ARTICLE 19

Informe Prácticas de Open Source Intelligence (OSINT) en México

Primera edición por ARTICLE 19

▌**La presente investigación retoma la metodología desarrollada por el Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Universidad de Palermo (Argentina) en el marco de una investigación sobre Open Source Intelligence (OSINT) en América Latina y refleja los resultados de la misma sobre el uso de estas prácticas en México.**

▌La Hoja en Blanco, Creatividad Editorial: **Portada:** Alberto Nava | **Corrección de estilo:** Bárbara Lara | **Diseño y formación:** Guadalupe Urbina y Alberto Nava/La Hoja en Blanco. Creatividad Editorial.

ÍNDICE

Introducción

En la actualidad, expresarnos y comunicarnos con herramientas o recursos en línea es una actividad cotidiana entre las personas que cuentan con acceso a estos. Utilizando plataformas disponibles en las páginas de internet es posible compartir información personal sobre rutinas, gustos, intereses y todo aquello que acontece dentro y fuera de nuestra esfera individual, aportando con ello datos que pueden ser de utilidad para otros actores ajenos a nuestro espacio digital.

De la misma forma en que la información en fuentes o plataformas digitales aumenta, también sucede igual con los mecanismos para recolectar, procesar y almacenar los datos que se encuentran disponibles en la red. Es el caso de la inteligencia de fuentes abiertas (OSINT, por sus siglas en inglés), práctica que cualquier persona puede realizar, pero que tiene el fin de producir tareas de inteligencia. Este asunto toma mayor relevancia particularmente en el caso de los Estados, cuando se implican temas de seguridad.

En el caso de México, esta cuestión se relaciona con una práctica implementada por la policía cibernética o por la unidad de policía científica preventiva de las entidades federativas del país, la cual se denomina "ciberpatrullaje" y que consiste en la búsqueda de datos en fuentes abiertas (como la red pública de internet) y en la llamada *deep web*,[1] con la finalidad de identificar posibles conductas constitutivas de delitos cibernéticos. Si bien los estados de la república no optan

[1] La *deep web* es una parte de la web a la que no acceden los motores de búsqueda estándar (como Google, Firefox o Safari, por mencionar algunos) porque los contenidos están almacenados en una base de datos que no está codificada ni es accesible mediante una interfaz de búsqueda. Fuente: University of Washington Libraries, *Surface Web, Deep Web, Hidden Web,* https://guides.lib.uw.edu/c.php?g=342031&p=2300191

por llamarlo "prácticas de OSINT para la prevención y combate a los delitos cibernéticos", se toma al ciberpatrullaje como su similar debido a que mediante este proceso de patrullaje cibernético generan inteligencia, tal como lo plantea la inteligencia de fuentes abiertas (OSINT).

No obstante, las tareas realizadas por las policías cibernéticas quedan en la opacidad al no existir información pública amplia y disponible respecto a qué se refieren con el término de "ciberpatrullaje"; qué hacen mediante el monitoreo en internet; qué tipo de datos buscan y recolectan; cuál es la justificación para recolectar información sobre una o varias personas o qué sucede con los datos que recolectan y almacenan. Por lo tanto, el monitoreo de redes y las labores de inteligencia en fuentes abiertas en internet dibujan una delgada línea entre las acciones legítimas de seguridad y la vigilancia de las comunicaciones de las personas.[2]

Como lo ha advertido la Relatoría Especial para la Libertad de Expresión (RELE) de la Comisión Interamericana de Derechos Humanos (CIDH) "la vigilancia en internet, en cualquiera de sus formatos o matices, constituye una injerencia en la vida privada de las personas y, de ejercerse ilegítimamente, puede afectar además los derechos al debido proceso y a un juicio justo, a la libertad de expresión y al acceso a la información".[3]

En nuestro país no existe una regulación específica sobre el procesamiento de datos en fuentes abiertas o de OSINT. Esta ausencia, así como la opacidad al transparentar la información, da origen a prácticas controversiales por parte de las instituciones del Estado. Por ejemplo, de 2019 a 2022, el Senado de la República pagó $99,988,000 pesos a las empresas de ciberseguridad Silent4Business, S.A. de C.V y a Mavape, S.A.P.I. de C.V., para realizar prácticas de ciberpatrullaje, monitoreando a personas usuarias de Facebook y Twitter, quienes publican información de tipo político contra el Senado y quienes lo integran.

Lo anterior dio como resultado la recolección y el análisis de tenden-

---

2 A. Del Campo y M. Schatzky (abril de 2021). "Marco normativo y grises en una discusión que impacta directamente en nuestros derechos humanos". Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE). https://observatoriolegislativocele.com/ciberpatrullaje-o-inteligencia/

3 Relatoría Especial para la Libertad de Expresión-Comisión Interamericana de Derechos Humanos (2017) "Estándares para una Internet libre, abierta e incluyente", párr. 212. https://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf

cias, el monitoreo del comportamiento e impacto de las publicaciones en las redes sociales, así como la detección de las redes de personas usuarias.[4] Esto representa una vulneración a derechos humanos como el de la libertad de expresión y el de la privacidad, debido a que las personas no tienen conocimiento de que sus actividades en la web están bajo vigilancia por entes estatales, por el hecho de expresar sus ideas y opiniones.

Las prácticas de OSINT también las ofrecen empresas constituidas o con sede en México, las cuales cumplen con distintos objetivos como monitoreo de audiencias y de mercados; validación de personas, entre otros. Asimismo, algunas instituciones académicas del país con objetivos de investigación científica, o bien, el periodismo de investigación, implementan prácticas OSINT. No obstante, las actividades de procesamiento de datos en fuentes abiertas de los sectores mencionados suelen estar sujetos a la normativa interna y distan de las prácticas del aparato estatal; de tal forma que OSINT sirve para fines múltiples dependiendo del actor.

Con base en el contexto descrito, este informe titulado *Prácticas de Open Source Intelligence (OSINT) en México* es un primer trabajo exploratorio sobre la disponibilidad de la información, hasta el momento, sobre las prácticas de OSINT en nuestro país. Es importante destacar que no pretende abarcar la totalidad que conlleva la exposición de este tema.

En primer lugar, el documento plantea de forma breve el significado de la OSINT y la recolección de información en medios digitales, para después resaltar el asunto de los datos personales en el país y su protección por el sector público y privado. En un tercer instante, se abordan las prácticas de la OSINT en México a partir del enfoque en tres actores: *i)* fuerzas de seguridad del estado; *ii)* instituciones académicas, y *iii)* empresas. Por último, se retoman algunos puntos para ofrecer una conclusión, así como una serie de recomendaciones que pueden ser de utilidad para los sectores planteados en esta investigación.

[4] I. Ojeda (18 de septiembre de 2022). "El Senado gasta 99 mdp y reserva hasta los *hashtags* para ocultar vigilancia excesiva en redes sociales". *Estado Red.* https://estadored.mx/2022/09/el-senado-gasta-99-mdp-y-reserva-hasta-los-hashtags-para-ocultar-vigilancia-excesiva-en-redes-sociales/

I. ¿OSINT?

Open Source Intelligence o inteligencia de fuentes abiertas (OSINT) refiere a un conjunto de técnicas y herramientas[5] para obtener conocimiento y generar inteligencia por medio de la recolección, el procesamiento y el análisis de la información pública. Dicha información se puede encontrar en diferentes fuentes no restringidas, como libros, periódicos, radio, televisión, base de datos gubernamentales, publicaciones en plataformas digitales como texto, fotografías, videos, voz, geolocalización, entre otras.

La obtención de la información puede ser de forma física o digital; sin embargo, la expansión de internet ha traído el aumento de datos o información expuestos, de forma consciente o inconsciente, por las personas usuarias que utilizan ese medio, lo que da lugar al desarrollo de herramientas innovadoras para automatizar la recolección y el análisis de datos[6] en fuentes abiertas.

Con la normalización del acceso a las tecnologías de información y comunicación (TIC) estamos acostumbrados a las búsquedas constantes en distintas plataformas de la web, donde la información esta al alcance de un clic para todas las personas, exceptuando aquella que por su configuración requiere de otro tipo de interacción, por ejemplo, la creación de cuentas anónimas o falsas, con la finalidad de proteger la identidad de una persona investigadora y con ello obtener información directa sobre uno o varios individuos.

---

5 A. Fonte. (08 de marzo de 2021). "OSINT. ¿Qué es? ¿Para qué sirve?". *Derecho de la red*. https://derechodelared.com/osint/

6 J. Pastor-Galindo, *et al.* (2019). OSINT is the next Internet goldmine: Spain as an unexplored territory. https://www.researchgate.net/publication/333703698_OSINT_is_the_next_Internet_goldmine_Spain_as_an_unexplored_territory

A propósito, debido al número de personas usuarias en redes sociales en México,[7] podemos decir que nos encontramos frente a grandes bloques de información personal; esta puede ser recolectada por uno o varios actores. Lo anterior recae en una disyuntiva debido a que una vez que las personas usuarias comparten sus datos en plataformas como Facebook,[8] Instagram, Twitter, TikTok y demás aplicaciones digitales, algunos datos son públicos, según los términos de privacidad de cada red social, lo que da mayor apertura a su recolección y procesamiento.

Por citar un ejemplo, los datos de las personas usuarias pueden encontrarse mediante un motor de búsqueda, ya que las políticas de privacidad de Twitter señalan que, al aceptar los términos y las condiciones de la plataforma, y si la persona usuaria está públicamente disponible (con una cuenta abierta, sin candados y con una configuración de privacidad sin restricciones), los datos como nombre, nombre de usuario (@), su imagen (fotografía), la información del perfil (biografía y ubicación declarada), los tuits pulicados,[9] el correo electrónico, entre otros datos, pasan a ser públicos y se pueden compartir con las personas que están "fuera" de Twitter o con terceros, mediante la interfaz de programación de aplicaciones (API, por sus siglas en inglés).[10]

Por otra parte, en México existen actores de los sectores público y privado que recopilan y procesan información mediante la OSINT, para cumplir con los propósitos que les dicten en sus áreas, entre estos:

- Instituciones de seguridad del Estado, por ejemplo: la Secretaría de Seguridad y Protección Ciudadana (SSPyPC) en el ámbito federal y las secretarías de Seguridad Pública de cada entidad de la república, las cuales se encargan de investigar y perseguir los delitos, entre otras actividades.

---

7 En el Reporte Digital 2022 en México se estima que las personas usuarias activas de plataformas sociales rondan entre los 102.5 millones, es decir, el 78.3 por ciento de la población del país, quienes pasan cerca de tres horas 20 minutos usando alguna red social. https://datareportal.com/

8 En 2019, Facebook (Meta) desmanteló el sistema de búsqueda conocido en inglés como *Graph Search* (búsqueda gráfica) que permitía "encontrar contenidos públicos –y sólo públicos– a los que no es fácil acceder mediante búsquedas por palabras clave". Dicho sistema era ampliamente utilizado por periodistas, centros académicos y personas defensoras de derechos humanos. C. Silverman (10 de junio de 2019). "Facebook Turned Off Search Features Used To Catch War Criminals, Child Predators, And Other Bad Actors". BuzzFeed. https://www.buzzfeednews.com/article/craigsilverman/facebook-graph-search-war-crimes

9 Twitter. Developer Policy. https://developer.twitter.com/en/developer-terms/policy

10 Twitter (10 de junio, 2022). Política de privacidad de Twitter, pp. 11-13. https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-june-10-2022/Twitter_Privacy_Policy_ESLA.pdf

- Investigadores de centros académicos públicos o privados, que realizan investigación científica o de divulgación sobre, por mencionar algunos casos, cuestiones sociales como análisis de percepción sobre temas políticos; documentación acerca de las violaciones de derechos humanos; el tipo de interacción entre las personas y gobierno, etc.
- Organizaciones privadas o empresas que brindan servicios de inteligencia al Estado a otras agrupaciones y personas en general, para asuntos de seguridad de la información, *marketing* e, incluso, para la identificación y validación de una persona.

A simple vista, es posible pensar que el uso de la inteligencia de fuentes abiertas es inofensiva porque versa sobre información ya disponible al público, pero la recolección de datos personales —aunque sean divulgados por la persona usuaria— por parte de distintos actores, en especial por las fuerzas de seguridad, presupone riesgos en los derechos de libertad de expresión y privacidad de las personas en la red.

II. Datos personales

Los datos personales aluden a la información que caracteriza, identifica y hace reconocible a una persona. Al mismo tiempo, esto nos hace únicos como individuos, ya que nos diferencian del resto de las personas. Por lo general, dichos datos corresponden al nombre, sexo, preferencia u orientación sexual, edad, domicilio, ideologías políticas o religiosas, entre otros que describen nuestra personalidad.

La importancia de los datos personales es vital para desarrollarnos y procurar nuestra identidad y seguridad,[11] por lo que podemos clasificarlos como sigue:

Clasificación de los datos personales	
De identificación	Nombre, domicilio, teléfono particular o celular, correo electrónico personal, estado civil, firma, firma electrónica, cartilla militar, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), nombres de familiares, dependientes o beneficiarios.
Laborales	Contenidos en las solicitudes de empleo, correo electrónico y número de teléfono institucionales, actividades extracurriculares, referencias laborales y personales, recomendaciones, capacitaciones, documentos de selección, reclutamiento, nombramiento, incidencias, hojas de servicio, entre otros.
Patrimoniales	Bienes muebles e inmuebles, ingresos y egresos, cuentas bancarias, seguros, fianzas, afores, historial crediticio, información fiscal, servicios contratados y afines.
Administrativos y jurisdiccionales	Procedimientos administrativos o juicios en materia laboral, civil, penal, fiscal, mercantil o de cualquier otra rama del derecho.
Académicos	Trayectoria académica y formación profesional, calificaciones, boletas, constancias, certificados, reconocimientos, títulos, cédulas profesionales, entre otros.
De tránsito y movimiento	Información acerca de nuestro tránsito dentro y fuera del país.

Fuente: INFOEM. ¿Cómo se clasifican los datos personales?, https://www.infoem.org.mx/es/contenido/datos-personales.

[11] INAI (s.f.). Guía para titulares de los datos personales (*1*). Conceptos generales de la protección de datos personales, p. 5.

También hay datos personales considerados *sensibles* que requieren de una alta protección y cuidado, porque están ligados a la esfera más íntima de nuestra vida, como el origen racial o étnico, el estado de salud, la información genética, las creencias religiosas, filosóficas y morales, la afiliación sindical, las opiniones políticas y la preferencia u orientación sexual.[12] La divulgación o la exposición de esos datos puede provocar actos de discriminación expresados, por ejemplo, mediante el acoso en redes sociales hacia una persona por tener alguna condición médica; ello pone en riesgo la integridad física, psicológica o emocional de un individuo o grupo.

Los datos mencionados pueden localizarse en fuentes abiertas, por lo que es indispensable tomar consciencia de con quiénes los compartimos y en qué medios lo hacemos.

PROTECCIÓN DE DATOS PERSONALES

Todas las personas en México tienen derecho a la protección de sus datos personales, según lo estipulado por la Constitución Política de los Estados Unidos Mexicanos (CPEUM), en el artículo sexto, apartado A, el cual señala ocho bases y principios que rigen al ámbito federal y a las entidades federativas, a fin de garantizar el ejercicio del derecho de acceso a la información, entre ellas, la fracción II, la cual indica que "(l)a información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes."[13]

Asimismo, el párrafo segundo del artículo 16 indica que "toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros."[14]

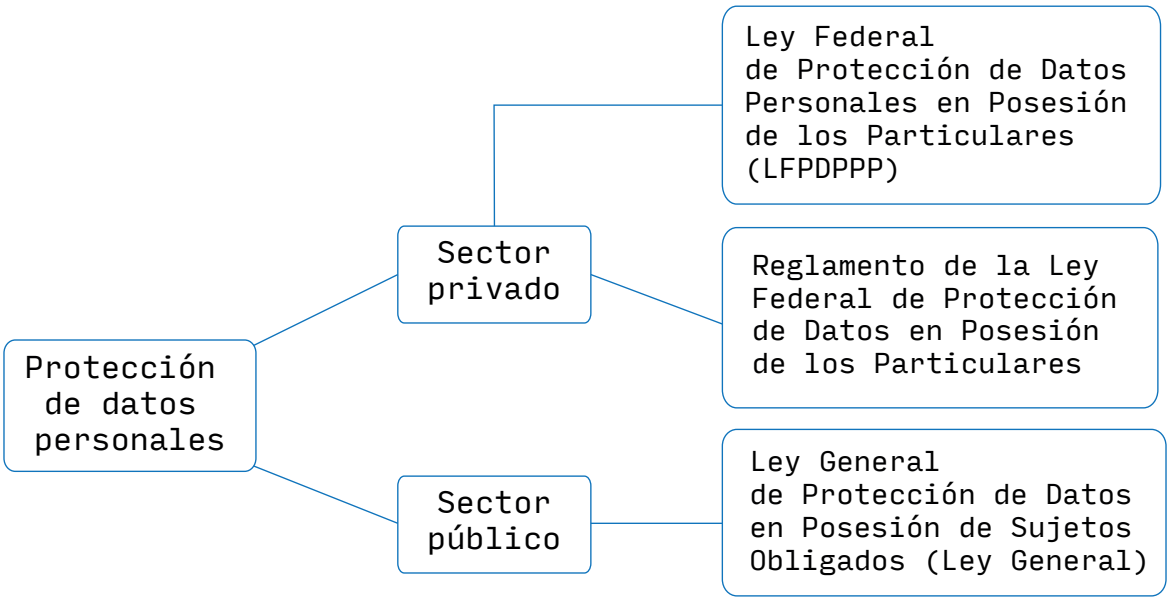
---

12 Ley Federal de Protección de Datos Personales en Posesión de los Particulares. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

13 Véase: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

14 *Idem*.

En ese sentido, para regular el tratamiento de los datos personales se han establecido leyes específicas vinculadas a los sectores que trabajan con estos, de acuerdo con el diagrama:



En el primer bloque se observa a las personas físicas y morales de carácter privado, por ejemplo, empresas y servicios médicos privados, que están sujetos a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su reglamento[15] aplicado en todo el territorio mexicano.

En el sector público ubicamos a la autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos de los ámbitos federal, estatal y municipal. Destaca en estos casos que cada estado de la república debe contar con una ley sobre el tratamiento de los datos

personales por parte del sector público, aplicable en su territorio y armonizado con la ley general.[16]

---

15 Además de la LFPDPPP y su reglamento, el INAI establece otros lineamientos para el sector privado, los cuales están disponibles en su portal.

16 INAI (s.f.). Guía para titulares de los datos personales (*1*)..., *op. cit.*, p. 9.

En resumen, todas las personas en el país tienen derecho a la protección de sus datos personales. Los responsables del tratamiento de esos datos deben protegerlos y adoptar las medidas necesarias para su cuidado, así como precisar mediante sus avisos de privacidad la finalidad que estos tendrán. También es indispensable que las personas que ceden su información presten atención a los avisos disponibles y cuestionen los usos que tendrán sus datos.

III. Prácticas de la OSINT en México

A pesar de ser una práctica que no está contemplada y, por lo tanto, prohibida o limitada en las leyes de México, el uso de las técnicas y las herramientas en fuentes abiertas comenzó, aproximadamente, hace menos de diez años, a cargo de las instituciones de seguridad pública del Estado. A ello se suman los centros académicos y las organizaciones con sede en el país, por lo que es pertinente puntualizar qué es lo que hace cada sector respecto a las prácticas de la OSINT.

FUERZAS DE SEGURIDAD

La inexistencia de protocolos específicos para las fuerzas de seguridad del Estado no exime que estas adquieran *software* y cursos relacionados con las funciones de la OSINT, especialmente para las tareas de vigilancia, bajo el supuesto de combatir el crimen y reducir los delitos.

En función de lo anterior, el primer registro que se encontró y que se relaciona con las tareas de la OSINT, se asimila en la actividad de ciberpatrullaje[17] contemplada en el Modelo Homologado de las Unidades de Policía Cibernética, del acuerdo 06/XLI/16 aprobado el 20 de diciembre de 2016, por el Consejo Nacional de Seguridad Pública, diseñado como respuesta a

[17] El documento en cuestión no delimita a qué se refiere con "ciberpatrullaje", pero este puede ser "una mezcla de técnicas, en su mayoría preventivas, con la finalidad de buscar actividad ilegal en la red y descubrir a los delincuentes [...] es la obtención y la recolección de información, el almacenamiento y el análisis del contenido que existe en las redes". El monitoreo se realiza en redes sociales, *dark web*, web. FIIAPP (14 de mayo de 2020). ¿Qué es... *ciberpatrullaje?* [archivo de video]. YouTube. https://youtu.be/0fXVnfYtJSA

la estrategia llamada Detección y atención oportuna de los delitos cibernéticos, del Programa Nacional de Seguridad Pública, 2013–2018. Lo anterior corresponde al gobierno del ex presidente Enrique Peña Nieto para fortalecer a las policías cibernéticas estatales en cuanto a sus capacidades humana, tecnológica y de infraestructura para detectar y atender delitos cibernéticos.[18]

Cabe destacar que el modelo comenzó su implementación en 2017, con relación a la madurez de las unidades de la policía cibernética de las entidades federativas, dividiéndolas en tres niveles:

Nivel 0: estados con unidades cibernéticas con operación mínima o que no cuentan con unidad.
Nivel 1: estados con unidades cibernéticas de operación básica.
Nivel 2: estados con unidades cibernéticas establecidas y en operación.

Las unidades que se encontraban en el primero y segundo nivel empezaron con los procesos de prevención y atención de delitos cibernéticos, así como de ciberpatrullaje; este último con el objetivo de identificar las probables conductas constitutivas de delitos cibernéticos cometidas en internet mediante la búsqueda de datos en fuentes públicas que permitieran la generación de inteligencia y nuevas líneas de investigación con otras unidades de la policía, con instituciones de los tres órdenes de gobierno (municipal, estatal, federal) y con autoridades competentes.[19]

Sin embargo, tras la llegada al poder de Andrés Manuel López Obrador, en 2018, se dio la extinción de la Policía Federal para dar apertura a la Guardia Nacional (GN), la cual, de acuerdo con su respectiva ley, tiene la facultad de *vigilar, identificar, monitorear y rastrear* la red pública de internet sobre sitios web, bajo el supuesto de prevenir conductas delictivas.[20]

Asimismo, en octubre de 2020, la Secretaría de Seguridad y Protección Ciudadana (SSPC), mediante el Secretariado Ejecutivo del Sistema Nacional

---

18 Modelo Homologado de Unidades de Policía Cibernética. https://www.gob.mx/cms/uploads/attachment/file/189189/Modelo_homologado_unidades_policia_cibernetica.pdf

19 *Ibídem*, p. 10.

20 Artículo 9, fracción XXXVIII de la Ley de la Guardia Nacional aprobada el 27 de mayo de 2019.

de Seguridad Pública (SESNSP) y el Centro Nacional de Información (CNI),[21] presentó el Sistema Multifuente para la estimación de la incidencia delictiva orientada a la inteligencia policial, como parte del fortalecimiento del Modelo Nacional de Policía y Justicia Cívica.[22] El Sistema Multifuente lo ideó el CNI con la finalidad de reducir la cifra negra y contribuir a la inteligencia policial por medio de diez fuentes sólidas y complementarias a las carpetas de investigación, entre ellas, el uso de datos e inteligencia operable de fuentes abiertas (OSINT).[23]

En ausencia de información detallada sobre el uso de la inteligencia de fuentes abiertas, se enviaron las siguientes solicitudes de acceso a la información utilizando la Plataforma Nacional de Transparencia (PNT):

- Secretaría de Seguridad y Protección Ciudadana (SSPC), folio 332069822000883.
- Guardia Nacional (GN), folio 332259822001253.
- Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), folio 330027622000619.

Las dependencias citadas respondieron que no contaban con los datos pertinentes respecto a las prácticas de recolección de datos personales; tampoco con los documentos realizados por medio de información en fuentes abiertas, ni los contratos con empresas privadas para la recopilación de datos personales.

ENTRE LAS PRÁCTICAS Y LA INEXISTENCIA DE LA INFORMACIÓN

Centro Nacional de Inteligencia

El proyecto sobre el Sistema Multifuente creado por el CNI propone que las unidades de análisis de las instituciones de seguridad pública implementen esta herramienta en el país para que ayude a integrar datos

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

[22] El modelo nacional de policía y justicia cívica fue aprobado el 8 de julio de 2019. Véase: https://www.gob.mx/sesnsp/articulos/modelo-nacional-de-policia-y-justicia-civica-238637

[23] Véase: https://www.gob.mx/sspc/prensa/presentan-sspc-sesnsp-sistema-multifuente-para-la-incidencia-delictiva

de manera efectiva y eficiente.[24] Una de las fuentes de información de las instituciones de seguridad pública son los mecanismos de proximidad: los chat vecinales y las redes sociales, aunque estas últimas "no cuentan con el mismo nivel de estandarización que el sistema de llamadas de emergencia".[25]

Lo anterior no es obstáculo para que el Sistema Multifuente pretenda explotar la información pública disponible en las redes sociales para "conocer el comportamiento de las personas y las estructuras sociales que se forman en comunidad",[26] de modo que, mediante las plataformas sociales en internet pueden detectar conductas delictivas y antisociales, y analizar las redes de vínculos entre actores o agentes relevantes para alguna investigación.[27]

A raíz de los párrafos expuestos, se estableció comunicación con una persona cercana al Centro Nacional de Información (CNI) para que aportara detalles acerca de este nuevo modelo.

El Sistema Multifuente no es específico a las prácticas de la OSINT, pues "el sistema pretende pasar de una sola fuente, que son justamente las carpetas, a la posibilidad de que las entidades utilicen distintas fuentes de información, como el 911 de emergencias, el 089 (de denuncia anónima) y otras fuentes de información, como el Registro Nacional de Detenciones".[28]

Hasta la fecha, se prevé que la implementación del Sistema Multifuente sea de naturaleza estatal, "(con la) firma de acuerdos entre las entidades que estén interesadas, y que cada una vaya desarrollando, en la medida de sus posibilidades, la capacidad de integrar esta información".

En cuanto a las fuentes abiertas, existen varias posibilidades de considerar de qué se trata este concepto. "Una de ellas, por ejemplo, es lo que las personas suben a las redes sociales: un video, o la descripción de un hecho. Básicamente, es información pública que está en

---

24 Modelo Nacional de Policía y Justicia Cívica (2020). Sistema Multifuente para la estimación de la incidencia delictiva orientada a la inteligencia policial, p. 15 https://www.gob.mx/cms/uploads/attachment/file/590581/sistema_multi-fuente_PP.pdf

25 *Ibídem*, p. 17.

26 *Ibídem*, p. 26.

27 *Ibídem*, p. 28.

28 ARTiCLE19 (20 de octubre de 2022). Entrevista a colaborador del CNI.

las redes sociales y que alguna persona sube". Sin embargo, las fuentes abiertas no se consideran una fuente fiable, pero sí de apoyo: "se utilizan las fuentes que son de carácter oficial, en particular el 911 y el 089, donde el ciudadano reporta los incidentes".

A propósito, el borrador del Sistema Multifuente señala la implementación de acciones preventivas mediante el monitoreo de redes sociales para la detección de conductas delictivas y antisociales, siendo este último un concepto ambiguo: "el modelo mexicano plantea dos tipos de delitos o conductas antisociales: delitos del fuero federal y de fuero común. La conducta antisocial es cualquier conducta que va en contra del reglamento municipal,[29] por ejemplo, el tema del ruido o no orinar en vía pública […] tiene que ver con una violación explícita a un reglamento de convivencia, o en su caso de justicia cívica".

Las prácticas de la OSINT no cuentan con protocolos específicos que lo regulen o limiten, debido a que su uso es complementario: "no existe un protocolo de búsqueda; en las entidades no es un fenómeno tan común, [por lo tanto] no existe como tal un instrumento en las entidades que estén monitoreando redes sociales de manera constante".

El Sistema Multifuente no representa ningún riesgo para los datos privados de las personas, pues "hay mecanismos para mitigar que los datos privados estén viajando por ahí. Las denuncias son anónimas; no preguntas el nombre de la persona".

Por otra parte, solo dos entidades federativas, Campeche y Quintana Roo, han suscrito el Sistema Multifuente para la estimación de la incidencia delictiva orientada a la inteligencia policial, por lo que, mediante la solicitud de acceso a la información con folio 040085000018722 a la Secretaría de Protección y Seguridad Ciudadana del Estado de Campeche, quien advirtió que en relación con el sistema en cuestión, se encuentra en proceso de implementación las acciones y las estrategias con el objetivo de contar con las herramientas para medir la incidencia delictiva y apoyo en la toma de decisiones.

---

[29] Respecto a las conductas antisociales, la alcaldesa del municipio de Acayucan, Veracruz, prohibió hacer bromas indecorosas, mortificantes o retos de redes sociales a las personas en lugar público, estipulado en el artículo 46, fracción III, del Bando de Policía y Buen Gobierno. Véase: https://imagendelgolfo.mx/estado/acayucan-prohibe-los-retos-virales-a-sus-habitantes/50251002

Guardia Nacional

De conformidad con el Censo Nacional de Seguridad Pública Federal, 2021, durante el año 2020 la División Científica de la Guardia Nacional, mediante el "monitoreo cibernético", identificó y desactivó 5,920 sitios web por actividades ilegales; entre ellas, el robo de datos financieros y personales con un total de 342 sitios.[30]

Si bien, lo anterior no hace referencia específica a una tarea de la OSINT, se asimila que el monitoreo cibernético recae en el concepto de ciberpatrullaje, actividad que está contemplada en la Ley de la Guardia Nacional, y dentro de las facultades de la División Científica previstas en el Manual de Organización General de la Guardia Nacional.

De modo similar, el 3 de octubre de 2022, la Guardia Nacional presentó la convocatoria IA-036H00998-E267-2022, para la contratación de un servicio de capacitación en Inteligencia en Fuentes Abiertas (Open Source Intelligence, OSINT)[31] que atiendiera los temas de: *(i)* teoría de la inteligencia y conceptos metodológicos y *(ii)* herramientas y bases de datos; impartido, tentativamente, en la Ciudad de México durante el mes de noviembre y diciembre de 2022. Cabe agregar que la convocatoria contradice a la respuesta de la Guardia Nacional por medio de la Plataforma Nacional de Transparencia (PNT) (folio: 332259822001253) en el marco de esta investigación, ya que mediante el oficio señalaron que no existía información respecto a las prácticas de la OSINT.

Entidades federativas

La poca transparencia de la información respecto a las prácticas de fuentes abiertas no solo atañe a las instituciones en el ámbito federal, porque en el estatal ocurre una situación similar puesto que los estados de Guerrero, Chihuahua y Veracruz han adquirido *software* relacionado con la OSINT.

---

30 Inegi (2021). Censo Nacional de Seguridad Pública Federal 2021. Presentación de resultados generales (actualizado el 11 de abril de 2022). https://www.inegi.org.mx/contenidos/programas/cnspf/2021/doc/cnspf_2021_resultados.pdf

31 La convocatoria fue eliminada del portal, aunque el documento (pdf) sigue disponible en: https://www.gob.mx/cms/uploads/attachment/file/765949/Convocatoria_IA-E267-2022_Curso_de_Inteligencia_en_Fuentes_Abiertas.pdf

En primer lugar, el Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública de Guerrero registró durante enero a junio de los años 2021 y 2022, respectivamente, un bien por el monto de $387,000 pesos mexicanos (19,903.41 USD), que corresponde a un "*software* para realizar la búsqueda de información sensible e investigaciones por medio de OSINT".[32]

Sumado a lo anterior, una nota periodística[33] reveló que uno de los Centros Regionales de Fusión de Inteligencia (Cerfi) ubicado en el 27 Batallón de Infantería en Iguala, Guerrero, realiza actividades de monitoreo de la intervención de comunicaciones privadas. La información corresponde a uno de los correos que filtró parte del *hackeo* del grupo Guacamaya a la Sedena, donde también se señala que con las capacidades tecnológicas del Cerfi realizan la intercepción de llamadas (CDR); geolocalizaciones; acceso a redes sociales; recuperación de datos (forensia digital); destacando una plataforma integral de inteligencia que opera con un módulo de la OSINT, con el cual recolectan datos de las plataformas de redes sociales.

En segundo lugar, el estado de Chihuahua, mediante la publicación del documento "Evaluación del Programa para el Fortalecimiento del Estado de Fuerza y las Capacidades Institucionales",[34] publicado en octubre de 2020, señala la creación de la policía cibernética con tecnología de punta que permite el ciberpatrullaje; además, el personal de dichas actividades cuenta con un perfil especializado en conocimientos técnicos en OSINT, con la finalidad de recabar información en redes sociales y cualquier sitio en internet.

Los datos obtenidos durante el ciberpatrullaje son procesados y analizados para generar "productos de inteligencia para la identificación de perfiles simulados con *modus operandi* o situaciones inusuales que vulneren la seguridad y/o situaciones inusuales que vulneren la seguridad de los cibernautas".[35]

---

32 La información referente al *software* está disponible en los datos abiertos de la Plataforma Nacional de Transparencia bajo el término "OSINT". Véase: https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=OSINT&coleccion=5

33 L. Ocampo Torres (3 de noviembre de 2022). En Iguala funciona un centro regional de espionaje del Ejército, revela el hackeo del grupo Guacamaya. *El Sur.* https://suracapulco.mx/en-iguala-funciona-un-centro-regional-de-espionaje-del-ejercito-revela-el-hackeo-del-grupo-guacamaya/

34 Gobierno del Estado de Chihuahua (2020). Evaluación del Programa para el Fortalecimiento del Estado de Fuerza y las Capacidades Institucionales. https://www.gob.mx/cms/uploads/attachment/file/604448/DIAGNO_STICO_CHIHUAHUA_2020.pdf

35 *Ibídem*, p. 11.

Al respecto, se envió una solicitud de acceso a la información a la Secretaría de Seguridad Pública del Estado de Chihuahua, por conducto de la PNT, con el folio 082467722000252. Sin embargo, a pesar de la ampliación del plazo para la entrega, el oficio de respuesta no contenía ningún dato, lo cual se excusó con el cambio de administración y se indicó que la información se haría llegar al correo electrónico registrado, acción que nunca se concretó. Por lo anterior, se localizó al responsable de la Unidad de Transparencia de la secretaría en cuestión, pero por segunda ocasión la información no fue enviada.

Similar al párrafo precedente, una nota periodística de *La Verdad Juárez* expuso la opacidad que conlleva la construcción del proyecto "Torre Centinela", que será la central de la Secretaría de Seguridad Pública del Estado de Chihuahua. Dicha torre es un proyecto ambicioso que integra tecnología de vigilancia como cámaras de videovigilancia, arcos de identificación y drones; no obstante, el cuerpo de la nota menciona que al solicitar información del proyecto a la SSPE, con folio 08246772200170, vía PNT, la respuesta fue negada por "adecuaciones administrativas". Ello fue similar a la respuesta que se recibió para los fines de esta investigación, por lo que la secretaría en cuestión mantiene una conducta reiterada de bloqueo al acceso a la información.

En tercer lugar, ubicamos al estado de Veracruz, el cual, en virtud del Informe Estatal de Evaluación 2021, adquirió y renovó licencias de *software* especializado para tareas específicas de la Policía Científica Preventiva, entre ellas, la inteligencia de fuentes abiertas,[36] con el objetivo de fortalecer y mejorar el desempeño de la policía científica y combatir la ciberdelincuencia. Por lo anterior, se registró una solicitud de acceso a la información en la PNT con folio 301153922000458, dirigida a la Secretaría de Seguridad Pública del Estado de Veracruz, la cual informó que:

> Se entiende por inteligencia de fuentes abiertas a la búsqueda de información pública en internet, según lo dispuesto en el artículo 143,[37] de la

[36] Gobierno del Estado de Veracruz-SESCESP (2021). Evaluación Integral del Fondo de Aportaciones para la Seguridad Pública (FASP) del Estado de Veracruz. Ejercicio fiscal 2021. Informe Estatal de Evaluación http://ftp2.fiscaliaveracruz.gob.mx/WEB%20FGE/FASP/2021/Evaluacion-Integral-FASP-Veracruz-2021.pdf

[37] Véase: http://www.ordenjuridico.gob.mx/Documentos/Estatal/Veracruz/wo120937.pdf

> Ley 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave; no obstante la información señalada por la Secretaría es errónea, debido a que el numeral en cuestión aborda la información entregable que se encuentra en el poder de los sujetos obligados.

Asimismo, por medio de la Secretaría Ejecutiva del Sistema y del Consejo Estatal de Seguridad Pública se dió conocer un importe de $1,774,782.12 pesos, por concepto de licencias y *software*. Lo anterior de acuerdo con los recursos del Fondo de Aportaciones para la Seguridad Pública (FASP) durante 2021. La SSP del estado de Veracruz facilitó los contratos (testados) de licencias y *software* adquiridos en ese año, de los cuales se encuentran las siguientes empresas:

Empresa	Tipo de adquisición	Monto total
Vanume S. de R.L. de C.V.	*Software*	$400,000.00
Corporativo S.O.S, S.A. de C.V.	Reservado	$781,956.62
Corporativo S.O.S.	Reservado	$974,840.80
Corporativo S.O.S.	Reservado + Licencia anual de Adobe Creative Cloud (todas las aplicaciones), incluye más de 20 aplicaciones y servicios para escritorio y dispositivos móviles.	$41,406.26
Corporativo S.O.S.	*Software*	$399,941.32

Fuente: elaboración propia con datos otorgados por la SSP de Veracruz.

No obstante, el monto total de las facturas facilitadas por la Secretaría de Seguridad Pública del Estado de Veracruz es de $2,598,145 pesos mexicanos, lo que contradice al monto señalado en el punto dos, aunque, por la reserva de información en los documentos, no hay forma de corroborar los datos. Además, dicha secretaría detalló que brindar información respecto a qué tipo de *software* y licencias ha implementado, constituye información de carácter reservado,[38] ya que puede producir un daño mayor en materia de seguridad pública.

En el mismo sentido, la exposición de las especificaciones tecnológicas, *software*, protocolos y demás información que comprende la estructura y el actuar de la Policía Científica Preventiva en cuanto al

[38] Artículo 113, fracción I, Ley General de Transparencia y Acceso a la Información Pública: como información reservada podrá clasificarse aquella cuya publicación: I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable.

monitoreo en fuentes abiertas, podrían ser susceptibles de sabotaje y producir una deficiencia en la operación de la unidad para salvaguardar la seguridad pública; en consecuencia, la información se clasificó como "reservada por cinco años".

ACADEMIA

En la actualidad, las prácticas de fuentes abiertas son comunes en el ámbito de la investigación académica. En el país, se hallaron distintos centros que se presupone realizan prácticas de OSINT para fines científicos o de divulgación. En la siguiente figura se muestran las instituciones académicas que participaron en el proceso de la presente investigación:

Centro académico	Desde cuándo utiliza información de fuentes abiertas	Por qué se presupone que se realizan prácticas de fuentes abiertas
Laboratorio para el Análisis de Información Generada a través de Redes Sociales en Internet (LARSI); Centro de Estudios de Opinión y Análisis (CEOA) de la Universidad Veracruzana.	2017	Debido a que el laboratorio fomenta y contribuye a la investigación interdisciplinaria en áreas relacionadas con ciencia de datos, big data, ciencia de redes, sistemas complejos y ciencia social computacional. Asimismo, se observa en su página web https://www.uv.mx/larsi/general/investigacion-2/ sus líneas temáticas, las cuales abarcan los tópicos: Minería social[39] de información proveniente de fuentes de datos abiertos y de plataformas sociales de internet; la exploración y el análisis entre la información generada en línea contra la información generada de forma oficial, entre otras.
Programa Política de Drogas; Centro de Investigación y Desarrollo Económico (CIDE), Región Centro.	Sin especificar	En vista del proyecto Base de datos de presencia criminal en México 2020 (BACRIM 2020), disponible en https://ppdata.politicadedrogas.org/#ppd.gc el cual utilizó la técnica web *scrapping*[40] de fuentes abiertas en internet para identificar 150 grupos criminales en México, el tipo de actividades que desarrollan, así como las alianzas y rivalidades entre los grupos.

continúa

39 Minería social (*social media data mining*) se refiere al proceso de extracción de datos en plataformas como Facebook, Twitter, TikTok, YouTube, etc. La minería social implica la recopilación, procesamiento y análisis de los datos para descubrir patrones y tendencias relevantes. Tomado de: Ausrine (22 de junio de 2021). Social Media Data Mining: What It Is, How It Works, and How to Use It. En: *Whatagraph*. https://whatagraph.com/blog/articles/social-media-data-mining

40 *Web scrapping* es una técnica que ayuda a extraer datos de un sitio web. Esta información es recolectada y exportada en un formato más útil para la persona como en una hoja de cálculo o una API (Application Programming Interfaces; español: Interfaz de Programación de Aplicaciones). Tomado de: Perez, M. (1 de agosto de 2021). What is Web Scraping and What is it Used for? *Parsehub*. https://www.parsehub.com/blog/what-is-web-scraping/

Centro académico	Desde cuándo utiliza información de fuentes abiertas	Por qué se presupone que se realizan prácticas de fuentes abiertas
Programa de Derechos Humanos; Universidad Iberoamericana (Ciudad de México).	Septiembre de 2020	Por el proyecto Violencia y terror. Hallazgos sobre fosas clandestinas en México, disponible en https://programadh.ibero.mx/#Publicaciones-title donde se pueden consultar los datos desagregados a nivel estatal y municipal de fosas clandestinas en el país. De modo similar, cuenta con el proyecto Digital Verification Corps, desarrollado por Amnistía Internacional y, en conjunto con centros de derechos humanos de distintas universidades como Berkeley, Cambridge y Essex, busca capacitar a estudiantes voluntarios, sobre posibles violaciones a derechos humanos, con el uso de herramientas OSINT.

Cabe destacar que las acciones de las y los investigadores se rigen por principios éticos que deben cumplir dentro de los centros universitarios a los que pertenecen, es decir, las instituciones citadas previamente contemplan códigos de ética con principios como el respeto, la responsabilidad, la integridad,[41] la seguridad y el cuidado, la honestidad, la imparcialidad,[42] el interés público,[43] la transparencia y la rendición de cuentas.

Por otro lado, con el objetivo de obtener mayores detalles acerca de las prácticas que llevan a cabo en fuentes abiertas, se entrevistó[44] a las y los investigadores de los tres centros académicos mencionados en la figura de arriba.

De acuerdo con la información brindada por las personas de los centros académicos se infiere que el concepto de *fuentes abiertas* refiere a toda información de libre acceso disponible en internet, tal como diarios digitales, sitios web, etc., así como la información que se encuentra en redes sociales como Facebook, Twitter y TikTok, por mencionar algunas.

Para llevar a cabo la recolección de datos en fuentes abiertas, especialmente en redes sociales, no es necesario contar con algún perfil personal o anónimo; basta con tener un *software* de licencia oficial, es

41 Código de Ética y Conducta de la Universidad Iberoamericana (2014). https://ibero.mx/sites/all/themes/ibero/descargables/corpus/codigo-etica-conducta.pdf

42 Código de Ética de la Universidad Veracruzana (2016). https://www.uv.mx/legislacion/files/2016/12/Codigo-de-Etica-UV.pdf

43 Código de Conducta del Centro de Investigación y Docencia Económicas (2019). https://www.cide.edu/wp-content/uploads/2019/10/codigo_de_conducta_2019.pdf

44 Las entrevistas fueron aplicadas en distintos momentos durante el mes de septiembre de 2022.

decir, un programa computacional de pago (licencia) el cual permite tanto conectarse a la plataforma, como descargar datos o contar con una licencia con fines de investigación que otorgan las plataformas digitales como Twitter para acceder a la información disponible; este es el caso del LARSI-UV, mientras que para los proyectos del Programa de Derechos Humanos-Ibero y del Programa Política de Drogas-CIDE suele utilizarse una identidad anónima o usar su propia identidad sin interactuar con otras personas usuarias en la red.

El uso de fuentes abiertas puede dar lugar a la recolección de datos personales de las personas usuarias en Internet, principalmente de aquellos que se encuentran en redes sociales. Es el caso del LARSI-UV, ya que "puedes llegar a tener acceso a información de cuentas públicas de políticos, actores, cantantes…, especialmente en la parte de sus fotografías en redes como Facebook e Instagram".[45] A diferencia de los programas de Política de Drogas-CIDE y el de Derechos Humanos-IBERO, los cuales no tienen información de personas individualizadas.

A propósito de lo anterior, solo el Programa de Derechos Humanos-IBERO cuenta con principios para el tratamiento de la información que se obtiene en fuentes abiertas, como el de "no sobrerecopilar información; y no exponer materiales que puedan poner en peligro la identidad o seguridad de las personas",[46] y la información recolectada se almacena en una base de datos que puede ser para un proyecto con Amnistía Internacional o para análisis que puede ser publicado o no.

Una situación distinta ocurre con el LARSI-UV que está en proceso de creación de un procedimiento para tratar la información que se obtiene en redes sociales en internet, pero, hasta el momento, se tiene la seguridad informática necesaria en la infraestructura donde se almacenan los datos, es decir, se protege mediante un servidor y un *firewall* y, en caso de que la información ya no sea requerida o que viole elementos de privacidad, se procede a su eliminación. A la par, el Programa de Política de Drogas-CIDE tampoco cuenta con un procedimiento y la información que reúne la almacena en una base datos, ya sea para su consulta posterior o, por ejemplo, "para alimentar el algoritmo de TikTok

45 ARTiCLE19 (31 de agosto de 2022). Entrevista al Dr. Carlos Piña, investigador y responsable del LARSI en el Centro de Estudios de Opinión y Análisis de la Universidad Veracruzana.

46 ARTiCLE19 (26 de septiembre de 2022). Entrevista a la Lic. Fernanda Lobo, colaboradora del Programa de Derechos Humanos de la Universidad Iberoamericana.

con la finalidad de conocer cómo es la comunicación entre la ciudadanía y el crimen organizado".[47]

En el mismo sentido, únicamente el Programa de Derechos Humanos-Ibero tiene límites para la búsqueda en fuentes abiertas, ya que se rige por el Protocolo de la Universidad Berkeley[48] y sigue los principios de: *i)* no sobrerrecolectar información; *ii)* enfocarse en la pregunta de investigación, y *iii)* no buscar más contenido del que se necesita. Ello en comparación con el Programa Política de Drogas-CIDE que no tiene límites y el LARSI-UV contempla los límites impuestos por las plataformas digitales.

A pesar de que las búsquedas de información en fuentes abiertas no conciernen esencialmente a datos personales, el LARSI-UV no podría realizar su trabajo sin tener estos datos, ya que en las redes sociales la información se vincula con la persona usuaria. En cambio, la recolección de dichos datos no es indispensable para el Programa de Política de Drogas-CIDE y el de Derechos Humanos-Ibero.

Por otra parte, la privacidad es un tema ligado a la búsqueda de información en fuentes abiertas; además, es analizado por las y los investigadores quienes han recibido capacitación sobre los estándares de protección de los datos personales en México, a excepción del equipo LARSI-UV que está próximo a hacerlo y, si bien no divulgan datos personales que encuentran durante la recolección, el investigador del LARSI-UV resalta que, al aceptar los términos y las condiciones de uso y realizar diversas publicaciones, exponemos nuestra información privada. Tal es el caso de compartir en un comentario nuestro correo electrónico o número de teléfono para que nos hagan llegar información acerca de un producto o, en su caso, para estar en contacto con una persona.

---

47 ARTiCLE19 (1 de septiembre de 2022). Entrevista a la Dra. Laura Atuesta, investigadora del Programa Política de Drogas del CIDE.

48 Berkeley Protocol on Digital Open-Source Investigations (Procotocolo de Berkeley sobre Investigaciones Digitales de Código Abierto) es un protocolo internacional que marca las directrices y los estándares para el procesamiento de la información recolectada mediante fuentes abiertas, como las fotografías, vídeos, textos, y otras publicaciones en redes sociales (Twitter, Instagram, TikTok, etc.) acerca de los crímenes y violaciones a derechos humanos. El documento aborda las formas éticas, profesionales y legales para usar la información, así como recomendaciones para proteger la integridad física/digital de los investigadores y de las personas que realizan las publicaciones. https://humanrights.berkeley.edu/berkeley-protocol-digital-open-source-investigations

A pesar de lo mencionado, manejar "información privada" que se encuentra disponible en las fuentes abiertas –y en redes sociales– presupone riesgos para los investigadores, debido a que tanto el Programa Política de Drogas–CIDE como el LARSI–UV han sido cuestionados e incluso denunciados por sus publicaciones. El primero fue cuestionado por personas del mismo gobierno, por publicar una base de datos (sin la información personal) filtrada por el gobierno; el segundo, por el "uso indebido de recursos para acosar cuentas pro–AMLO" donde se le vinculaba con la plataforma de Twitter bajo el supuesto de recibir información privada de las personas usuarias; empero, se demostró que la acusación estaba infundada.[49]

Finalmente, aunque las y los investigadores de los tres centros académicos citados trabajan y recolectan información en fuentes abiertas, la mayoría no está de acuerdo con que recopilen datos referidos a su persona, aunque al estar expuestos en redes sociales conocen los riesgos que esto puede generar en su esfera privada.

SECTOR PRIVADO

Los servicios de inteligencia de fuentes abiertas en el país los efectúan empresas nacionales e internacionales con sede en México. Estos van desde las prácticas de seguridad de la información y monitoreo de mercados, hasta la búsqueda de información para la validación de una persona. Por lo anterior, se entrevistó[50] a tres personas de este sector, las cuales pertenecen a las siguientes organizaciones:

49 La información relativa a la acusación de la persona investigadora se encuentra en el siguiente tuit: https://twitter.com/Piniisima/status/1511079716366782467?s=20&t=6EoyMixPueC2zaLnziIN4Q

50 Las entrevistas se realizaron en el mes de septiembre y octubre de 2022.

Empresa	Inicio de labores/ búsquedas en fuentes abiertas	Por qué se presupone que realizan prácticas en fuentes abiertas
OSINT Latinoamérica	2016	Por la información en su sitio web https://osintlatinoamerica.com/ en el cual ofrecen cursos de inteligencia y seguridad, entre ellos, la certificación de competencia en inteligencia de fuentes abiertas.
ReconoSER ID	2018	En vista de los servicios de "Identidad digital" disponibles en https://reconoserid.mx en especial Identification aaS, donde recopilan y analizan información de las personas por medio de fuentes abiertas, como redes sociales, monitores de búsqueda, bases gubernamentales, fotografías, entre otros.
Pentesting-Seguridad Informática	Sin especificar	Debido a la información publicada en https://www.pentesting.com.mx/index.php/servicios-especializados/investigacion-osint donde ofrecen investigación por fuentes abiertas respecto a personas y empresas, enfocado a la contratación de recursos humanos.

Las personas del sector privado que trabajan con fuentes abiertas las describen como toda fuente de acceso sin ningún tipo de restricción o privilegio de acceso; es decir, es toda la información expuesta y alcanzable en cualquier parte de internet, por ejemplo, las bases públicas del gobierno que permiten comprobar la identidad de una persona, tales como Renapo e INE.

De la información que recolectan, las empresas en cuestión reconocen que existen datos de personas individualizadas; sin embargo, para realizar este tipo de prácticas debe existir un consentimiento de la persona u organización que requiera el servicio, por ejemplo, en *Pentesting* llegan a tener acceso a datos personales debido a las malas prácticas de protección a la información personal.

En contraste con la investigación en redes sociales, las técnicas implementadas suelen ser anónimas o con un perfil falso; esta última opción se emplea para acceder a grupos cerrados con el objetivo de mantener la seguridad del investigador; así lo menciona el responsable de OSINT Latinoamérica. Además, no es necesario autenticarse en las redes sociales para extraer información, ya que hay formas de brincar las restricciones y visualizar la información que se pudiera ocupar, según el director de Pentesting.

El sector privado cuenta con procedimientos internos para el tratamiento de la información recolectada mediante fuentes abiertas. En el caso de OSINT Latinoamérica, existe una metodología de recolección, verifi-

cación y una cadena de custodia digital; ReconoSER ID tiene un acuerdo de términos y condiciones y un aviso de privacidad, mientras que Pentesting firma acuerdos de confidencialidad y siguen prácticas basadas en 27001 y 27002, así como un protocolo y una metodología escrita donde indican cómo se recolecta la información, qué recolectan, cuál es la evidencia y, posteriormente, efectúan un procedimiento de destrucción digital controlado y documentado.

Hasta el momento, la búsqueda de información disponible en fuentes abiertas no tiene límites y las empresas solo toman en cuenta las restricciones relacionadas con los factores tecnológicos: fallas, caídas y cambios (ReconoSER ID) o los que establece quien produce la información (OSINT Latinoamérica), tal como las empresas que no poseen límites y no hacen pruebas de seguridad y ponen en riesgo información que no desean exponer (Pentesting).

Por otra parte, la búsqueda y la recolección de información personal en fuentes abiertas varía de acuerdo con el servicio que ofrece cada empresa. En el caso de ReconoSER ID, quien se encarga de identificar y acreditar a una persona, es imposible prescindir de los datos personales, en comparación con Pentesting que no necesita buscar información personal. Destaca que en OSINT Latinoamérica depende de si esa información personal ya es pública.

En un primer acercamiento, podría parecer que las empresas no procuran ni piensan en la privacidad de las personas, pero las búsquedas que realizan en su ámbito laboral son autorizadas por las personas usuarias del servicio; sin embargo, el directivo de OSINT Latinoamérica cuestiona la responsabilidad de las personas usuarias: “¿dónde empieza la responsabilidad de la persona y dónde queda la ética?”.

En adición a lo anterior, todo el personal del sector privado ha recibido capacitación sobre los estándares de protección de datos personales en México e incluso en Pentesting, que forma parte de AMECI,[51] son una fuente de capacitación en la materia para otras organizaciones. Por demás, las empresas mencionadas no han sido cuestionadas o denunciadas por recopilar datos personales.

[51] AMECI (Asociación Mexicana de Ciberseguridad). https://www.ameci.org/

Finalmente, existe una negativa para que otras personas recopilen datos referidos a ellos, aunque dentro de su ámbito de trabajo haya un consentimiento para obtener los datos referidos a otros. No obstante, al estar expuestos a las redes sociales y aceptar los términos y las condiciones de uso de cada una de las plataformas, la responsabilidad de la información y, en este caso, la privacidad, concierne a cada persona; es decir, cada individuo decidirá con quién y qué tanto quiere compartir a otros sobre los aspectos de su vida.

Cabe destacar que las empresas en cuestión cuentan con un aviso de privacidad colocado en su página web donde señalan cuáles son los datos personales que recolectan, así como la finalidad de estos. Además, el aviso muestra las formas en las que las personas usuarias (titulares de los datos) pueden ejercer sus derechos de acceso, rectificación, cancelación u oposición de sus datos personales.

IV. Conclusiones

De conformidad con la información presentada en esta investigación, podemos empezar a concluir que el uso de la inteligencia de fuentes abiertas en México es una práctica compleja que carece de regulación y de transparencia, principalmente por los organismos del Estado.

Aunque el término parezca novedoso, las prácticas de OSINT por parte de las instituciones de seguridad pública se han implementado en las últimas dos administraciones bajo el supuesto de investigar delitos, primero: como parte del combate al "cibercrimen", y en segundo: como un monitoreo en la red pública de internet para vigilar, identificar y rastrear conductas delictivas.

A partir de lo mencionado, algunas instituciones de seguridad han adquirido herramientas OSINT para realizar tareas de inteligencia que ayuden a cumplir con sus fines. A pesar de ello, no hay documentos específicos, al menos de consulta pública, que den luz sobre la adquisición e implementación de este sistema para la recolección y procesamiento de datos personales, y sobre qué fuentes disponibles se hace.

Por otro lado, el uso de fuentes abiertas entre las instituciones académicas es cada vez más frecuente debido a la forma en que se presenta y difunde la información a través de las redes sociales, así como a los distintos tipos de reacción que produce en las personas usuarias. No obstante, si bien sólo una institución (PDH, IBERO) cuenta con un protocolo OSINT para sus trabajos en fuentes abiertas, las instituciones mencionadas en este informe pueden prescindir del uso de datos personales, en razón de que procuran conducirse con ética durante las estampas de toda investigación.

En el caso de las empresas con sede en México, estas cuentan con protocolos internos para la recolección, procesamiento y almacenamiento de datos personales, con el fin de apegarse a lo establecido por legislación de protección de datos personales en el país, además de integrar documentos de observancia internacional en la materia.

Las empresas señaladas en el marco de esta investigación se encargan de realizar múltiples tareas a través de OSINT, especialmente sobre seguridad de la información, y otros como: monitoreo de mercados y validación de la identidad de una persona, esta última actividad se realiza bajo el consentimiento de la persona. Y, de forma similar, estas organizaciones ponen a disposición de las personas la posibilidad de ejercer sus derechos ARCO.

Finalmente, mientras no exista un marco jurídico para las prácticas realizadas con OSINT del Estado, ni transparencia por parte de sus instituciones, la explotación de los datos por diversos organismos del sector público pueden fácilmente alejarse de las acciones de seguridad y convertirse en un instrumento de vigilancia de las comunicaciones y generar efectos inhibitorios o de autocensura al expresarnos en línea.[52]

[52] "El hecho de que la persona deje rastros públicos de sus actividades –en internet de manera inevitable– no habilita al Estado a recolectarla sistemáticamente salvo en las circunstancias específicas donde dicha injerencia estuviera justificada". "Estándares para una Internet libre...", *op. cit.*, párr. 214.

v. Recomendaciones

Es indispensable prestar atención a las tareas que realizan las instituciones federales y estatales de seguridad por medio del monitoreo en fuentes abiertas, es decir, actividades como el ciberpatrullaje en la red de internet, específicamente en redes sociales, ya que estas carecen de reportes oficiales disponibles al público, a excepción de aquella que es publicada y responde al "combate a la ciberdelincuencia".

Las instituciones de seguridad del Estado deben observar si las medidas que contemplan en la planeación, creación, divulgación e implementación de un proyecto que incluye el uso de tecnología para la vigilancia, detección para la preservación de la seguridad pública o nacional, responden en medida de lo posible a la protección de los derechos humanos de las personas, como la libertad de expresión y la privacidad.

Por lo tanto, las acciones del Estado en esta materia deben cumplir el test tripartito desarrollado en el sistema internacional de derechos humanos para que cualquier medida de vigilancia sea legal, necesaria y proporcionada.

En este sentido, los Estados también deben contemplar lo siguiente:

> De conformidad con los estándares internacionales en la materia,[53] las fuerzas de seguridad del Estado deben informar si las actividades de ciberpatrullaje corresponden a medidas de prevención del delito o a medidas de vigilancia de las personas.

[53] Principio 10 (12 de junio de 2013). "Principios globales sobre seguridad nacional y el derecho a la información (Principios de Tshwane)". https://www.oas.org/es/sla/ddi/docs/acceso_informacion_Taller_Alto_Nivel_Paraguay_2018_documentos_referencia_Principios_Tshwane.pdf

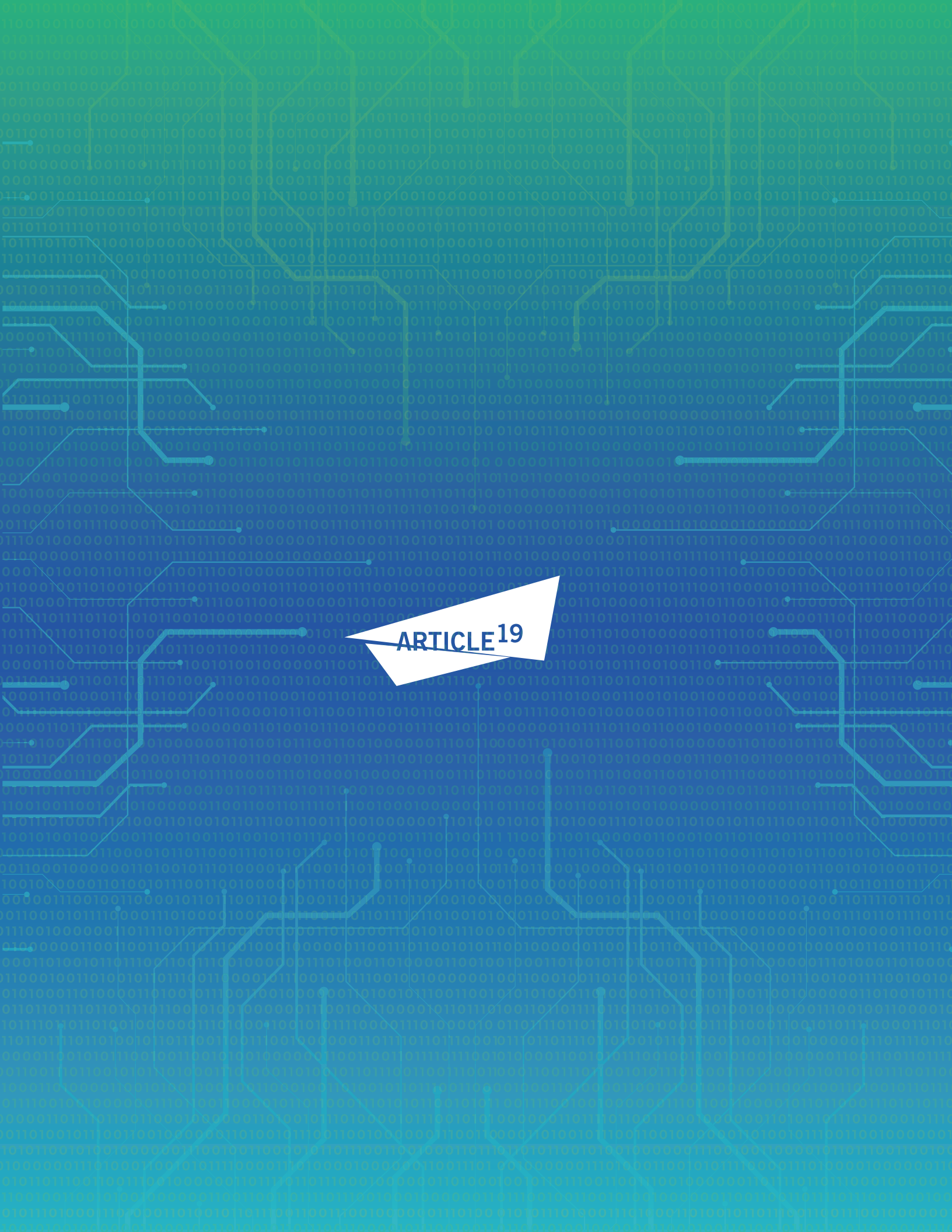
Es esencial la creación de un protocolo específico que regule la recolección y el procesamiento de datos en fuentes abiertas, mismo que deberá ser aplicado por todas las instituciones de seguridad pública de las entidades federativas y cumplir con el principio de máxima publicidad.

El protocolo deberá precisar qué tipo de datos se pueden recolectar en fuentes abiertas y qué fines cumplirá dicha recolección; además, procurará proteger la privacidad de las personas usuarias y tolerar todas las expresiones permitidas por el marco jurídico mexicano e internacional en materia de libertad de expresión.

El documento deberá establecer principios de rendición de cuentas, como la publicación de reportes que señalen las prácticas que se realizaron en fuentes abiertas digitales, la asignación de recursos y el gasto realizado para esas tareas en cuanto a licencias, *software* y equipo. Igualmente, el protocolo debe establecer los principios previstos por la Ley General de Protección de Datos en Posesión de Sujetos Obligados para que los titulares de los datos puedan ejercer sus derechos de acceso, rectificación, cancelación y oposición.

En segunda instancia, si bien la mayoría de las entidades académicas no cuentan con protocolos que guíen o limiten las prácticas de OSINT, y en adición, sus publicaciones no revelan datos personales, es imprescindible que las y los investigadores contemplen y discutan en torno a la proporcionalidad de la recolección y el procesamiento para no vulnerar los derechos de las personas usuarias en las plataformas digitales, así como adecuar las medidas requeridas para el debido resguardo de la información.

Por último, el sector privado debería dar a conocer aquellos contratos en relación con las instancias de seguridad del Estado, a fin de que la sociedad conozca las prácticas, así como los montos que reciben por llevar a cabo tareas con fines de inteligencia que contengan la recolección de datos personales en fuentes abiertas. Asimismo, procurar que sus avisos de privacidad sean una lectura accesible y que sean visibles para que las personas usuarias puedan decidir sobre sus datos.


ARTICLE 19