 2019, disponible en: https://www.corteidh.or.cr/tablas/34016.pdf, último acceso: 23 de agosto de 2023.

[31] "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, Serie C, Nº 449, disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_449_esp.pdf, último acceso: 14 de agosto de 2023.

[32] 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.

siciones de los marcos jurídicos de protección de datos personales, dado que la autorización para el tratamiento está inherentemente relacionada con el consentimiento otorgado para que esos datos sean accesibles libremente.

En lo que sigue examinaremos brevemente la idea de la expectativa (o no) de privacidad en internet de manera general y en las redes sociales en particular. Se analizarán cuáles son las características mínimas que debe tener el consentimiento otorgado para ser considerado válido, de acuerdo a ciertos estándares internacionales. Seguido a ello, se planteará un segundo dilema relacionado con el uso de OSINT por parte de las fuerzas de seguridad, utilizaremos el caso del "protocolo de ciberpatrullaje" en Argentina y, por último, se dedicará un apartado especial para la relación entre OSINT y el derecho a la libertad de expresión: se presentará que, si bien es problemático desde el punto de vista de la privacidad, OSINT es una herramienta clave para el ejercicio de este derecho en la búsqueda y el acceso a información.

### *IV.1. La recolección de datos y las "fuentes abiertas"*

Un caso interesante para analizar en esta investigación surge de lo que Facebook considera "información pública":

> Información que compartes que siempre es pública: algunos de los datos que nos proporcionas al completar tu perfil, como tu rango de edad, tu idioma y tu país, son públicos. También usamos una parte de tu perfil, que se denomina "perfil público", para ayudarte a conectarte con amigos y familiares. El perfil público incluye tu nombre, sexo, nombre de usuario e identificador de usuario (número de cuenta), foto del perfil y foto de portada. Esa información también es pública.[33]

Este ejemplo sirve para elucidar un primer dilema asociado a OSINT: los conceptos de "información pública" o "información privada" esconden cierta ambigüedad y pueden alcanzar datos de carácter tanto público como privado. En este sentido, existe información accesible en fuentes abiertas –incluso considerada "información pública" por Facebook–, que no es información "pública" en su naturaleza: pensemos, por ejemplo, en aquellos datos personales que consideramos importantes en nuestras vi-

[33] Facebook, "Información pública en Facebook", disponible en: https://www.facebook.com/help/203805466323736/?helpref=uf_share, último acceso: 23 de agosto de 2023.

das privadas, como puede ser nuestro número de teléfono. El hecho de que el número de teléfono esté disponible públicamente no lo convierte en información pública *per se*, por lo que su recolección puede implicar vulneraciones al derecho a la protección de datos personales y, consecuentemente, violaciones de la privacidad.

Ahora bien, un argumento en favor de la recolección de datos personales en redes sociales se funda en que los usuarios y las usuarias titulares de los datos aceptan los "términos y condiciones" de las plataformas y que esta aceptación transformaría esos datos en "datos públicos". En otras palabras, el argumento se sustenta en que se perdería cualquier expectativa de privacidad por el solo hecho de haber prestado consentimiento a los términos y condiciones de la plataforma, por lo que la recolección de esos datos no violaría ningún derecho. Esto es cuanto menos dudoso y presenta algunos matices.

Quizás la primera pregunta que debemos hacernos es cuánto conocen y cuánto controlan las personas los datos sobre ellas que se encuentran en las redes sociales. Según Leandro Ucciferri, la autodeterminación informativa –es decir, el control sobre estos datos en las redes sociales– no parece ser una cuestión simplemente voluntaria, sino que involucra diversos factores ajenos a la voluntariedad del o de la titular de los datos.[34] Esta autodeterminación se ve impactada, por ejemplo, por los "metadatos" (geolocalización, fecha, idioma, dispositivos utilizados, etc.); por publicaciones realizadas por terceros; e incluso por ciertas configuraciones sobre las reglas de privacidad de las plataformas (que suelen sufrir modificaciones constantes, no siempre protectoras por defecto). Estos factores exceden la capacidad de control y la voluntariedad por parte del o de la titular de los datos sobre el tratamiento de estos.[35] En otras palabras, los usuarios y las usuarias pueden consentir al tratamiento de sus datos según los términos y las condiciones de las plataformas sin conocer con precisión cuál es el alcance de esos tratamientos.

Estas ideas están íntimamente vinculadas al objeto de este trabajo. Como fue explicado antes, las empresas que ofrecen servicios OSINT muchas veces se jactan de hacer uso "legal" de los datos.[36] Algunas incluso se valen de contratos de

---

[34] ADC, *supra* nota 2, pp. 8-9.

[35] *Ibíd*., p. 8.

[36] En el sitio web de Pipl, por ejemplo, se indica que "siempre mantenemos altos estándares de ética y cumplimiento para garantizar que cumplimos con todas las leyes y reglamentaciones aplicables; independientemente del método de obtención de datos que utilicemos, mantenemos un registro de auditoría claro para cualquier dato agregado a nuestro servicio para garantizar que podamos realizar un seguimiento de la calidad de la fuente de datos, las licencias y los cambios normativos" (la traducción es propia). Ver Pipl, *supra* nota 22.

cesión y/o tratamiento de datos con distintas aplicaciones o plataformas para acceder a los datos de sus clientes, quienes previamente han consentido a la posible existencia de esos contratos.

Para determinar si ese consentimiento es suficiente para el tratamiento de datos mediante técnicas de OSINT debemos revisar aquellas regulaciones sobre privacidad y protección de datos que atienden detalladamente, como veremos a continuación, el modo en que debe prestarse el consentimiento. El único tratado internacional que da protección específica a los datos personales que, además, aborda la cuestión del consentimiento es el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108), un compromiso internacional que fue emitido por el Consejo de Europa en 1981 y que ha sido recientemente modernizado (Convenio 108+).[37] Las legislaciones de protección de datos de Latinoamérica siguen de cerca los estándares de este Convenio. El artículo 5º, inciso 2 del Convenio 108+ dice que cada Parte dispondrá que el tratamiento de datos pueda realizarse sobre la base del consentimiento libre, específico, informado e inequívoco del interesado o de alguna otra base legítima establecida por la ley.

En el ámbito interamericano merece destacarse la aprobación de los "Principios actualizados sobre la privacidad y la protección de datos personales" (principios OEA), en 2021.[38] Se trata de un conjunto de recomendaciones y de principios que, si bien no son vinculantes, podrían inspirar un futuro tratado o los marcos normativos nacionales de los diferentes países que integran la Organización de los Estados Americanos (OEA). El principio 2 establece que "cuando el procesamiento [de datos personales] se base en el consentimiento, los datos personales solamente deberían ser recopilados con el consentimiento previo, inequívoco, libre e informado de la persona a que se refieran".

El Reglamento General de Protección de Datos 2016/679 (RGPD)[39] de la Unión

[37] Ver el cuadro de firmas y ratificaciones del Convenio 108 en Council of Europe, "Chart of Signatures and Ratifications of Treaty 108", disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=O1ZGs4lK, último acceso: 23 de agosto de 2023.

[38] Ver Organización de los Estados Americanos (OEA), Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos, "Principios actualizados sobre la privacidad y la protección de datos personales", 2021, disponible en: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf, último acceso: 23 de agosto de 2023.

[39] Para un análisis más detallado de la relación entre el RGPD y el Convenio 108, así como de sus efectos en Latinoamérica, ver Bertoni, Eduardo, "Convention 108 and the GDPR: Trends and Perspectives in Latin America", en: *Computer Law & Security Review*, vol. 40, 2021, disponible en: https://www.sciencedirect.com/science/article/pii/S0267364920301217, último acceso: 23 de agosto de 2023.

Europea también se ocupa de la cuestión del consentimiento en el artículo 4º, apartado 11, donde se estipula que el consentimiento del interesado es toda manifestación de voluntad libre, específica, informada e inequívoca, por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

En ese marco, el European Data Protection Board (EDPB)[40] ha opinado que:

> el consentimiento es una herramienta que otorga a los interesados el control sobre si los datos personales que les conciernen van a ser tratados o no. Si no es así, el control del interesado será meramente ilusorio y el consentimiento no será una base jurídica válida para el tratamiento, lo que convertirá dicha actividad de tratamiento en una actividad ilícita.

Según la opinión del EDPB, el término "libre" implica la elección y el control real por parte de los interesados. A su vez, el artículo 7º, apartado 4 del RGPD indica que, a los fines de evaluar si el consentimiento es libre, se debe tener en cuenta si la ejecución del contrato, incluida la prestación de un servicio, está condicionada al consentimiento para el tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Resultan interesantes, por el paralelo que puede hacerse cuando se utiliza OSINT, los casos donde el EDPB ha entendido que no puede considerarse que el o la titular de los datos personales ha dado su consentimiento para el tratamiento por terceras partes. Así ha opinado en casos donde un banco requiere de sus clientes el consentimiento para que terceros puedan utilizar sus datos con fines de marketing, cuando esa utilización no es una actividad necesaria para la ejecución del contrato ni para la prestación de servicios entre el banco y el cliente. Si ante la negativa el banco procede al cierre de la cuenta o al aumento en comisiones, entonces el consentimiento no podría haberse dado libremente. En otro ejemplo, una empresa solicita de sus clientes el consentimiento para utilizar sus datos a fin de enviarles publicidad por correo electrónico y para compartir sus datos con otras empresas de su grupo. El problema aquí, para el EDPB, es la falta de granularidad o especificidad del consentimiento: si no es posible consentir por separado a dos fines diferentes, el consentimiento será inválido. Por último, otro

[40] Ver European Data Protection Board (EDPB), "Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679", 2020, disponible en: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_es, último acceso: 23 de agosto de 2023.

ejemplo interesante dado por el EDPB se da cuando una compañía de televisión utiliza los datos de sus abonados, con su consentimiento, para realizar recomendaciones personales de películas nuevas basadas en sus intereses. Si la compañía desea permitir que terceros puedan mostrar publicidad específica, basada en los hábitos de los abonados, se deberá obtener un nuevo consentimiento específico para esta nueva finalidad.

Estos ejemplos son extremadamente útiles a la hora de analizar si la forma en que se solicita el consentimiento en algunas plataformas –de donde se recogen datos mediante técnicas OSINT– es válida para su posterior recolección vía OSINT o si, por el contrario, debe considerarse que el consentimiento sobre los términos de las plataformas no alcanza para justificar la legalidad en la recolección y el tratamiento de datos vía OSINT por terceros, con otros fines.

Con esto queda claro, entonces, que la expectativa de privacidad en redes sociales no puede ni debe estar solamente vinculada con la aceptación de las condiciones de uso de una determinada plataforma, sino que se relaciona, además, con el conocimiento que se tiene sobre el funcionamiento de esa plataforma: principalmente, qué datos esconde detrás de aquellos otorgados por los usuarios y las usuarias, a quiénes se los comparte y para qué fines. Para que el conocimiento sea informado, las plataformas deben explicar con mucha claridad su funcionamiento y alcance de los tratamientos de datos personales.

Si a ello sumamos que OSINT se caracteriza por ser una recolección pasiva o semipasiva de datos a efectos que el o la titular de datos personales no advierta su recolección, surge la incógnita de si la creación de una identificación falsa para recolectar los datos torna inválido el consentimiento dado por el o la titular de los datos al aceptar la política de privacidad de la plataforma que sea. Esta reflexión tiene sentido en tanto se considere que el otorgamiento del consentimiento de la manera que se solicita en la política de privacidad es un mecanismo válido. De no ser así, cualquier operación de OSINT quedaría severamente cuestionada porque estaría vulnerando el derecho a la privacidad de todos aquellos sobre los que se recolectan datos personales.

Si bien en muchos casos el consentimiento dado para el tratamiento de datos puede incluso ser válido para técnicas OSINT, esto no quita que –sin perjuicio de su licitud– la privacidad de la persona sufra alguna vulneración. La robustez de la regulación en materia de privacidad y protección de datos es una pieza clave en esta problemática, pues determina la capacidad en la que los usuarios y las

usuarias pueden administrar sus datos en línea y la forma en la que el consentimiento debe darse para ser considerado válido. En este sentido, ciertos autores argumentan a favor de una regulación que vaya "más allá de una mayor autogestión de la privacidad"[41] de los sujetos cuando utilizan plataformas: una regulación centrada en la arquitectura, que por defecto considere inadmisible ciertos tipos de transferencias de datos personales, o que prohíba diseños de productos o servicios capaces de causar daños, por ejemplo.

Como conclusión provisoria puede resumirse, entonces, que la práctica OSINT puede ser ilícita o lícita según diversos factores. Por un lado, no toda información disponible en fuentes abiertas puede ser objeto de tratamiento por terceros. De esta forma, el uso de técnicas OSINT puede vulnerar la protección de datos personales si el consentimiento dado originalmente por los o las titulares de los datos no necesariamente alcanza para justificar su tratamiento por quien realiza OSINT: esta actividad sería ilícita conforme a la regulación de privacidad o la protección de datos personales. Por el contrario, si el consentimiento dado originalmente incluye, además, consentir al tratamiento de los datos vía OSINT, entonces esta actividad sería considerada lícita.

De cualquier forma, aun si es a través de prácticas lícitas, el uso de OSINT puede conllevar a posibles intromisiones de la privacidad ya no desde un punto de vista jurídico –si, como vimos, la práctica se realiza lícitamente–, sino desde un punto de vista ético. Una propuesta, desde el punto de vista jurídico, para superar esto se encuentra en la revisión de los marcos jurídicos de protección a la privacidad a fin de actualizarlos con un enfoque integral, que vaya más allá de la autogestión del individuo. Además de ello, estas leyes deberían regular con mejor atención cómo deben relacionarse las compañías que intercambian datos personales.

### *IV.2. El caso argentino del "protocolo de ciberpatrullaje"*

El segundo dilema se presenta cuando los organismos que realizan OSINT o utilizan servicios de OSINT están vinculados a las fuerzas de seguridad de un Estado. Un caso paradigmático para mencionar es el del "Protocolo general para la

[41] Ver Solove, Daniel J., "The Myth of the Privacy Paradox", en: *The George Washington Law Review*, vol. 89, Nº 1, 2021. Solove deconstruye y critica la "paradoja de la privacidad", el fenómeno en el que las personas dicen que valoran mucho la privacidad, pero en su comportamiento ceden sus datos personales por muy poco a cambio o no toman medidas para proteger su privacidad.

prevención policial del delito con uso de fuentes digitales abiertas"[42] (en adelante, el Protocolo) aprobado en 2020 por el Ministerio de Seguridad de la Nación, en Argentina. Tal como se explica en una nota de la Agencia de Acceso a la Información Pública (AAIP) de ese país, se trata de un protocolo que establece las directrices para las "tareas de prevención del delito que desarrollan en el espacio cibernético los cuerpos policiales y fuerzas de seguridad" dependientes de dicho ministerio.[43] Cabe destacarse que este Protocolo, conocido como el "protocolo de ciberpatrullaje" está expresamente asociado a OSINT al indicar que el ámbito de aplicación de las tareas de prevención a las que se refiere:

> será únicamente a través de "fuentes digitales abiertas" definidas como 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.[44]

Las fuerzas de seguridad están habilitadas, a raíz de este Protocolo, a recabar información en lo que consideran "fuentes abiertas", analizar esa información y todo ello con fines de prevención del delito. Para la AAIP, de acuerdo a lo que surge del Protocolo, podría interpretarse que sus operaciones de tratamiento de datos personales se efectúan bajo las bases legales de los apartados a) y b) del artículo 5º, inciso 2 la Ley Nº 25.326 de Protección de Datos Personales en Argentina, que establecen, respectivamente, que "no será necesario el consentimiento [del o de la titular de los datos] cuando: a) los datos se obtengan de fuentes de acceso público irrestricto; b) se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".

Establecida la base legal del tratamiento de datos por parte de las fuerzas de seguridad, la AAIP aclaró que aun cuando un dato personal se encuentre en una

---

[42] Ver 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: 9 de agosto de 2023.

[43] Ver República de Argentina, Poder Ejecutivo Nacional, "Protocolo general para la prevención policial del delito con uso de fuentes digitales abiertas", respuesta a nota NO-2020-41096462-APN-UGA-MSG, 2020, disponible en: https://www.argentina.gob.ar/sites/default/files/no-2020-47326285-apn-aaip.pdf, último acceso: 24 de agosto de 2023. El Protocolo mantiene su vigencia durante el plazo de la emergencia pública en materia sanitaria, establecida por ley Nº 27.541 y el decreto DNU Nº 260/2020.

[44] *Ibíd*., art. 2º.

fuente digital abierta, o una fuente de acceso público irrestricto, ello no implica de ninguna manera que quien trate ese dato no deba cumplir con los restantes principios y obligaciones que se establecen por ley; entre ellos, el principio de calidad del dato, principio de información, los principios de seguridad y confidencialidad, entre otros. Esta aclaración es relevante porque podría concluirse que esos principios también los deben cumplir quienes realizan operaciones similares en el sector privado como las que se mencionaron antes, más allá de que se asuma que esas operaciones se hacen con consentimiento y en fuentes abiertas.

El principal dilema sobre este Protocolo radica en que se utilice OSINT para fines de vigilancia o inteligencia criminal a escala sobre la población y que, en consecuencia, se desvirtúen los estándares sobre la mínima sospecha razonable que justifican la intervención punitiva del Estado.[45] En este sentido, la AAIP consideró que, atenta a que lo que se preveía en el Protocolo podía llevar a un tratamiento de datos personales a gran escala, se podría llevar a cabo una evaluación de impacto en materia de datos personales en la que: i) se detalle exhaustivamente el funcionamiento del Protocolo; ii) se identifiquen los riesgos para la privacidad de las personas; y iii) se explique qué salvaguardas se emplearán para mitigar dichos riesgos.

Explicado de otra manera: en el ámbito "analógico" y específicamente vinculado con las técnicas aceptadas de investigación o prevención de delitos, la figura del "agente provocador" ha sido cuestionada desde puntos de vista éticos.[46] ¿Es ético que el aparato estatal "engañe" a una persona aun para obtener un fin legítimo? Las aguas están divididas en este aspecto, pero la base de la discusión es similar a la que puede plantearse con las prácticas OSINT, cuando es el Estado quien las utiliza y cuando, como vimos, el o la titular de los datos personales que se recolectan no lo sabe.

---

[45] Ver Monte y Sánchez, *supra* nota 6. Además, Amnistía Internacional también manifestó preocupación por la utilización de "fuentes abiertas" por parte de las fuerzas de seguridad. En palabras del comunicado de prensa de esa ONG del 3 de junio de 2020, "la guía aprobada aún autoriza a las fuerzas de seguridad a realizar actividades de investigación preliminar o prevención de delitos en lugar de restringirlas a casos en los que existe un marco judicial aplicable a una investigación concreta. Este tipo de actividad generalizada de vigilancia puede afectar el derecho a la privacidad y a la libertad de expresión. Por esta razón, la investigación en fuentes abiertas debería aplicarse en situaciones muy excepcionales, con el debido marco legal, y con un amplio debate parlamentario con participación social". Amnistía Internacional, "Ministerio de Seguridad aprobó el protocolo que regula la vigencia en internet", 2020, disponible en: https://amnistia.org.ar/el-ministerio-de-seguridad-aprobo-protocolo-que-regula-la-vigilancia-en-internet, último acceso: 24 de agosto de 2023.

[46] Maximiliano Rusconi, al abordar el tema del "agente provocador" desde la perspectiva de la dogmática penal, reconoce que "la necesidad, conveniencia político-criminal, solvencia *ética,* (…) son cuestiones muy poco claras". Aun reconociendo el dilema *ético,* este autor se muestra a favor de esta figura: "Desde el punto de vista *ético* es posible sostener que, más allá de algunas fórmulas especialmente criticables que han generado el rechazo justificado de la doctrina, no parece inapropiado otorgarle al sistema estatal de investigación las posibilidades de una actuación inteligente en la búsqueda sobre la información del supuesto de hecho". Rusconi, Maximiliano, *Derecho Penal. Parte general*, Buenos Aires, Ad-Hoc, 3º ed. actualizada y ampliada, 2016, pp. 886-891.

Si bien en este caso parece existir un fundamento legal para realizar estas actividades, aparece un cuestionamiento de tipo ético que alcanza incluso a las actividades de OSINT que son tercerizadas por los Estados (cuando no es el Estado quien realiza OSINT, sino que contrata a empresas privadas para realizar lo que no puede realizar por falta de recursos técnicos o humanos debidamente capacitados). Un cuestionamiento similar, aunque de menor intensidad, puede hacerse cuando se trata de cuestiones entre particulares, y cuando las prácticas OSINT tienen como *output* fines simplemente comerciales. La intensidad más baja de cuestionamientos éticos pueden estar vinculados a las puesta en práctica de técnicas OSINT por investigadores académicos, donde el *output* comprende información agregada o anonimizada y carece de impacto en el o la titular de los datos.

### *IV.3. OSINT y la libertad de expresión*

Internet brinda la posibilidad de almacenar y acceder a enormes cantidades de datos –públicos y privados– mediante una búsqueda relativamente sencilla. Por ello es posible argumentar que OSINT es una herramienta que contribuye al ejercicio del derecho de la libertad de expresión: buscar, acceder y conocer información permite que las personas puedan formarse de opinión y participar de los debates más valiosos para la vida democrática. Sin embargo, la relación de OSINT con este derecho tiene claroscuros: las ventajas de acceso a la información pueden ser directamente proporcionales al impacto negativo que OSINT provoca para la privacidad, como vimos en el apartado anterior. Sumado a esto, perder toda expectativa de privacidad tiene un impacto directo –aunque no necesariamente deseado– en la libertad de expresión al provocar el *chilling effect*. En palabras de Ucciferri:

> Las personas ajustan o modifican su comportamiento cuando saben o sienten, aun en una remota posibilidad, que están siendo observadas y juzgadas. El uso de técnicas de SOCMINT alimenta un efecto inhibitorio, *chilling effect* en el derecho anglosajón, sobre la expresión de las personas en internet, llevando en muchos casos al ajuste incremental de sus propios niveles de autocensura.[47]

[47] ADC, *supra* nota 2, p. 10.

En esta sección, corresponde identificar primero cuáles son los estándares que garantizan el ejercicio de la libertad de expresión y el acceso a la información, para luego describir cómo ello se relaciona con OSINT. El derecho a la libertad de expresión se encuentra garantizado a nivel universal por el artículo 19 de la Declaración Universal de Derechos Humanos (DUDH) y el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP); y a nivel regional por el artículo 13 de la Convención Americana sobre Derechos Humanos (CADH).

Merece destacarse que a nivel universal el Comité de Derechos Humanos de las Naciones Unidas (CCPR, por sus siglas en inglés), órgano que monitorea la implementación del PIDCP, interpretó los estándares mínimos que emanan del artículo 19 del tratado en la observación general Nº 34.[48] Allí, el Comité se preocupó por aclarar que el artículo 19 del Pacto protege todas las formas de expresión y los medios para su difusión, entre ellos los modos de expresión electrónicos o de internet.

En el ámbito del Sistema Interamericano de Protección de los Derechos Humanos (SIDH), vale la pena remarcar la opinión consultiva Nº 5 de 1985[49] y los casos de la CtIDH que tratan sobre el artículo 13 de la CADH (entre ellos, La Última Tentación de Cristo (Olmedo Bustos y otros),[50] Ivcher Bronstein,[51] Herrera Ulloa,[52] Ricardo Canese,[53] Palamara Iribarne,[54] Claude Reyes y otros,[55] Kimel,[56]

[48] Véase en Organización de las Naciones Unidas (ONU), Pacto Internacional de Derechos Civiles y Políticos, Comité de Derechos Humanos, "Artículo 19. Libertad de opinión y libertad de expresión", observación general Nº 34, CCPR/C/GC/34, 12 de septiembre de 2011, disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/453/34/PDF/G1145334.pdf, último acceso: 24 de agosto de 2023. En adelante "observación general Nº 34".

[49] "La comparación hecha entre el artículo 13 y las disposiciones relevantes de la Convención Europea (artículo 10) y del Pacto (artículo 19) demuestra claramente que las garantías de la libertad de expresión contenidas en la Convención Americana fueron diseñadas para ser las más generosas y para reducir al mínimo las restricciones a la libre circulación de las ideas". CtIDH, "La colegiación obligatoria de periodistas. Arts. 13 y 29 Convención Americana sobre Derechos Humanos", opinión consultiva OC-5/85, 13 de noviembre de 1985, Serie A, Nº 5, §50, disponible en: https://www.corteidh.or.cr/docs/opiniones/seriea_05_esp.pdf, último acceso: 24 de agosto de 2023.

[50] CtIDH, "La *Última* Tentación de Cristo (Olmedo Bustos y otros) vs. Chile", sentencia del 5 de febrero de 2001, Fondo, Reparaciones y Costas, Serie C, Nº 73.

[51] CtIDH, "Ivcher Bronstein vs. Perú", sentencia del 6 de febrero de 2001, Reparaciones y Costas, Serie C, Nº 74.

[52] CtIDH, "Herrera Ulloa vs. Costa Rica", sentencia del 2 de julio de 2004, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, Nº 107.

[53] CtIDH, "Ricardo Canese vs. Paraguay", sentencia del 31 de agosto de 2004, Fondo, Reparaciones y Costas, Serie C, Nº 111.

[54] CtIDH, "Palamara Iribarne vs. Chile", sentencia del 22 de noviembre de 2005, Fondo, Reparaciones y Costas, Serie C, Nº 135.

[55] CtIDH, "Claude Reyes y otros", sentencia del 19 de septiembre de 2006, Fondo, Reparaciones y Costas, Serie C, Nº 151.

[56] CtIDH, "Kimel vs. Argentina", sentencia del 2 de mayo de 2008, Fondo, Reparaciones y Costas, Serie C, Nº 177.

Tristán Donoso,[57] Ríos y otros,[58] Perozo y otros[59], Usón Ramírez,[60] Gomes Lund y otros[61] y Fontevecchia y D'Amico).[62] Es preciso destacar que ninguna de estas decisiones ha tenido como base hechos relacionados con el ejercicio de la libertad de expresión en internet o su vinculación con una posible "autocensura" como consecuencia de la pérdida de expectativa de privacidad en la red.[63]

De todos modos, la jurisprudencia vigente tiene impacto en el ejercicio de la libertad de expresión en, al menos, tres ejes: 1) la prohibición de la censura previa; 2) el derecho de acceso a la información; y 3) la imposición de responsabilidades ulteriores. Estos temas se encuentran atravesados por tres criterios interpretativos generales que son relevantes destacar: el valor democrático de la libertad de expresión,[64] su aspecto dual[65] y el "test tripartito" a la hora de analizar las restricciones.[66]

---

[57] CtIDH, *supra* nota 28.

[58] CtIDH, "Ríos y otros vs. Venezuela", sentencia del 28 de enero de 2009, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, Nº 194.

[59] CtIDH, "Perozo y otros vs. Venezuela", sentencia del 28 de enero de 2009, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, Nº 195.

[60] CtIDH, "Usón Ramírez vs. Venezuela", sentencia del 20 de noviembre de 2009, Excepción Preliminar, Fondo, Reparaciones y Costas, Serie C, Nº 207.

[61] CtIDH, "Gomes Lund y otros ("Guerrilha do Araguaia") vs. Brasil", sentencia del 24 de noviembre de 2010, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, Nº 219.

[62] CtIDH, *supra* nota 27.

[63] Entre otros casos se incluyen: CtIDH, "Vélez Restrepo y familiares vs. Colombia", sentencia del 3 de septiembre de 2012, Excepción Preliminar, Fondo, Reparaciones y Costas, Serie C, Nº 248; CtIDH, "Uzcátegui y otros vs. Venezuela", sentencia del 3 de septiembre de 2012, Fondo y Reparaciones, Serie C, Nº 249; CtIDH, "Mémoli vs. Argentina", sentencia del 22 de agosto de 2013, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, Nº 265; CtIDH, "Norín Catrimán y otros (dirigentes, miembros y activistas del pueblo indígena mapuche) vs. Chile", sentencia del 29 de mayo de 2014, Fondo, Reparaciones y Costas, Serie C, Nº 279; CtIDH, "López Lone y otros vs. Honduras", sentencia del 5 de octubre de 2015, Excepción Preliminar, Fondo, Reparaciones y Costas, Serie C, Nº 302; CtIDH, "Granier y otros (Radio Caracas Televisión) vs. Venezuela", sentencia del 22 de junio de 2015, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, Nº 293; CtIDH, "Palacio Urrutia y otros vs. Ecuador", sentencia del 24 de noviembre de 2021, Fondo, Reparaciones y Costas, Serie C, Nº 446; y CtIDH, "Pueblos indígenas maya kaqchikel de Sumpango y otros vs. Guatemala", sentencia del 6 de octubre de 2021, Fondo, Reparaciones y Costas, Serie C, Nº 440.

[64] En palabras de la CtIDH: "La libertad de expresión es una piedra angular en la existencia misma de una sociedad democrática. Es indispensable para la formación de la opinión pública (…). Es, en fin, condición para que la comunidad, a la hora de ejercer sus opciones, esté suficientemente informada. Por ende, es posible afirmar que una sociedad que no esté bien informada, no es plenamente libre". CtIDH, *supra* nota 50, § 70.

[65] En palabras de la CtIDH, el derecho a la libertad de expresión "requiere que nadie sea arbitrariamente menoscabado o impedido de manifestar su propio pensamiento y representa, por tanto, un derecho de cada individuo; pero implica también, por otro lado, un derecho colectivo a recibir cualquier información y a conocer la expresión del pensamiento ajeno". *Ibíd*., § 30.

[66] La CtIDH en sus decisiones ha mencionado este test y entiende que "la legalidad de las restricciones a la libertad de expresión, fundadas sobre el artículo 13.2, dependerá de que estén orientadas a satisfacer un interés público imperativo. Entre varias opciones para alcanzar ese objetivo debe escogerse aquella que restrinja en menor escala el derecho protegido. Dado este estándar, no es suficiente que se demuestre, por ejemplo, que la ley cumple un propósito útil u oportuno; para que sean compatibles con la Convención las restricciones deben justificarse según objetivos colectivos que, por su importancia, preponderen claramente sobre la necesidad social del pleno goce del derecho que el artículo 13 garantiza y no limiten más de lo estrictamente necesario el derecho proclamado en el artículo 13. Es decir, la restricción debe ser proporcionada al interés

Veamos ahora unas breves anotaciones sobre la relación entre el acceso a internet como herramienta fundamental para el ejercicio de la libertad de expresión y el acceso a la información en un sentido amplio. Esta relación es evidente y así lo han dejado saber los organismos internacionales de promoción y protección de derechos humanos que hemos citado.

En la relación entre internet y libertad de expresión es importante destacar el rol de esta tecnología en la difusión masiva de expresiones que, antes, solo era posible de manera individual y mediante el "boca en boca". El uso de esta tecnología hace que sea muy económico llegar con nuestras expresiones a miles o millones de personas y que, incluso, no necesitemos de los medios de comunicación que supieron ser el paradigma de la libertad de expresión, como la prensa, la radio y la televisión. El valor que hoy tiene internet en nuestras vidas es tal que, sin su acceso, es imposible ejercer adecuadamente la libertad de expresión.

También merece mayor atención el hecho de que las prácticas OSINT parecen estar inherentemente relacionadas con el derecho a "buscar" información, y no solo con el derecho de "acceso" a la misma. El PIDCP en su artículo 19.2 dispone que "toda persona tiene derecho a la libertad de expresión; este derecho 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".[67] La CADH en su artículo 13, por su parte, también aclara que el derecho a la libertad de expresión 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".[68]

Sin dudas hace falta un estudio en profundidad de OSINT para entender las implicancias (positivas y negativas) que estas prácticas pueden tener sobre este derecho. Sumado a ello, el derecho de acceso a la información "pública" en manos del Estado está claramente garantizado a partir de la interpretación del artículo 13 de la CADH que hizo la CtIDH en los casos "Claude Reyes y otros vs. Chile", y

---

que la justifica y ajustarse estrechamente al logro de ese legítimo objetivo". *Ibíd*., § 42. También este test surge en el Sistema Universal de Protección de los Derechos Humanos, por ejemplo, en el informe del Relator Especial sobre la "Promoción y la protección del derecho a la libertad de opinión y de expresión" de la ONU de 2011. Ver ONU, Asamblea General, "Promoción y protección del derecho a la libertad de opinión y de expresión", A/66/290, 10 de agosto de 2011, § 15, disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/449/81/PDF/N1144981.pdf, último acceso: 14 de agosto de 2023.

67 El destacado no pertenece al original.

68 *Ibíd*.

"Gomes Lund y otros ("Guerrilha do Araguaia") vs. Brasil", mencionados antes. La CtIDH afirmó que:

> el artículo 13 de la C[ADH], al estipular expresamente los derechos a "buscar" y a "recibir" "informaciones", protege el derecho que tiene toda persona a solicitar el acceso a la información bajo el control del Estado, con las salvedades permitidas bajo el régimen de restricciones de la Convención. Consecuentemente, dicho artículo ampara el derecho de las personas a recibir dicha información y la obligación positiva del Estado de suministrarla, de forma tal que la persona pueda tener acceso a conocer esa información o reciba una respuesta fundamentada cuando por algún motivo permitido por la Convención el Estado pueda limitar el acceso a la misma para el caso concreto.[69]

La CtIDH no solo interpretó que el acceso a la información pública es un derecho garantizado por la Convención, sino que destacó que no se requiere acreditación de un interés directo para la obtención de la información. También recalcó la relevancia del "principio de máxima divulgación", que establece la presunción de que toda información pública es accesible, sujeto a un sistema restringido de excepciones previamente fijadas por ley: toda limitación que impida a los ciudadanos y las ciudadanas ejercer su derecho de acceso a la información pública debe sujetarse a un control en el marco del test tripartito.

Una cuestión que repetidamente se debate en los ámbitos que favorecen el acceso a la información pública se vincula con la excepción a ese derecho en caso de que el acceso a datos personales implique la vulneración del derecho a la privacidad. En este sentido, resulta importante dar algunas pautas de lo que las leyes de acceso a la información pública entienden que incluye y no incluye la información pública, y luego describir cómo se determina la excepción. Utilizaremos como fuente la Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública (Ley 2.0),[70] aunque aclaramos que este ejercicio explicativo podría hacerse con muchas de las leyes de acceso a la información pública que están vigentes en la región y que siguen lo expresado por la Ley 2.0.

---

[69] CtIDH, *supra* nota 56, § 77.

[70] Ver OEA, "Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública", 2020, disponible en: http://www.oas.org/es/sla/ddi/docs/publicacion_Ley_Modelo_Interamericana_2_0_sobre_Acceso_Informacion_Publica.pdf, último acceso: 23 de agosto de 2023.

Para la Ley 2.0, "información" (pública) es todo dato que esté en custodia o control de una autoridad pública, partido político, gremio y organización sin fines de lucro, mientras que "información personal" se refiere a aquella "relacionada a una persona viva y a través de la cual esa persona puede ser identificada".[71] Se aclara que la ley aplica a las:

> organizaciones privadas, partidos políticos o movimientos de esa índole, gremios, sindicatos y organizaciones sin fines de lucro (incluidas las organizaciones de la sociedad civil), las cuales deberán responder a las solicitudes de información con respecto a los fondos o beneficios públicos recibidos o a las funciones o servicios públicos desempeñados.[72]

En su artículo 32, la Ley 2.0 determina que, como excepción, los sujetos podrán denegar el acceso a la información pública si la divulgación puede dañar intereses privados, entre ellos "a) el derecho a la privacidad, incluyendo privacidad relacionada a la vida, la salud o la seguridad, así como el derecho al honor y la propia imagen;" y "b) los datos personales cuya difusión requiera el consentimiento de sus titulares". El artículo aclara que las excepciones no aplican cuando:

a) el individuo haya consentido expresamente la divulgación de sus datos personales;

b) las circunstancias del caso muestren con claridad que la información fue entregada al sujeto obligado como parte de aquella información que debe estar sujeta al régimen de publicidad;

c) la información se encuentre en registros públicos o fuentes de acceso público;

d) la información tenga el carácter de pública de acuerdo con la presente ley.[73]

Los sujetos obligados tampoco podrán negarse en caso de que exista supremacía del interés público en acceder a esa información, y en caso de violaciones graves de derechos humanos o delitos contra la humanidad.[74]

Ahora, imaginemos que una persona realiza una solicitud de acceso a la informa-

[71] *Ibíd*., art. 1.g y 1.h.

[72] *Ibíd*., art. 3.1.

[73] *Ibíd*., art. 32.2.

[74] *Ibíd*., arts. 26 y 27.

ción pública ante un sujeto obligado a darla, que esa información se encuentra en una base de datos de acceso restringido –a la que no accede cualquiera– y que el pedido incluye información personal que debe entregarse –por ejemplo, porque se asume que el o la titular de los datos dio su consentimiento expreso o porque se trata de información que ya está en un registro de acceso público–. Si por aplicación de los principios establecidos en la regulación los datos personales deben divulgarse, entonces, existe una paradoja relacionada con las prácticas OSINT. Como vimos más arriba, OSINT puede implicar vulneraciones a la privacidad, pero, al mismo tiempo, los principios y los estándares de acceso a la información protegen la divulgación de esos datos. En consecuencia, puede advertirse que no es muy relevante dónde o cómo se encuentra la información: lo relevante es que, aun siendo información privada, existen autorizaciones legales para darla.

OSINT, como vimos, puede implicar la recolección de datos personales que provengan de fuentes abiertas en manos del Estado (por ejemplo, información que surge de registros públicos). ¿Podríamos negar esa recolección para su tratamiento por OSINT, en casos de datos personales que las leyes de acceso a la información pública obligan a los Estados a entregarlos? Una respuesta que rechace el acceso a esos datos mediante prácticas OSINT parecería contradictoria con lo que estipulan las propias leyes de acceso a la información pública. Y allí está la paradoja.

A este argumento hay que agregarle un componente fundamental: en las solicitudes de acceso a la información pública existe un sujeto obligado que determina la validez del pedido y, de ser pertinente, la aplicación de una excepción. Los sujetos obligados y órganos creados para garantizar el acceso a la información pública se ocupan de resolver esta posible contradicción. En OSINT, en cambio, esto puede no ocurrir: nadie resuelve esa contradicción, lo que conduce a un problema de compleja solución. En consecuencia, desde un punto de vista conceptual, parecería que OSINT se lleva "mal" con la protección de datos, pero se lleva "bien" con el derecho a buscar y acceder a información.

## V. Conclusión

Esta investigación busca dar una primera aproximación al marco jurídico aplicable a OSINT, con todas las complejidades alcanzadas por esta práctica: el carácter polisémico del concepto, las implicancias detrás de "fuentes abiertas" e "inteligencia", y las consecuencias para con el derecho a la privacidad y el derecho a la

libertad de expresión y acceso a la información. Vimos que quienes se dedican a OSINT pueden ser tanto organizaciones u oficinas gubernamentales, empresas del sector privado, centros de investigación académica o individuos, con fines variados. También se advierte con preocupación el uso de OSINT por parte de las fuerzas de seguridad con fines de vigilancia y la falta de límites claros en estas actividades, capaces de afectar garantías constitucionales básicas.

La investigación arroja múltiples conclusiones preliminares, sobre las que se sugiere un estudio adicional que profundice el impacto que OSINT tiene sobre los derechos fundamentales. Entre las conclusiones se destacan las siguientes:

1. 1. No toda recolección de datos de fuentes abiertas es OSINT. Las prácticas OSINT deben entenderse como un *output* al que se llega luego de un proceso de recolección específica de datos crudos o de información existente –los *inputs*– que, además, luego son debidamente analizados con el objetivo de brindar información con un objetivo específico.

2. Es necesario tener presente la ambigüedad en los alcances de "información pública" e "información privada", ya que dentro de cada uno de estos niveles también pueden encontrarse datos de carácter tanto público como privado. En este sentido, no toda información disponible en fuentes abiertas puede ser objeto de tratamiento en el marco de las regulaciones de protección de datos personales.

   La licitud de la práctica OSINT está relacionada con el consentimiento que pudo haber otorgado el o la titular de los datos para que esos datos puedan ser de libre acceso y tratamiento. La práctica OSINT no se lleva bien con la protección de los datos personales desde distintas perspectivas: o bien se puede afirmar que no hay consentimiento del o de la titular para tratar sus datos porque la forma del consentimiento requerido no es válida; o bien se puede sostener que, aun siendo válida esa forma de otorgamiento de consentimiento, de ninguna manera puede aplicarse que los datos personales sean tratados por distintos actores con diferentes finalidades; o bien, finalmente, aun sorteando las dos cuestiones anteriores, puede afirmarse que debería hacerse una distinción de los datos que existen en fuentes públicas o semipúblicas porque la fuente no es lo importante, sino el tipo de datos que se trata.

3. Negar las prácticas OSINT bajo el argumento de una vulneración a la privacidad puede ser problemático a la luz del ejercicio de otro derecho fundamental: el de la libertad de expresión y acceso a la información. En consecuencia,

se argumenta que existe una paradoja asociada con OSINT: por un lado, es posible que se vulnere la privacidad al acceder a datos personales, mientras que, por el otro, los principios y las disposiciones internacionales en materia de acceso a la información exigen conocer y/o divulgar los mismos.

Es difícil afirmar de manera contundente que esas prácticas vulneran los derechos humanos en todos los casos, pero aún más complejo es afirmar que ello no sucede. Las perspectivas del análisis de las prácticas OSINT demuestran que la complejidad de la temática impide sostener posiciones claras en cuanto al impacto en los derechos humanos.

4. Por último, es necesario realizar una futura investigación que analice en profundidad el impacto de OSINT en los derechos humanos. Allí debe profundizarse el debate sobre las limitaciones ya no jurídicas, sino éticas, cuando OSINT sea practicado por actores privados o por actores públicos, especialmente por las fuerzas de seguridad. Es posible establecer límites éticos según el uso que se le dé a la recolección de datos luego de su análisis.

La limitación ética de OSINT adquiere más relevancia cuando, aunque sea lícito su tratamiento, OSINT conlleva un impacto negativo en los derechos del o de la titular de los datos. Las regulaciones de protección de datos personales incluyen la idea de impacto negativo al o a la titular de los datos personales que pueden producir, por ejemplo, los resultados de decisiones automatizadas. Lo que no siempre queda claro es qué se considera "impacto negativo". En algunos casos se sugiere que el impacto puede ser tanto moral como económico.[75] Estas cuestiones de análisis ético están vinculadas con el *output* de OSINT, mientras que la cuestión que merece un análisis más detallado en futuros estudios de OSINT se vincula más con el *input*, esto es con la recolección de los datos.

Si asumiéramos que la respuesta es que no hay un impacto negativo, una pregunta que queda abierta es si el o la titular de los datos no merecería recibir una contraprestación por el tratamiento de sus datos personales. Esta idea de "monetizar los datos personales" excede los objetivos de nuestra investigación, pero podría ser

[75] Por ejemplo, el perfilamiento de un individuo que concluye en la negativa de darle un crédito puede ser considerado un impacto negativo.

abarcada en el futuro estudio.[76] Sin duda este tema es uno pendiente de profundización y que se vincula con las prácticas OSINT.

Finalmente, se necesita tener más información sobre el uso de las prácticas OSINT en general. Es incuestionable que estas prácticas son cada vez más frecuentes, pero carecemos –al menos no los hemos encontrado– de estudios empíricos que permitan conocer la magnitud del uso de estas prácticas, quiénes son los actores en cada uno de los países de la región que la utilizan, y cuál ha sido, si es posible medirlo, el impacto o la utilidad de OSINT.

Por ello, y para concluir, un expresidente de un país de la región, que venía del campo académico, contó en sus memorias que cuando debía diseñar ciertas políticas públicas, reunía antes los datos que las justifiquen.[77] En el campo de OSINT, para explorar propuestas de políticas públicas tendientes a regular –o no– esas prácticas, tener la información como la mencionada –quiénes, cuánto, impacto– será fundamental.

[76] En una nota de divulgación, Jack M. Germain dice: "Actualmente, las grandes empresas de tecnología y la industria publicitaria utilizan información sobre usted de forma gratuita. Ambas entidades se benefician generosamente de sus datos con fines publicitarios dirigidos. No le ofrecen un centavo en compensación por usar sus datos privados ahora. Pero eso probablemente cambiará a medida que los consumidores se vuelvan más inflexibles sobre el robo y el uso flagrante de sus datos privados". Ver Germain, Jack M., "Consumers Can Now Monetize Personal Data to Earn Passive Income", Commerce Times, 2021, disponible en: https://www.ecommercetimes.com/story/consumers-can-now-monetize-personal-data-to-earn-passive-income-87205.html, último acceso: 23 de agosto de 2023; ver también Elvy, Stacy-Ann, "Paying for Privacy and the Personal Data Economy", en: *Columbia Law Review*, vol. 117, Nº 6, 2017, disponible en: https://columbialawreview.org/content/paying-for-privacy-and-the-personal-data-economy, último acceso: 23 de agosto de 2023; y el estudio de Bataineh, Ahmed Saleh y otros, "Monetizing Personal Data: A Two-Sided Market Approach", en: *Procedia Computer Science*, vol. 83, 2016, disponible en: https://www.sciencedirect.com/science/article/pii/S1877050916302447, último acceso: 23 de agosto de 2023.

[77] Ver Cardoso, Fernando Henrique y Winter, Brian, *The Accidental President of Brazil: A Memoir*, Nueva York, Public Affairs, 2006. En palabras de Cardoso, "Antes de tomar una decisión, me esforzaba por recopilar toda la información relevante y entender todos los puntos de vista, como me había enseñado mi antiguo mentor de la USP, Florestand Fernandes. La metodología, más que la ideología, fue el verdadero legado de mi carrera académica", p. 206 (la traducción es propia).